ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA METODOLOGÍA MAGERIT PARA EL ÁREA DE DATACENTER DE UNA ENTIDAD PROMOTORA DE SALUD

CARLOS ARTURO GUAMANGA CHILITO
CARLOS LEONARDO PERILLA BUITRAGO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2015

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA METODOLOGÍA MAGERIT PARA EL ÁREA DE DATACENTER DE UNA ENTIDAD PROMOTORA DE SALUD

CARLOS ARTURO GUAMANGA CHILITO
CARLOS LEONARDO PERILLA BUITRAGO

Proyecto de grado para optar al título de
Especialista en Seguridad Informática

Director:
ING. CESAR RODRÍGUEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2015

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma de Jurado

_____

Firma de Jurado

Bogotá D.C. 10 de diciembre de 2015

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

En Colombia una entidad promotora de salud, que en adelante se le denominara EPS, puede pertenecer a dos regímenes ya sea contributivo o subsidiado. Para contextualizar, el régimen contributivo es en el cual se afilian las personas con capacidad de pago, es decir que tienen un vínculo laboral como los trabajadores formales e informales. Por otro lado el régimen subsidiado es el que da cobertura a la población de escasos recursos, haciendo que dicha población tenga acceso al derecho de la salud por medio del estado colombiano que a su vez delega responsabilidades a los entes territoriales.

Como tal una EPS no presta el servicio médico, las entidades encargadas de prestar dichos servicios son las IPS (instituciones prestadoras de servicios), es decir los hospitales, clínicas y centros médicos. La función de una EPS es promover la afiliación de las personas al sistema de seguridad social, una vez la persona es afiliada, la EPS se encarga de actualizar y almacenar su hoja de vida o más conocida como historia clínica, con base en las novedades que reporten las IPS.

Dentro de la hoja de vida de un paciente en la EPS se puede encontrar historial clínico, estado de afiliación, grupo familiar, citas faltantes, citas cumplidas, cantidad de hospitalizaciones entre otras. El dato más sensible sin lugar a dudas es el historial clínico puesto que allí se encuentra toda la información médica del afiliado, esta información solo puede ser accedida por personal autorizado de la EPS y también por solicitud del afiliado.

Es responsabilidad de la EPS almacenar y brindar el cuidado adecuado a todas las historias clínicas de sus afiliados, aunque aún se manejan las historias en documentos físicos, hoy en día la mayor parte se maneja en medios digitales. Para el caso de la EPS en estudio de este proyecto no es la excepción, ya que para alimentar las historias clínicas de sus afiliados hace uso de sistemas de información los cuales procesan y almacenan la información en bases de datos que su vez se alojan en servidores ubicados en los datacenter de la EPS en la ciudad de Bogotá.

Al estar concentrada toda la información de cientos de afiliados se crea la necesidad de gestionar los posibles riesgos a los que pueda estar expuesta, bien sean de origen externo o interno. Suponga un escenario en el que se divulga públicamente sin autorización las historias clínicas de diversos afiliados, esto

podría acarrear altas multas a la EPS o una fuerte sanción por parte de las entidades competentes. Es por esto que es pertinente una buena gestión de riesgos, así la EPS reduce la posibilidad de que este y otros escenarios negativos se materialicen.

La EPS que se estudia en este proyecto concentra sus comunicaciones e información digital en dos datacenter, uno principal y el otro alterno; ambos ubicados en la ciudad de Bogotá D.C. El datacenter principal es administrado por un proveedor externo con características de Tier3 y el datacenter alterno por el área de centro de datos de la EPS. Se ha identificado la carencia de gestión de riesgos de la seguridad de la información, constituyéndose en un riesgo inminente para la continuidad del negocio en caso de materialización de los riesgos de la EPS.

Con este proyecto se busca conocer y analizar los riesgos presentes en el área de datacenter utilizando diversas matrices y escalas en las que se pueda tener gestión de los mismos. Al aplicar una buena gestión de los riesgos se pueden controlar nuevos riesgos generados por la operación o crecimiento de la EPS, al igual se tiene monitoreo de controles aplicados y actualización de los mismos.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar un análisis de riesgos de seguridad de la información para el área de datacenter de una EPS, aplicando una metodología que permita identificar los activos, las amenazas y los controles existentes.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico en el área datacenter para la Identificación de riesgos inherentes de seguridad de la información.

- Analizar y clasificar los riesgos encontrados de acuerdo a su nivel de impacto y probabilidad de ocurrencia.

- Evaluar y comunicar a los directivos de la EPS los resultados del análisis de riesgos y la situación actual del área de datacenter.

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

Estamos en una era en que la información es el activo más preciado para nuestras empresas e incluso para nuestra vida cotidiana, se puede decir incluso, que causa más impacto en una empresa el daño de un servidor que un robo a sus instalaciones; con la inclusión de nuevas tecnologías y la masificación de la información viajando por diferentes canales, se hace evidente que el perfil de riesgos para las personas y empresas también cambia, incrementando el nivel de riesgos de la información en sus tres aspectos fundamentales, disponibilidad, integridad y confidencialidad.

Es por esto, que las empresas de ahora tienen áreas especializadas en la mitigación de los riesgos, elaborando estrategias tales como los planes para la gestión de dichos riesgos totalmente alineados al plan estratégico del negocio.
Teniendo en cuenta este preámbulo, este proyecto se apoyó en avances de los planes de gestión de riesgos ya aplicados en algunas empresas siguiendo como directriz las normas ISO 27001, 27005 las cuales suministran directrices para la gestión de riesgos.

Aunque las normas ISO son el estándar internacional, no se dejaron de lado otras metodologías de análisis de riesgos, como es el caso de Magerit, la cual se detalla en el diseño metodológico.

Para cualquier metodología siempre van a haber elementos transversales en el análisis y gestión de riesgos, que para entenderlos mejor se describen a continuación:

Activo: es cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección[1].

Vulnerabilidad: debilidad inherente al activo, su presencia no causa daño por sí misma, ya que necesita presentarse una amenaza que la explote[2].

Amenaza: circunstancia o evento que tiene el potencial de causar daño a un activo y por lo tanto a la organización[3].

[1] SECUREIT INFORMATION TECHNOLOGIES. ¿Qué es activo?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://secureit.com.mx/gestion-de-riesgos/
[2] SECUREIT INFORMATION TECHNOLOGIES. ¿Qué es vulnerabilidad?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://secureit.com.mx/gestion-de-riesgos/
[3] SECUREIT INFORMATION TECHNOLOGIES. ¿Qué es Amenaza?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://secureit.com.mx/gestion-de-riesgos/

Impacto: daño causado por una amenaza que explota una vulnerabilidad en un activo y que afecta adversamente los objetivos de negocio[4].

Riesgo en la seguridad de la información: potencial de que una amenaza explote las vulnerabilidades de un activo, causando daño a la organización[5].

Según Manual de certificación CISM 2012 la gestión de riesgos se define como:

"La gestión de riesgos es, en términos generales, un proceso encaminado a alcanzar el equilibrio óptimo entre concretar oportunidades para obtener ganancias y minimizar las vulnerabilidades y las pérdidas."

"La gestión de riesgos, el desarrollo de las evaluaciones y los análisis de impacto al negocio son requerimientos previos fundamentales para el desarrollo de una estrategia de seguridad de la información efectiva"[6].

2.2 MARCO LEGAL

De acuerdo a las leyes colombianas las EPS están obligadas a cumplir con ciertas condiciones en el manejo de su información y brindar los mecanismos apropiados para garantizar la integridad, disponibilidad y confidencialidad de la información de sus beneficiarios o afiliados. La resolución 1995 de 1999, del Ministerio de Salud establece las normas para el manejo de la historia clínica.

Dentro de esta norma se pueden encontrar varios artículos que de manera general imparten directrices a todas las EPS de Colombia, entre estos los más importantes son:

Artículo 16: trata de la seguridad que debe tener la EPS en el lugar donde almacene las historias clínicas, además de velar por la conservación de la misma. También ordena que el lugar en donde se almacenen solo podrá ser accedido por personal autorizado con el fin de garantizar la integridad de las historias clínicas.

---

[4] INCONTEC. NTC-ISO/IEC 27005:2008. ¿Qué es impacto?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://tienda.icontec.org/brief/NTC-ISO-IEC27005.pdf

[5] INCONTEC. NTC-ISO/IEC 27005:2008. ¿Qué es Riesgo en la seguridad de la información?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://tienda.icontec.org/brief/NTC-ISO-IEC27005.pdf

[6] ISACA; CSIM. Manual de certificación CISM 2012. [en línea] , [consultado en Febrero de 2015]. disponible en: http://www.isaca.org/chapters7/Madrid/Events/Formacion/Pages/Curso-de-preparacion-CISM.aspx

Artículo 17: trata de las condiciones físicas en las cuales se deben almacenar las historias clínicas, siguiendo los parámetros establece el Archivo General de la Nación.

Artículo 18: trata se los medios técnicos que se usan para el registro y conservación de las historias clínicas. Este artículo deja de lado los documentos físicos y se enfoca en los sistemas automatizados que procesan la información que se almacena en la historia clínica y todo lo que intervenga en este proceso, incluyendo personas y equipos. Para lo anterior se imparten ciertas condiciones:

- Equipos, sistemas y sus respectivos soportes deben tener mecanismos de seguridad, con el fin de que no se alteren sin autorización las historias clínicas una vez sean guardadas.

- La historia clínica se debe proteger por mecanismos de seguridad que impidan que se elimine o destruya de forma accidental o intencionada.

- Los sistemas deben identificar al personal responsable de cargar datos a las historias clínicas, por medio de códigos o identificadores únicos, de manera que se conozca con certeza la persona que realizo algún cambio, la fecha y hora del mismo.

3. DISEÑO METODOLÓGICO

Se realizó un estudio comparativo entre la metodología ISO27005 Y MAGERIT con el objetivo de aplicar la que mejor se adapte y le convenga más al datacenter de la EPS:

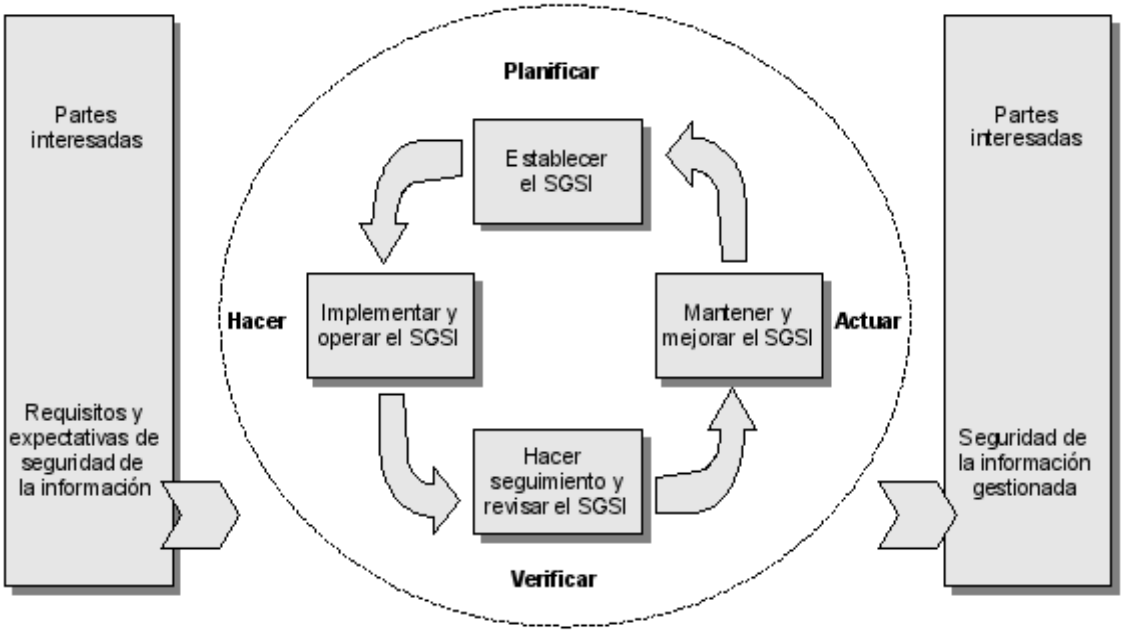
3.1 ISO 27005

Esta norma se enfoca específicamente en la gestión de los riesgos de seguridad de la información, apoyándose en los conceptos y lineamientos que imparte ISO 27001 – Gestión de la seguridad de la información.

ISO 27001 tiene inmerso el proceso de "análisis y gestión de riesgos" en la etapa de implementación del SGSI, pero ISO 27005 va más allá, debido a que se enfoca únicamente en riesgos de seguridad de la información y aplica el ciclo PHVA.

La figura 1 muestra las fases de implantación de un sistema de gestión de seguridad de la información SGSI, consta de 4 fases: planificar, hacer, verificar y actuar, conforme a lo anterior recibe el nombre de ciclo PHVA.

Figura 1. Ciclo PHVA - ISO 27005



Fuente: Ofiseg Consulting, S.L. Modelo para implementar un SGSI. 2010. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://www.ofisegconsulting.com/iso27000.htm

3.1.1 Pasos para su aplicación

3.1.1.1 Paso 1: Establecimiento del contexto. El contexto de la organización se debe conocer tanto interno como externo, así como la actividad a la que se dedica y sus procesos críticos. Una vez se conoce el 'core' del negocio hay que identificar toda la información acerca de la organización relevante a la gestión de seguridad de la información. En este paso por lo general se trabaja en conjunto con el área de tecnología de la organización.

Establecer el contexto de la organización ayuda inicialmente a formular un diagnóstico del estado en que se encuentra la misma, además de establecer el alcance del proceso de gestión de riesgos. Una forma práctica de comenzar a establecer el contexto es por medio de la matriz DOFA.

3.1.1.2 Paso 2: Valoración del riesgo en la seguridad de la información. Se deben clasificar los riesgos debido a su criticidad y nivel de aceptación de la organización. El riesgo depende de varios componentes o elementos que de cumplirse hacen que se materialice, los componentes del riesgo son: activos, vulnerabilidades, amenazas, eventos, impacto.

La valoración del riesgo consta de las siguientes sub etapas:

- **Identificación de Activos**: son todos aquellos que tienen valor para la organización y por consiguiente deben protegerse. No basta solo con identificarlos sino que se debe hacer una descripción de cada uno para que la información sea suficiente en el momento de realizar la valoración del riesgo. Finalmente si se materializa el riesgo lo que se ve afectado es el activo, por ello es importante que estén bien documentados.

- **Identificación de Vulnerabilidades**: se deben identificar las vulnerabilidades que puedan ser explotadas por las amenazas y a su vez afecten los activos. La vulnerabilidad también puede ser vista como las debilidades que tenga el activo.

- **Identificación de Amenazas**: una vez se determinan las vulnerabilidades, hay que listar las posibles amenazas que las pueden explotar. Para esto se deben clasificar según su tipo: naturales, humanas, operacionales, sociales, técnicas, etc.

- **Identificación de Controles:** por lo general la identificación de los controles existentes se realiza inspeccionando cada proceso y área responsable. Sin embargo se pueden comparar los controles que hay frente al listado de controles recomendados por ISO 27001.

- **Identificación de impactos**: esta etapa consiste en identificar los daños que puede llegar a generar en el evento que una amenaza explote la vulnerabilidad y afecte el activo de la organización. El impacto se puede clasificar en términos de tiempo de investigación y reparación, tiempo de trabajo perdido, costo financiero o pérdida de imagen, costo de recuperación, etc.

3.1.1.3 Paso 3: Análisis de riesgos. El análisis se realiza en diferentes grados de exactitud, dependiendo de los criterios y escalas cualitativas/cuantitativas que se utilicen. A esto se le conocen como métricas ya que son más fáciles de entender y calcular. Algunos ejemplos de cómo se pueden aplicar son:

- **Valorar impactos:** es directamente relacionado con el activo y se puede medir en una escala numérica en donde 0 es un impacto insignificante y 5 es grave.

- **Valorar Probabilidades:** hace referencia a la probabilidad de ocurrencia de un evento de riesgo y se puede calcular por medio de una escala numérica, en donde 0 es nula/rara vez ocurre y 5 es extrema/pasa varias veces a la semana.

Finalmente se toman las dos métricas anteriores y se procede a estimar el riesgo.

La figura 2 muestra un ejemplo de cómo se puede estimar nivel de riesgo con base a la valoración del impacto y la probabilidad, dando como resultado un mapa de calor y sus respectivas zonas de riesgo.

Figura 2. Ejemplo de estimación del riesgo

	Impacto				
Probabilidad	Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
Raro 1	Bajo	Bajo	Moderado	Alto	Alto
Improbable 2	Bajo	Bajo	Moderado	Alto	Extremo
Posible 3	Bajo	Moderado	Alto	Extremo	Extremo
Probable 4	Moderado	Alto	Alto	Extremo	Extremo
Casi seguro 5	Alto	Alto	Extremo	Extremo	Extremo

Extremo: Los riesgos extremos deben ponerse en conocimiento de los Directores y ser objeto de seguimiento permanente.
Alto: Los riesgos altos requieren la atención del Presidente / Director General / Director Ejecutivo.
Moderado: Los riesgos moderados deben ser objeto de seguimiento adecuado por parte de los niveles medios de Dirección.
Bajo: Los riesgos bajos deben ser objeto de seguimiento por parte de los supervisores.

Fuente: Riesgo y administración del riesgo. ¿Qué es una Matriz de Riesgo?. [en línea], [consultado el 24 de marzo de 2015]. Disponible en: https://swescom.wordpress.com/riesgo-y-administracion-del-riesgo/

3.1.1.4 Paso 4: Evaluación del riesgo. La evaluación del riesgo siempre se debe realizar con los dueños de proceso y la gerencia de la organización ya que en este paso se compara el nivel de riesgo encontrado en el paso anterior y el nivel de aceptación que tiene la empresa.

A partir de esta comparación se debe determinar si la empresa acepta o no los riesgos.

3.1.1.5 Paso 5: Tratamiento del Riesgo. Luego del resultado de la valoración del riesgo se debe dar tratamiento a los riesgos latentes que la empresa no acepta, haciendo uso de las estrategias ya conocidas:

- Reducir o mitigar
- Asumir o retener
- Evitar
- Transferir

Una vez se aplica alguna estrategia se debe evaluar si en verdad se redujo el nivel de riesgo y proceder a calcular el nivel de riesgo residual.

3.1.1.6 Paso 6: Comunicación del riesgo. Se deben proponer acuerdos de cómo gestionar los riesgos, compartiendo información entre los dueños de los procesos y los encargados de ejecutar las acciones.

La organización debe implementar planes de comunicación de riesgo tanto para operaciones normales como para las situaciones de emergencia. Por lo tanto se deben verificar con cierta periodicidad.

3.1.1.7 Paso 7: Monitoreo y revisión del riesgo. Por último se debe hacer un monitoreo constante ya que los riesgos no son estáticos y esto implica que se deben identificar nuevos activos, nuevas amenazas, nuevas vulnerabilidades y de ser necesario replantear las escalas de impacto y probabilidad. Para estar al tanto de nuevas amenazas y vulnerabilidades se puede optar por servicios externos como los boletines informativos de las casas de antivirus y de seguridad.

3.2 MAGERIT

Acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, es una metodología para el análisis y la gestión de riesgos

desarrollada por el Consejo Superior de Administración Electrónica CSAE. Esta metodología es abierta al público y cualquier persona puede hacer uso de la misma sin necesidad de solicitar autorización del Ministerio de Administraciones Publicas de España.

Actualizada en 2012 a la versión 3 consta de tres libros:

- Libro I: Método
- Libro II: Catálogo de Elementos
- Libro III: Guía de Técnicas

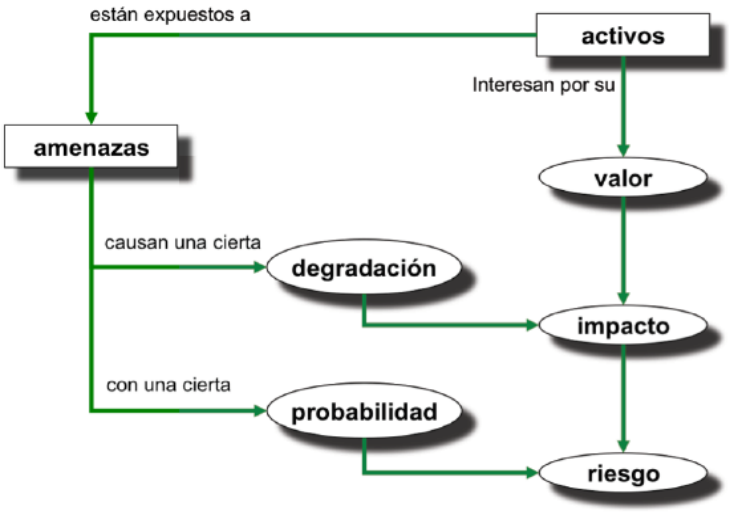
Los tres libros son gratuitos y se pueden encontrar en sitio web del Portal de Administración Electrónica de España.

3.2.1 Pasos para el análisis de riesgos

3.2.1.1 Paso 1: Activos. Determinar los activos más importantes para la empresa, su valor y nivel de criticidad en caso de que se vea afectado.

La figura 3 reúne las variables y elementos que se derivan de la importancia de proteger los activos.

Figura 3. Elementos del análisis de riesgos.



Fuente: MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.]. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

3.2.1.2 Paso 2: Amenazas. Determinar las amenazas que pueden llegar a afectar los activos identificados en el paso anterior. Se debe tener en cuenta no solo factores internos sino también ajenos a la organización.

Dentro del capítulo 5 del libro II “Catálogo de elementos” brindan varios tipos de amenaza:

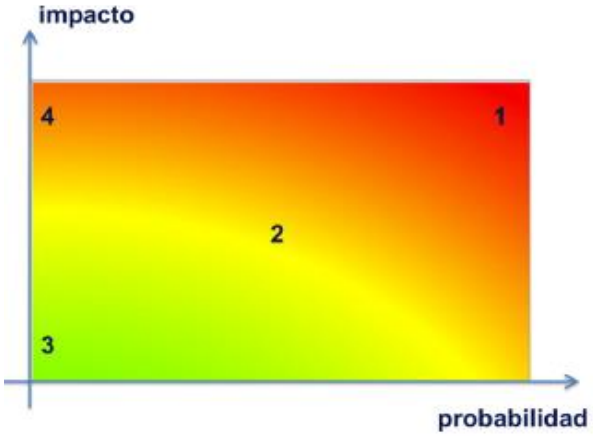
- De origen natural
- De origen industrial
- Fallas en las aplicaciones
- De origen Humano

Esta última puede ser de forma accidental o intencionada.

Una vez se identifican y se clasifican las amenazas se debe valorar en qué grado puede afectar el activo, a esto se le conoce como impacto potencial. Se usan los criterios de probabilidad e impacto. En ambos casos se pueden usar métricas, por ejemplo para determinar la probabilidad es más cómodo usar una métrica cuantitativa que representaría la frecuencia de ocurrencia. Para el caso del impacto al activo se usa una métrica cualitativa que da una escala de muy alta a muy baja.

En la figura 4 se observa el riesgo en función del nivel de impacto y la probabilidad de ocurrencia, también se nota que entre mayor sea la valoración del impacto y más probabilidades tenga de suceder, el riesgo aumenta.

Figura 4. El riesgo en función del impacto y la probabilidad



Fuente: MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.]. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

En la figura 4 cada número corresponde a una zona:

- Zona 1: riesgos críticos con probabilidad e impacto muy alto.

- Zona 2: riesgos con situaciones improbables y de impacto medio o riesgos muy probables pero de impacto bajo o muy bajo.

- Zona 3: riesgos improbables y de impacto bajo

- Zona 4: riesgos improbables pero de impacto muy alto

Se tienen en cuenta los siguientes aspectos antes del Paso 3 salvaguardas, en el caso que no hubiese controles implementados:

Impacto potencial. Es el nivel de degradación del activo por causa de la materialización de una determinada amenaza, se aclara que aunque una misma amenaza afecte a más de un activo, su nivel de degradación o impacto puede ser diferente. Lo anterior debido a que no todos los activos tienen el mismo valor y hay unos más importantes para la organización que otros. Para calcular el impacto potencial por lo general se emplea una escala en la que se determina el nivel de degradación del activo. Dicha escala se aplica por cada amenaza y a su vez por cada activo.

Riesgo potencial. Como se puede observar en la figura 4, el riesgo potencial se calcula con base al impacto potencial que genera una amenaza y su probabilidad de ocurrencia. Tomando estas dos variables se puede decir que entre más alto sea el impacto y más probable sea la ocurrencia más crítico será el riesgo. Sin embargo para medir el riesgo se emplea un mapa de calor en el cual se ubican los niveles resultantes del impacto potencial y la probabilidad, su ubicación determinara la zona de riesgo y por lo tanto el nivel del mismo.

3.2.1.3 Paso 3: Salvaguardas. Este paso consiste en determinar que salvaguardas o controles existen actualmente en la organización y verificar su nivel de eficacia frente al riesgo.

Una vez determinado el nivel de riesgo potencial, se debe hacer la verificación de que salvaguarda de los que se identificaron hace que el riesgo se mitigue o por lo menos su nivel baje. La efectividad del salvaguarda puede darse de dos formas, la primera reduciendo la probabilidad de las amenazas y la segunda limitando el daño causado al activo.

Los salvaguardas pueden prestar distintos tipos de protección dependiendo del activo, los más comunes son: preventivo, detectivo, correctivo y disuasivo. Sin embargo para obtener un abanico más amplio de controles, en el capítulo 6 del libro II “Catalogo de elementos” se detallan los más adecuados para cada tipo de activo.

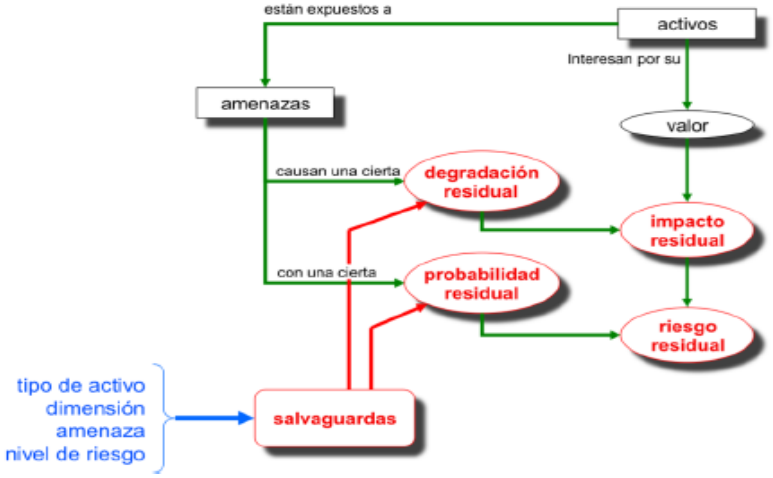
3.2.1.4 Paso 4: Impacto residual. Se define como el daño sobre el activo debido de la materialización de la amenaza aun existiendo las salvaguardas, es decir pasó de impacto potencial a impacto residual. Para calcularlo se debe realizar el mismo procedimiento que se usó para hallar el impacto potencial, con la diferencia que se le debe aplicar la efectividad del control, con esto logra que la degradación del activo disminuya o sea nula.

En el Libro III “Guía de técnicas” se pueden encontrar diversos modelos, métricas y escalas en las que se pueden calcular las diferentes variables.

3.2.1.5 Paso 5: Riesgo residual. El riesgo residual se calcula usando el impacto residual y la probabilidad residual de ocurrencia (es residual en caso de que las salvaguardas afecten la frecuencia de ocurrencia).

La figura 5 muestra como las salvaguardas intervienen directamente disminuyendo la degradación causada por una amenaza y la probabilidad de la misma, dando como resultado el nivel de riesgo residual.

Figura 5. Elementos de análisis del riesgo residual



Fuente: MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.]. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Me

todologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

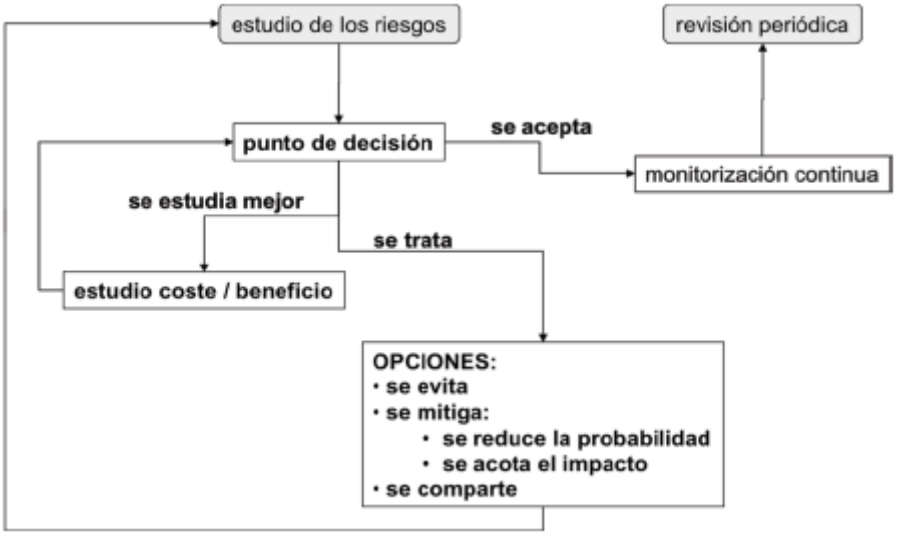
3.2.2 Proceso de gestión de riesgos. Finalizado el proceso de análisis de riesgos se debe comenzar su gestión, que comprende las actividades del tratamiento del riesgo residual. Lo primero que se debe realizar es darle una calificación a cada riesgo:

- Crítico: requiere atención inmediatamente
- Grave: requiere atención
- Apreciable: podría ser objeto de estudio para su tratamiento
- Asumible: se acepta el riesgo y no se toman acciones al respecto.

La calificación anterior se deriva del impacto o consecuencias que puedan derivar a causa de la materialización de una amenaza, dichas consecuencias por lo general afectan la imagen pública de la organización, indisponibilidad de servicio, pérdidas económicas e implicaciones legales.

La figura 6 muestra un esquema de la gestión del riesgo con las actividades y decisiones que se deben realizar una vez se termina el análisis de riesgos, en cierta medida combina en un solo diagrama el proceso de análisis y gestión.

Figura 6. Actividades del tratamiento de los riesgos



Fuente: MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.]. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

3.3 SELECCIÓN DE LA METODOLOGÍA.

Esta parte es de suma importancia para el desarrollo del proyecto, es en la cual se decide que metodología es la más apta y la que mejor le conviene al área de datacenter de la EPS. Se estudiaron de manera general y superficial ambas metodologías sin adentrar en la parte técnica como tablas, estadísticas, métricas, etc.

En el cuadro 1 se realiza una comparación entre las metodologías ISO27005 y Magerit, de los aspectos más relevantes como: costo, factibilidad y aplicabilidad.

Cuadro 1. Comparación de metodologías

Beneficio - Característica	ISO27005	MAGERIT
Costo	Se debe comprar la norma, además se debe contar con la norma ISO27001 en el caso de requerir alguna referencia específica.	Es de uso libre y los 3 libros de la metodología son gratuitos para su descarga.
Factibilidad	Consta de 7 fases para su implementación, pero dependiendo el proyecto debe recurrir al SGSI que imparte ISO27001.	Consta de 5 pasos para su desarrollo e implementación. Se enfoca especialmente en el análisis de riesgos de la información.
Aplicabilidad	Sistemática, rigurosa y compleja para su aplicación en el caso de una empresa mediana o pequeña.	De fácil aplicación para cualquier tipo de empresa y que no tengan algún tipo de experiencia en un sistema de gestión de riesgos.

Fuente: autores

La metodología seleccionada como guía y para el desarrollo del análisis de riesgos es Magerit, por las siguientes razones:

- Consta de 5 pasos documentados y argumentados de forma muy clara para realizar el análisis de riesgos. De esta forma reduce la generación de posibles dudas o vacíos que se puedan presentar en el momento del desarrollo.

- Separa el proceso de análisis del proceso de gestión, enfocándose en los resultados del primero para hacer uso de estos en la parte evaluativa de los riesgos.

- Es una metodología de uso público, es decir se puede hacer uso de ella sin ningún problema. Adicional está disponible para descargar los tres libros de forma gratuita y en español.

- Es ideal para empresas que no tienen experiencia o conocimiento en la gestión de riesgos de la información.

- Se encuentra alineado a los estándares que imparten las normas ISO y se puede convertir en la base para una futura certificación.

4. DESARROLLO, RESULTADOS Y APORTES

4.1 DEFINICIÓN DE METODOLOGÍA Y APROBACIÓN DE LAS ETAPAS O FASES DE TRABAJO

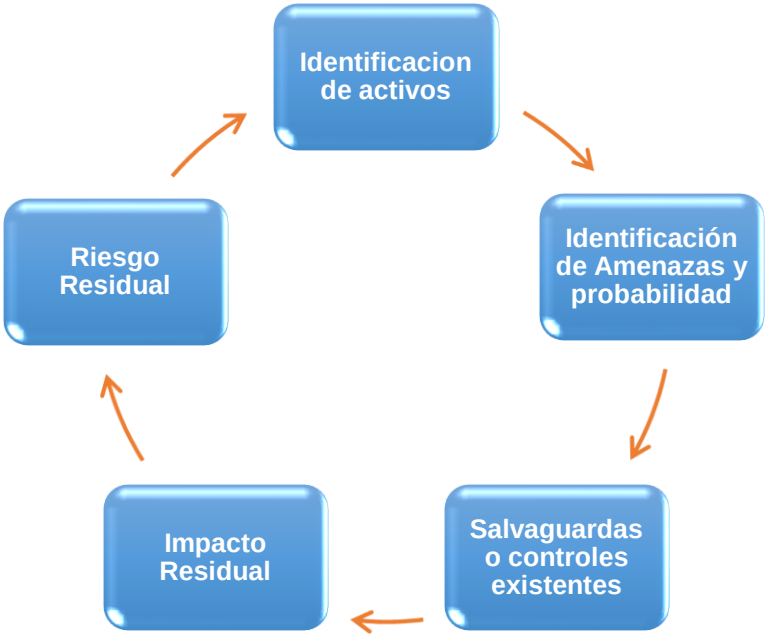
Para comenzar con el desarrollo de este proyecto de grado, fue necesario establecer reuniones con los altos directivos de la EPS, donde se les compartió la información de la metodología Magerit y sus ventajas frente a otras metodologías.

Al igual se comparte la idea de no olvidar la ISO27001 para alinearse a los estándares de nuestro país.

Después de que se define la metodología con la cual se va a abordar el análisis de los riesgos inherentes a un centro de datos de una EPS en Colombia, se definen las etapas o fases a seguir para lograr una identificación efectiva de los riesgos y tratamiento de los mismos.

La figura 7 establece el flujo de trabajo para el desarrollo del análisis de riesgos bajo la metodología Magerit.

Figura 7. Fases de trabajo - metodología Magerit



Fuente: autores

- Por lo tanto para el desarrollo de primera fase es necesario establecer un equipo de trabajo para la identificación de los activos que pasan o son inherentes al centro de datos de la EPS.

- El equipo se establece mediante una reunión con los directivos de la EPS, para que brinden el tiempo y el apoyo en cuanto al conocimiento de la misma, por lo cual se define en las siguientes actividades:

4.2 CONFORMACIÓN DEL EQUIPO DE TRABAJO

4.2.1 Roles y responsabilidades del equipo de análisis

- Trabajar con los directivos y dueño de los procesos para identificar, evaluar y seleccionar los activos de la EPS.

- Coordinar con los directivos, dueños de procesos, administradores de infraestructura y administradores de la información para identificar las vulnerabilidades que se encuentran en cada uno de los procesos.

- Recopilar y analizar las vulnerabilidades encontradas para realizar la construcción de la matriz de riesgos inherentes en el centro de datos de la EPS.

4.2.2 Habilidades del equipo de análisis

- Habilidades de trabajo en equipo.

- Habilidades Analíticas.

- Habilidades de para desarrollar y presentar trabajos con los altos directivos, directivos de áreas operativas y personal en general.

- Análisis y conocimiento de la EPS.

- Conocimiento sobre la infraestructura y la información de la EPS.

Se conformó un equipo de trabajo interdisciplinario para realizar la identificación de los activos, vulnerabilidades implícitas en los mismos y posterior análisis para la construcción de las matrices de riesgos para dar el tratamiento adecuado.

Equipo de trabajo, que de ahora en adelante se denominara SGI (Sistema Gestión de Información):

- Estudiante especialización seguridad informática (Externo).

- Estudiante especialización seguridad informática (Administrador de infraestructura de la EPS).
- Director de tecnología.
- Vicepresidenta de operaciones y tecnología.
- Oficial de seguridad.

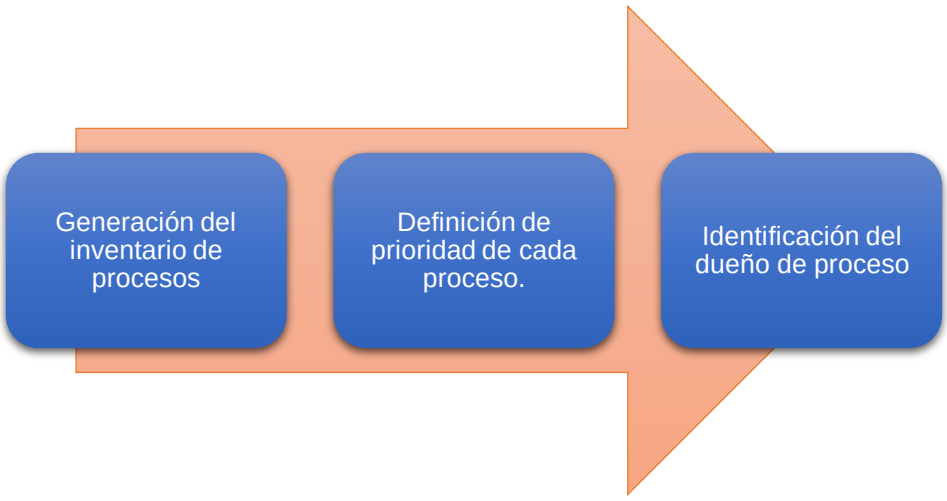
4.3 IDENTIFICACIÓN DE ACTIVOS

Dando inicio a la primera fase establecida para el desarrollo de este proyecto de grado y siguiendo con los pasos de la metodología Magerit, se procede con la identificación de los activos inherentes en el centro de datos de la EPS.

El objetivo de esta fase es identificar y/o validar los procesos para los cuales la EPS desea y debe realizar una identificación y clasificación de activos, que intervengan o que se vean afectados por el área de centro de datos de la EPS.

La figura 8 describe las 3 actividades que se deben realizar con antelación para que la identificación de activos sea efectiva.

Figura 8. Actividades previas a la identificación de activos



Fuente: autores

Las actividades antes mencionadas se alinearon así:

Generación del inventario de procesos. Se genera un listado completo de los procesos de la EPS, tanto estratégicos, misionales y de apoyo.

Definición de prioridad de cada proceso. Priorizar los procesos de acuerdo con los criterios que considere pertinentes la EPS. Por ejemplo: importancia del proceso para el cumplimiento de los objetivos de negocio, materialidad del proceso, procesos prioritarios según lineamientos de entidades reguladoras, entre otros.

Identificación del dueño de proceso. Identificar y registrar el dueño de cada proceso listado en el inventario.

Con los procesos ya listados, debidamente documentados y con sus respectivos dueños identificados, se procederá con el inventario de activos de la información.

Entre los principales procesos se encuentran:

- Direccionamiento Estratégico
- Gestión Documental
- Gestión del Talento Humano
- Gestión Contractual
- Gestión Financiera
- Gestión Legal
- Gestión de Bienes y Servicios
- Gestión de Tecnologías de Información
- Mejora Continua
- Área de Telemática

Se procede a realizar reuniones con los dueños de los procesos, el personal idóneo por su conocimiento en el sector de la salud y la EPS, así como personal propio del centro de datos o que intervienen con el centro de datos de la EPS, todo esto con el objetivo de realizar el inventario de activos de información.

A continuación se describen los cargos de los funcionarios entrevistados. Cabe anotar que para efectos de este proyecto de grado, no se anexaran las actas de las reuniones realizadas debido a políticas de confidencialidad de la EPS.

- Director de operaciones
- Operador de backups
- Directora de riesgos
- Coordinador de activos fijos y mantenimiento
- Coordinador de telecomunicaciones
- Administradores de Infraestructura
- DBA

4.3.1 Elaboración del inventario de activos de información

4.3.1.1 Consideraciones para la elaboración del Inventario. A continuación, algunas consideraciones importantes que se tuvieron en cuenta en la elaboración del inventario de activos de información.

¿Cómo se identificaron los activos de información? Para realizar la identificación de los activos de información de cada uno de los procesos se tuvieron en cuenta los siguientes tipos de activos de información que comúnmente intervienen en los procesos:

- Soportes físicos que intervienen en los procesos. Es decir, documentos que apoyen o definan los procesos.
- Manuales, procedimiento y en general documentación de proceso.
- Uso de herramientas de Ofimática para el desarrollo de las actividades de los procesos (archivos de Word, Excel, PowerPoint, Access, archivos de texto, correos electrónicos, etc.)
- Registros de transacciones u operaciones electrónicas que se llevan a cabo durante el proceso, identificando adicionalmente aplicaciones y sistemas involucrados.

Adicionalmente, para facilitar la identificación de los activos se utilizó el siguiente cuestionario:

- ¿Durante el proceso, se utiliza, transforma, extrae o genera información a través de archivos electrónicos de Excel, Word, Access, PowerPoint, archivos de texto?

- ¿Se utiliza, transforma, extrae o genera información que se encuentra o se registra en una base de datos?

- ¿Se utiliza, transforma, extrae o genera información que se encuentra o registra en una aplicación?

- Como parte del proceso, ¿se ejecuta alguna interfaz entre aplicaciones mediante la cual se transfiera un archivo o lotes de información?

- ¿Qué información se imprime y/o se utiliza, transforma o genera en papel?

- ¿Existe información en papel que además durante el proceso sea digitalizada?

Existencia única de un activo de información

- Cada activo de información debe tener un único número consecutivo que lo identifique. No deben registrarse dos activos de información con las mismas características y números consecutivos diferentes.

- Un mismo activo de información puede hacer parte de varios procesos. En este caso no se debe repetir el activo de información; se debe tener en cuenta el activo ya existente en el inventario y complementar la información que ya tiene creada.

4.3.1.2 Levantamiento de activos de información. El propósito de este proceso es hacer una recolección de los activos de información involucrados en los procesos críticos identificados en el proceso anterior, ya sea información de entrada, salida o utilización dentro del proceso. Para ello, se realizaron reuniones de identificación y validación de activos de información con los dueños de los procesos y demás personal idóneo para la elaboración de los perfiles de información.

Cabe aclarar que pueden existir varias clases de activos de información por ejemplo: de hardware, de software y de información (digital y física), por lo que se definen tres tipos de matrices para el levantamiento de información y su posterior caracterización.

La tabla 1 muestra las columnas o campos a diligenciar, cuando el activo sea de tipo hardware.

Tabla 1. Ejemplo activo de hardware

Tipo de activo	Nombre de activo	Sistema operativo (si aplica)/ versión software
Servidor	Server 1	WINDOWS 2003

Fuente: autores

La tabla 2 muestra las columnas o campos a diligenciar, cuando el activo sea de tipo software.

Tabla 2. Ejemplo activo de software

Tipo de activo	Nombre de activo	Tipo de aplicación
Software	Office Professional	Ofimática

Fuente: autores

La tabla 3 muestra las columnas o campos a diligenciar, cuando el activo sea de tipo información.

Tabla 3. Ejemplo activo de información

Tipo de activo	Información física/digital	Nombre de activo
Documento	Digital	Guías

Fuente: autores

Lo próximo que se debe registrar son las características de los activos de información identificados (información de la aplicación ejecutada, base de datos, entre otros) estas características fueron registradas en la matriz o formato de inventario de información.

En este proceso se registraron las características básicas de cada activo de información, tales como: Sistema Operativo, Dirección IP, Base de Datos, Fecha del Inventario.

La tabla 4 muestra un ejemplo de los campos adicionales para la caracterización de un activo tipo hardware.

Tabla 4. Características del activo

Tipo de activo	Nombre de activo	Sistema operativo (si aplica)/ versión software	Dirección IP (si aplica)
Servidor	Server 1	WINDOWS 2003	192.168.1.12

Fuente: autores

En la tabla 5 se observan los campos que se deben diligenciar para definir e identificar el funcionario dueño o propietario del activo, así como también el custodio y su localización.

Tabla 5. Propiedades del activo

Propietario del activo	Custodio del activo/ nombre propietario	Localización	Proceso	Responsable del proceso
Director de tecnología	Tecnología - Director TI	Datacenter principal	Gestión documental	Director gestión documental

Fuente: autores

4.3.1.3 Clasificación de los activos en términos de confidencialidad, integridad y disponibilidad. Esta matriz se construyó utilizando la Metodología propuesta por el oficial de seguridad de la EPS y los estudiantes que desarrollaron este proyecto de grado, para la clasificación de activos de información se tuvieron en cuenta su costo e impacto en términos de confidencialidad, integridad y disponibilidad.

Se procede a realizar una reunión con los funcionarios involucrados en cada uno de los procesos que intervienen en el inventario de activos, indagando acerca de la afectación que sus activos podrían causar en referencia con los dominios mencionados (Confidencialidad, integridad y disponibilidad).

En el cuadro 2 se describe el nivel de clasificación por cada uno de los principios de la seguridad de la información.

Cuadro 2. Clasificación de activos

Principio de seguridad	Clasificación	Definición
Confidencialidad	Público (1)	Esta información es considerada de carácter público y puede ser divulgada a cualquier persona o entidad interna o externa a la EPS, sin ninguna restricción y está contemplada en las leyes de transparencia de datos de Colombia.
	Interna (2)	Esta información es utilizada por los funcionarios autorizados de la EPS para la ejecución de sus labores, y no puede ser conocida por terceros sin autorización del responsable del activo de información o directivas de la EPS.
	Confidencial (3)	Esta información se considera altamente sensible y es utilizada solo por un grupo limitado de funcionarios o áreas para la ejecución de labores y no puede ser conocida por otros funcionarios de la EPS o terceros externos sin autorización especial del Responsable de la información o directivas de la EPS.
Integridad	No sensitiva (1)	La pérdida o modificación no autorizada de esta información podría causar un daño leve o nulo para la EPS.
	Sensitiva (2)	La pérdida o modificación no autorizada de esta información podría causar un daño que genere perjuicios importantes que afectan a la EPS, pero que puede ser absorbido o asumido por éste (Por ejemplo: perjuicios legales, imagen, perjuicios económicos, operación, entre otros).
	Altamente sensitiva (3)	La pérdida o modificación no autorizada de esta información podría causar un daño grave que genere perjuicios que afectan significativamente a la EPS y que difícilmente podrían ser asumidos por éste (Por ejemplo: imagen, perjuicios económicos o legales en los términos que la ley indique, operación, entre otros).
Disponibilidad	No crítico (1)	La información puede no estar disponible por un período de tiempo extendido, sin afectar la operación de la EPS.
	Importante (2)	La no disponibilidad de esta información afectaría operaciones, y servicios de los funcionarios de la EPS.

Principio de seguridad	Clasificación	Definición
	Misión crítica (3)	La no disponibilidad de esta información afectaría significativamente las operaciones, servicios de la EPS y el acceso a la información acorde a lo indicado en la Ley 1712 de 2014 - Ley de Transparencia.

Fuente: autores

Con base en las calificaciones dadas anteriormente, se determinan cualitativamente los impactos potenciales a los cuales se vería enfrentada la EPS en el evento de un incidente de seguridad que comprometa la confidencialidad, integridad y/o disponibilidad, según corresponda.

En el cuadro 3 se muestran las 4 columnas que complementan el inventario de activos. En estas columnas se diligencia el valor del activo dado por la EPS de acuerdo a los tres pilares de la seguridad de la información.

Cuadro 3. Ejemplo de valores de un activo

Clasificación de activos de información			
C	**I**	**D**	**Valor final**
2	2	1	2

Fuente: autores

A continuación se describen los elementos del cuadro anterior:

- C: Confidencialidad
- I: Integridad
- D: Disponibilidad
- Valor Final: Se toma el valor más alto de los tres dominios, para referenciar el activo y conocer su criticidad dentro de la EPS, así como las consecuencias que se pueden llegar a presentar en caso de que se vea vulnerado dicho activo.

Se da por concluida la primera etapa o fase de la metodología Magerit, identificación de activos, con el siguiente anexo:

- Anexo A. Activos de información clasificados por confidencialidad, integridad y disponibilidad.

4.4 IDENTIFICACIÓN DE AMENAZAS Y PROBABILIDAD

Dando continuidad al plan de trabajo y la metodología Magerit se procedió con la segunda fase donde se identifican las amenazas que pueden llegar a afectar los activos, pero para esto es necesario clasificar su nivel de probabilidad (NP) es por esto que se construyó una escala para clasificar la probabilidad de ocurrencia apoyada en incidentes antes ocurridos en la EPS.

La tabla 6 muestra los niveles de probabilidad de ocurrencia de la amenaza, definidos por la EPS.

Tabla 6. Escala de probabilidad de ocurrencia

Nivel	Descripción de probabilidad
1	Improbable y no se tiene evidencia de que ha ocurrido
2	Probable que se produzca una vez cada dos años
3	Probable que se produzca una vez cada trimestre

Fuente: autores

Se realiza la identificación de amenazas, se estable un código para las mismas y se clasifican de acuerdo a la probabilidad de ocurrencia, para ello fue necesario realizar una evaluación lógica y física de las instalaciones del edificio de la EPS e instalaciones del proveedor, tanto a nivel general como a nivel de centro de datos.

Por lo tanto se gestionaron los debidos permisos para ingresar a las instalaciones y acuerdos de confidencialidad necesarios para obtener acceso a la información.

Después de realizadas las debidas visitas y reuniones con la EPS se establecen las amenazas que se van a considerar para el presente proyecto de grado; y con el desarrollo de la siguiente fase se verificaron los controles que se tienen para los mismos y la efectividad que estos tienen de acuerdo al activo vs la amenaza.

El cuadro 4 codifica y describe las amenazas consideradas y aprobadas por la EPS. Además se incluye el nivel de probabilidad (NP) y su razón de calificación.

Cuadro 4. Amenazas identificadas

	Amenaza	Descripción	NP	Razón de la calificación
A1	Fuego	Un incendio puede dejar una parte o la totalidad de las instalaciones inservibles.	1	El edificio es antiguo y no cuenta con los controles de seguridad para incendios, no se tiene evidencia de eventos de incendio
A2	Desastres Naturales	Terremotos, rayos, inundaciones, cambios en la temperatura y humedad, de impacto considerable que puedan afectar las operaciones de la Entidad.	1	La zona es de bajo riesgo frente a los eventos mencionados y no se tiene registro de ocurrencia en los últimos 3 años
A3	Intrusión en la red y ataques de ingeniería social	Intrusos en la red, hace referencia a la actividad de ingresar en un sistema ya sea un ordenador o a la red con una intención maliciosa para robar o dañar la información, y obstaculizar el buen funcionamiento de las operaciones de la Entidad. Los intrusos en la red pueden ser externos o internos. Incluso una intrusión no intencional en la red de la Entidad podría ser denominada como intrusos, ya que expone la vulnerabilidad de los sistemas de defensa de Entidad. Se considera dentro de esta categoría, los ataques de virus, intentos de hackers y ataques de denegación de servicio. Así mismo los ataques de Spam y de ingeniería social.	3	Se han presentado eventos de seguridad y se tiene evidencia de ataques en la EPS.
A4	Daños por agua	Fugas de agua o inundaciones, debido a filtraciones de agua a través de grietas en las paredes / techos, ventanas rotas, tuberías de agua rotas, etc., generado por factores como construcciones defectuosas, tuberías dañadas, desgaste e inadecuado mantenimiento.	1	El edificio es antiguo pero cuenta con los controles de seguridad para daños por agua, no se tiene evidencia de eventos de inundación.
A5	Robo y sabotaje	Retiro de activos de la Entidad no autorizados se considera como robo. Los activos de información se pueden clasificar para este caso en las siguientes categorías: hardware, software, documentos físicos y propiedad intelectual (Propiedad intelectual hace referencia a software de la EPS).	3	Se han presentado el robo de equipos, y existe un nivel de riesgo frente a los activos de la EPS
A6	Mal uso del software	El uso de software no autorizado y sin licencia en los sistemas de la entidad, ya sea por los administradores, funcionarios o contratistas de la EPS, serán considerados como mal uso del software.	2	No se han presentado eventos, sin embargo existe alta probabilidad de que ocurran.

	Amenaza	Descripción	NP	Razón de la calificación
A7	Fallas en infraestructura y en las redes	Fallas en los equipos de infraestructura y en las redes afectando la disponibilidad de los servicios de la EPS y la comunicación con otras sedes y entidades.	3	Se han presentado eventos que han afectado la infraestructura, como caídas de sistemas e infraestructura, debido a fallas de los proveedores.
A8	Errores humanos	Los errores humanos pueden ser causados por negligencia o falta de información/conocimiento por parte del personal de la EPS, causando una interrupción de las actividades normales de trabajo.	2	No se han presentado eventos, sin embargo existe la probabilidad de que ocurran.
A9	Terrorismo	Un ataque terrorista podría afectar la disponibilidad de las actividades de la EPS.	1	No se tiene evidencia que haya ocurrido.
A10	Amenazas legales	Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la EPS.	3	Las entidades del estado o mixtas constantemente se ven impactadas por nueva normatividad o nuevos decretos, los cuales afectan directamente a la EPS.

Fuente: autores

Con el siguiente anexo se da por cerrada la segunda fase, identificación de amenazas:

- Anexo B. Amenazas clasificadas por su tipo y su nivel de probabilidad.

Impacto Potencial. Posteriormente se procede a verificar y calificar el nivel de eficacia del control, pero antes de construir dicha matriz, se realizó una reunión con los directivos de la EPS, donde se expusieron los activos con sus diferentes amenazas, con su impacto potencial y riesgo potencial, es decir el impacto que se podría generar en caso de materializarse alguna de las amenazas antes mencionadas, y a su vez excluyendo los controles que se tienen, esto con el fin de que las directivas de la EPS tengan una visión de sus riesgos antes de los controles es decir sus riesgos potenciales. La matriz en cuestión se encuentra en el siguiente anexo:

- Anexo C. Matriz de impacto potencial y riesgo potencial.

En este anexo también se incluye una escala donde se dio un valor al impacto causado por la materialización de alguna de las amenazas. Para la realización de esta escala se tuvo en cuenta el nivel de impacto en 4 aspectos:

Impacto de confidencialidad en la información. Hace referencia a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la

información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad[7].

Impacto de credibilidad o imagen. El impacto de credibilidad se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la entidad[8].

Impacto legal. El impacto legal se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable[9].

Impacto operativo. El impacto operativo aplica en la mayoría de las entidades para los procesos clasificados como de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos[10].

La tabla 7 muestra el valor cuantitativo y cualitativo del impacto en caso de que la amenaza se materialice.

Tabla 7. Escala de impacto

Valor	Descriptor	Descripción del impacto
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Fuente: autores

Riesgo Potencial. Además de las consideraciones para establecer el impacto, también es necesario establecer unas zonas de riesgo, las cuales se detallan en un mapa de calor, y con las cuales la EPS deberá tomar las medidas necesarias para salvaguardar los activos involucrados.

[7] DAFP. Guía de administración de riesgos. 4 ed. Bogotá D.C., 2011. p. 29.
[8] Ibid., p. 29.
[9] Ibid., p. 29.
[10] Ibid., p. 30.

En el cuadro 5 se observa el mapa de calor, en el cual las zonas de riesgo derivan del producto de los valores de impacto y probabilidad.

Cuadro 5. Mapa de Calor - Zonas de riesgo

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
1	B (1)	B (2)	B (3)	B (4)	M (5)
2	B (2)	B (4)	M (6)	A (8)	E (10)
3	B (3)	M (6)	A (9)	E (12)	E (15)
	B: Zona de riesgo baja: Asumir el riesgo. (1-4)				
	M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo. (5-7)				
	A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir. (8-9)				
	E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir. (10-15)				

Fuente: autores

Teniendo la escala de impacto y el mapa de calor construido, se comunica a los directivos de la EPS y se presenta un informe del conteo de amenazas por cada una de las zonas de riesgo.

El cuadro 6 presenta un resumen en cifras de cuantas veces una amenaza se ve involucrada en cada una de las zonas de riesgos, según el tipo de activo.

Cuadro 6. Número de amenazas por zona de riesgo y tipo de activo

Zona de riesgo	Hardware	Información	Software	Total general
Zona B	2	1	1	4
Amenazas legales	1	0	0	1
Desastres Naturales	1	0	0	1
Terrorismo	0	1	1	2
Zona M	4	4	4	12
Daños por agua	1	1	1	3
Desastres Naturales	0	1	1	2
Errores humanos	1	1	1	3
Fuego	1	1	1	3
Terrorismo	1	0	0	1
Zona A	2	1	2	5
Fallas en infraestructura y en las redes.	1	0	1	2

Zona de riesgo	Hardware	Información	Software	Total general
Mal uso del software	1	1	1	3
Zona E	2	4	3	9
Amenazas legales	0	1	1	2
Fallas en infraestructura y en las redes.	0	1	0	1
Intrusión en la red y ataques de ingeniería social	1	1	1	3
Robo y sabotaje	1	1	1	3
Total general	10	10	10	30

Fuente: autores

Para obtener un mayor nivel de detalle acerca del mapa de calor e impacto potencial, remitirse al Anexo C.

4.5 SALVAGUARDAS O CONTROLES EXISTENTES

Con esta visión preliminar del impacto potencial y los riesgos potenciales, se procedió a verificar los controles que se tienen activos por cada amenaza y que a su vez custodian los activos antes inventariados, para lo cual se creó una matriz por cada amenaza. Dicha matriz se presentó ante el comité SGI de la EPS y fue aprobada por el mismo.

La tabla 8 muestra la escala para determinar el nivel de efectividad de los controles identificados.

Tabla 8. Escala de efectividad del control

Nivel	Descripción de la efectividad del control
3	Control está garantizado para funcionar eficazmente en cada caso de ocurrencia de la amenaza.
2	El control es parcialmente eficaz y podría funcionar la mayor parte del tiempo en el caso de que se produzca una amenaza.
1	El control es probable que falle en todos los casos de ocurrencia de la amenaza o No existe un control para mitigar esta amenaza.

Fuente autores

Posteriormente se realizó un análisis de la situación de los activos frente a sus controles la cual se puede encontrar en el siguiente anexo:

- Anexo D. Controles implementados según el activo, la amenaza y su nivel de efectividad.

Para la identificación de estos controles se tomaron como referencia los controles de la norma **ISO/IEC 27002:2013**, los controles facilitados por la EPS los cuales están alineados a la norma **ISO/IEC 17799:2007** y los elementos descritos por la metodología Magerit. Se analizaron los controles y el estado actual del mismo, por otra parte los controles se clasificaron de acuerdo a la metodología Magerit libro I, al igual se incluyen comentarios, los cuales fueron formalizados con el comité creado para la seguridad de la información.

4.6 IMPACTO RESIDUAL

Luego de verificar los controles o salvaguardas existentes en la EPS, se obtiene el impacto residual, dejando al descubierto que se tienen controles ineficientes o se carecen de ellos para proteger un determinado activo. Es decir que en caso de materializarse la amenaza, el impacto seguirá siendo perjudicial para la EPS.

Para calcular el impacto residual, se tomaron los valores de impacto potencial sobre la eficacia del control.

En la tabla 9 se muestra un ejemplo para calcular el impacto residual, para el tipo de amenaza ‘desastres naturales’. En donde el impacto residual es “1,7”, resultado de dividir el valor de impacto potencial (5) entre la eficacia del control (3).

Tabla 9. Ejemplo de cálculo de impacto residual

Tipo de activo	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Impacto potencial	Impacto residual
Hardware	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un área propensa a inundaciones.	Minimizadoras	SI	3	5	1,7

Fuente: autores

Se observa que el impacto potencial para el tipo de activo hardware tiene un valor de “5” es decir un impacto catastrófico para la EPS, sin embargo después de verificar la implementación y eficacia del control el impacto pasa de potencial a residual con un valor de “1,7”.

El ejercicio anterior se realizó con todos los tipos de activos y por cada amenaza, dando como resultado la matriz que se encuentra en el anexo E.

- Anexo E. Matriz de impacto residual y riesgo residual.

4.7 RIESGO RESIDUAL

El paso final del análisis es la identificación del riesgo residual, para calcularlo se tomó el valor del impacto residual por el nivel de probabilidad de ocurrencia. Para explicar el riesgo residual se continúa con el ejemplo que se propuso en el paso 4.6 impacto residual.

La tabla 10 da continuación al ejemplo propuesto en la tabla 9 y muestra cómo se calcula el riesgo residual y su respectiva ubicación en una zona de riesgo. El riesgo residual es “1,7”, resultado del producto del impacto residual (1,7) por el nivel de probabilidad (1).

Tabla 10. Ejemplo de cálculo de riesgo residual

Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
3	5	1,7	1	1,7	B

Fuente: autores

Se observa que el valor de riesgo residual es de “1,7”, resultado del producto entre el valor de nivel de probabilidad e impacto residual. Posteriormente y de la misma forma que se ubicaron los riesgos potenciales en el mapa de calor, se hace con el

riesgo residual. Para el caso del ejemplo anterior se ubica en una zona de riesgo residual “B” o baja.

El procedimiento anterior se realizó para todos los tipos de activos y se incluyó en el anexo E.

4.8 GESTIÓN DEL RIESGO

4.8.1 Comunicación del riesgo y recomendaciones. Una vez terminada la etapa de análisis de riesgos, los resultados de la situación actual de la EPS se presentaron a los directivos con el fin de que sean ellos los que determinen que acciones emprender en cuanto a los riesgos encontrados.

Por parte del comité SGI se recomienda a los directivos las diferentes medidas de tratamiento del riesgo con base en la metodología Magerit:

Para los riesgos ubicados en las zonas baja (B) y media (M), se recomienda aceptarlos, siempre y cuando exista una monitorización continua de los mismos. Además se deben revisar periódicamente los niveles de impacto y probabilidad ya que los riesgos se pueden tornar cambiantes.

Para los riesgos ubicados en las zonas alta (A) y extrema (E), se recomienda que se lleve a cabo un tratamiento de inmediato. Las opciones de tratamiento que se sugieren son:

- Eliminación: consiste en suprimir uno o varios elementos que intervienen en el riesgo siempre y cuando se empleen otros en su reemplazo y no se afecte el correcto funcionamiento de la EPS.

- Mitigación: consiste en implementar nuevos controles o aumentar la madurez del control existente y por ende la efectividad del mismo, con el objetivo de reducir el impacto o reducir la probabilidad de ocurrencia.

- Compartición: hace referencia a la transferencia del riesgo, ya sea parcial o total se puede dar de dos formas: la primera, es tercerizar los servicios o componentes en riesgo, acordando niveles de servicio que garanticen la operatividad de los mismos. La segunda es directamente con una aseguradora, la cual por medio de una cuantía monetaria se hace responsable de las consecuencias a causa de la materialización del riesgo.

- Financiación: consiste en un ahorro o ‘fondo de contingencia’ que la EPS aprovisiona para responder a las consecuencias a causa de la materialización del riesgo.

Respuesta y decisión de los directivos de la EPS. Las directivas comunicaron que se acogerán a las sugerencias dadas por el comité SGI. Para los riesgos ubicados en las zonas baja (B) y media (M) los aceptarán y no tomarán acciones inmediatas para los mismos, sin embargo harán un monitoreo constante.

Para los riesgos ubicados en las zonas alta (A) y extrema (E), las directivas han decidido iniciar un plan de tratamiento de riesgos priorizando los que se encuentran en la zona de riesgo extrema (E).

El cuadro 7 presenta un resumen de la cantidad de riesgos en las zonas alta y extrema, agrupados por tipo de amenaza.

Cuadro 7. Número de riesgos en zona alta y extrema

Amenaza	Zona de riesgo	
	Alta	Extrema
Intrusión en la red	44	29
Robo y sabotaje	60	47
Mal uso del software	7	0
Fallas en infraestructura y redes	6	0
Legal	0	6
Total	117	82

Fuente: autores

4.8.2 Tratamiento de riesgos. Los directivos de la EPS, determinaron que el plan de tratamiento de riesgos se iniciara a nivel interno y por lo tanto no se harán participes a los estudiantes que desarrollaron el presente proyecto de grado. Mas sin embargo toda las matrices y el análisis de los riesgos serán el punto de partida y el insumo para el desarrollo del plan de gestión de riesgos.

5. CONCLUSIONES

- Se cumplió con el objetivo principal y los objetivos específicos, donde la EPS ahora es consciente de sus riesgos, amenazas, vulnerabilidades y el impacto que podría causar el no atenderlas. A su vez se obtiene una herramienta metodológica para la identificación de estos elementos.

- La EPS podrá, si así lo desea, continuar con la metodología MAGERIT aplicada en este proyecto para la elaboración e implementación de un plan de gestión de riesgos que contemplará las actividades posteriores al análisis, como el tratamiento, comunicación, seguimiento y revisión.

- Se puede asegurar que el análisis de riesgos permitió determinar a qué riesgos está expuesta la EPS y estimar el nivel de impacto en caso de materializarse. Este análisis también permitió implementar una metodología para el levantamiento de activos, identificación de amenazas y efectividad de controles implementados.

- Con el análisis de riesgos desarrollado en este proyecto, la EPS podrá emprender un plan de tratamiento de riesgos que le permitirá afrontar su defensa organizacional de manera más concienzuda y prudente, previniendo sucesos o situaciones perjudiciales y al mismo tiempo prepararse para evitar desastres en el centro de datos, así como lograr generar un plan de recuperación de desastres.

- Dentro del presente análisis de riesgos se clasificaron los activos de acuerdo a los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad, permitiendo que el dueño del activo o de proceso reconociera el valor y la importancia real que tiene para la organización.

- Una de las principales dificultades que se presentó en el desarrollo de este proyecto fue lograr un espacio de tiempo con los propietarios de los activos y/o dueños de proceso, esto a pesar de contar con el aval y la autorización de los directivos de la EPS. Finalmente luego de superar esta y otras dificultades en el desarrollo del proyecto se logró completar las actividades que conllevan el análisis de riesgos de seguridad de la información.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ; NORMAS. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, 1712 DE 2014. [en línea], [consultado en Junio de 2015], disponible en: http://www.alcaldiabogota.gov.co/sisjur /normas/Norma1.jsp?i=56882

_____. Normas para el manejo de la Historia Clínica, Resolución 1995 DE 1999. [en línea], [consultado en Junio de 2015], disponible en: http://www. alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=16737

_____. Disposiciones generales para la protección de datos personales, ley Estatutaria No.1581 de 2012. [en línea], [consultado en Junio de 2015], disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

DAFP. Guía de administración de riesgos. 4 ed. Bogotá D.C., 2011

ESCUELA POLITÉCNICA NACIONAL; REPOSITORIO DIGITAL EPN. Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctrica Quito S.A., 2011. [en línea], [consultado en Febrero de 2015], disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Sistemas de gestión de la seguridad de la información. Primera actualización. Bogotá D.C.: ICONTEC, 2013. NTC ISO/IEC 27001.

_____. Código de prácticas para controles de seguridad de la información. Primera actualización. Bogotá D.C.: ICONTEC, 2013. NTC ISO/IEC 27002.

_____. Código de práctica para la gestión de la seguridad de la información. Primera actualización. Bogotá D.C.: ICONTEC, 2007. NTC ISO/IEC 17799.

_____. Gestión de riesgos de la seguridad la información. Primera actualización. Bogotá D.C.: ICONTEC, 2008. NTC ISO/IEC 27005.

ISACA; CSIM. Manual de certificación CISM 2012. [en línea] [consultado en Febrero de 2015.], disponible en: http://www.isaca.org/chapters7/Madrid/Events/Formacion/Pages/Curso-de-preparacion-CISM.aspx

MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.], disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#Vlo6huKLOW4

SECUREIT INFORMATION TECHNOLOGIES. ¿Qué es vulnerabilidad?. [en línea], [consultado el 23 de marzo de 2015], disponible en: http://secureit.com.mx/gestion-de-riesgos/

_____. ¿Qué es Amenaza?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://secureit.com.mx/gestion-de-riesgos/

_____. ¿Qué es gestión de riesgos?. [en línea], [consultado el 23 de marzo de 2015]. Disponible en: http://secureit.com.mx/gestion-de-riesgos/

ANEXOS

Anexo A. Activos de información clasificados por confidencialidad, integridad y disponibilidad

Anexo A.1 Activos de información tipo hardware

Información del activo								Información proceso / actividad		Clasificación de activos de información			
Ítem	**Tipo de activo**	**Nombre de activo**	**Sistema operativo (si aplica)/ versión software**	**Dirección IP (si aplica)**	**Propietario del activo**	**Custodio del activo/ nombre propietario**	**Localización**	**Proceso**	**Responsable del proceso**	**C**	**I**	**D**	**Valor final**
1	Servidor	Server 1	Windows 2003	192.168.1.12	Director de tecnología	Tecnología - director TI	Datacenter principal	Gestión documental	Director gestión documental	2	2	1	2
2	Servidor	Srvandje	Windows server 2012	192.168.10.1	Director de tecnología	Tecnología - director TI	Datacenter principal	Directorio activo	Director de tecnología	2	2	2	2
3	Servidor	Srvandje01	Windows server 2012	192.168.10.101	Director de tecnología	Tecnología - director TI	Datacenter principal	virtualización de maquinas	Director de tecnología	2	2	2	2
4	Servidor	Srvandje02	Windows server 2012	192.168.10.102	Director de tecnología	Tecnología - director TI	Datacenter principal	virtualización de maquinas	Director de tecnología	2	2	2	2
5	Servidor	Srvandje03	Windows server 2012	192.168.10.103	Director de tecnología	Tecnología - director TI	Datacenter principal	virtualización de maquinas	Director de tecnología	2	2	2	2
6	Servidor	Srvstorage	Windows server 2012	192.168.10.15	Director de tecnología	Tecnología - director TI	Datacenter principal	Servidor de almacenamiento de información de la EPS	Director de tecnología	2	2	2	2
7	Servidor/ appliance	Audicodes/sba	Windows server 2012	192.168.10.9	Director de tecnología	Tecnología - director TI	Datacenter principal	Servicio de telefonía	Director de tecnología	2	2	2	2
8	Conmutador	Switch	Cisco	10.10.10.1	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
9	Conmutador	Switch	Cisco	10.10.10.2	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
10	Conmutador	Switch	Cisco	10.10.10.3	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
11	Conmutador	Switch	Cisco	10.10.10.4	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
12	Conmutador	Switch	Cisco	10.10.10.5	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
13	Conmutador	Switch	Cisco	10.10.10.6	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
14	Conmutador	Switch	Cisco	10.10.10.7	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
15	Conmutador	Switch	Cisco	10.10.10.8	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
16	Conmutador	Switch	Cisco	10.10.10.9	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
17	Conmutador	Switch	Cisco	10.10.10.10	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
18	Conmutador	Switch	Cisco	10.10.10.11	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
19	Conmutador	Switch	Cisco	10.10.10.12	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
20	Conmutador	Switch	Cisco	10.10.10.13	Director de tecnología	Coordinador de telecomunicaciones	Datacenter principal	Dispositivo de interconexión de redes	Director de tecnología	2	1	2	2
21	Switch	Switchs brokade	Brokade		Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	3	3	3	3
22	Switch	Switchs brokade	Brokade		Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	3	3	3	3

Anexo A.1 (Continuación)

Información del activo								Información proceso / actividad		Clasificación de activos de información			
Ítem	Tipo de activo	Nombre de activo	Sistema operativo (si aplica)/ versión software	Dirección IP (si aplica)	Propietario del activo	Custodio del activo/ nombre propietario	Localización	Proceso	Responsable del proceso	C	I	D	Valor final
23	Servidor	Hc especialistas aplicación	Windows server 2012 standard x64	192.168.90.21	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	3	3	3	3
24	Servidor	Hc especialistas base de datos	Windows server 2012 standard x64	192.168.90.22	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	3	3	3	3
25	Servidor	Hc especialistas aplicación - pruebas	Windows server 2012 standard x64	192.168.90.15	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	3	1	1	3
26	Servidor	Hc especialistas base de datos - pruebas	Windows server 2012 standard x64	192.168.90.19	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	3	1	1	3
27	Servidor	Transaccional aplicación	Windows server 2012 standard x64	192.168.80.11	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema transaccional de la EPS	Dirección de gestión de información	3	3	3	3
28	Servidor	Transaccional bd	Windows server 2012 standard x64	192.168.80.10	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema transaccional de la EPS	Dirección de gestión de información	3	3	3	3
29	Servidor	Mantis	Windows server 2012 standard x64	192.168.90.14	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema transaccional de la EPS	Dirección de gestión de información	2	2	3	3
30	Servidor	Portal hc especialistas	Windows server 2012 standard x64	192.168.90.18	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	1	2	2	2
31	Servidor	Poweredge - host1	N/a	192.168.99.10	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	2	3	3	3
32	Servidor	Poweredge - host2	N/a	192.168.99.11	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	2	3	3	3
33	Servidor	Poweredge - host3	N/a	192.168.99.12	Director de tecnología	Proveedor de comunicaciones	Datacenter alterno	Gestión del sistema único de información de historias clínicas	Dirección de gestión de información	2	3	3	3
34	Servidor	Calidad.eps.com.co	Windows server 2012	192.168.10.12	Director de tecnología	Director de tecnología	Datacenter principal	Oficina planeación	Oficina de planeación	1	1	2	2
35	Servidor	Intranet.eps.com.co, eps.com.co	Windows server 2012	192.168.10.20	Director de tecnología	Director de tecnología	Datacenter principal	Sistema de información - intranet	Director de tecnología	1	1	2	2
36	Servidor	Hc especialistas	Windows server 2012	192.168.10.21	Director de tecnología	Director de tecnología	Datacenter principal	Dgi	Ti gestión de la información	1	1	3	3
37	Servidor	Orfeo.eps.com.co	Centos 6.0	192.168.10.40	Director de tecnología	Director de tecnología	Datacenter principal	Secretaria general	Director de tecnología	1	1	3	3

Fuente: autores

Anexo A.2 Activos de información tipo software

Información del activo							Información proceso / actividad		Clasificación de activos de información			
Ítem	**Tipo de activo**	**Nombre de activo**	**Tipo de aplicación**	**Propietario del activo**	**Custodio del activo/ nombre propietario**	**Localización**	**Proceso**	**Responsable del proceso**	**C**	**I**	**D**	**Valor final**
1	Software	Sistema integrado de gestión institucional	Producción	Gestión de Tecnologías de Información	Gestión de Tecnologías de Información	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	2	2	2	2
2	Software	Office Professional	Ofimática	Secretaria General	Secretaria General	Nube	Paquete ofimático para la EPS	Secretaria General	2	1	1	2
3	Software	Core Infraestructura Server Suite Datacenter - 2 Proc	Windows Server Datacenter	Secretaria General	Secretaria General	Nube	Sistemas Operativo Windows Server	Secretaria General	2	1	1	2
4	Software	Lync Server	Comunicaciones Unificadas	Secretaria General	Secretaria General	Nube	Telefonía y Presencia	Secretaria General	2	1	1	2
5	Software	Lync Server Enterprise - Device CAL	Licenciamiento Lync Server 2013	Secretaria General	Secretaria General	Nube	Telefonía y Presencia	Secretaria General	2	1	1	2
6	Software	Lync Server Plus - Device CAL	Licenciamiento CAL Lync Server 2013 Device Plus	Secretaria General	Secretaria General	Nube	Telefonía y Presencia	Secretaria General	2	1	1	2
7	Software	Lync Server Standard - Device CAL	Licenciamiento CAL Lync Server 2013 Device Estándar	Secretaria General	Secretaria General	Nube	Telefonía y Presencia	Secretaria General	2	1	1	2
8	Software	SharePoint Server	Licenciamiento Plataforma Share Point	Secretaria General	Secretaria General	Nube	Telefonía y Presencia	Secretaria General	2	1	1	2
9	Software	SharePoint Server Standard CAL - Device CAL	Licenciamiento CAL Share Point Device CAL	Secretaria General	Secretaria General	Nube	Portal web intranet extranet	Secretaria General	2	1	1	2
10	Software	SQL Server Enterprise Core	Licenciamiento SQL Server	Secretaria General	Secretaria General	Nube	Herramienta de bases de Bases de Datos para: Gestión de Infraestructura Portal Web telefonía y presencia	Secretaria General	2	1	1	2
11	Software	System Center Configuration Manager Client ML	Licenciamiento Client System Center Configuration Manager	Secretaria General	Secretaria General	Nube	Gestión de Infraestructura	Secretaria General	2	1	1	2
12	Software	Windows Server - Device CAL	Licenciamiento CAL Windows Server	Secretaria General	Secretaria General	Nube	Sistemas Operativo Windows Server	Secretaria General	2	1	1	2
13	Software	Windows Server Storage	Licenciamiento Windows Server funcionalidad Storage	Secretaria General	Secretaria General	Nube	Sistemas Operativo Windows Server	Secretaria General	2	1	1	2
14	Software	Windows Server - Standard	Licenciamiento Windows Server funcionalidad Storage	Secretaria General	Secretaria General	Nube	Sistemas Operativo Windows Server	Secretaria General	2	1	1	2

Anexo A.2 (Continuación)

Información del activo							Información proceso / actividad		Clasificación de activos de información			
Ítem	**Tipo de activo**	**Nombre de activo**	**Tipo de aplicación**	**Propietario del activo**	**Custodio del activo/ nombre propietario**	**Localización**	**Proceso**	**Responsable del proceso**	**C**	**I**	**D**	**Valor final**
15	Software	Exchange Online Plan 1	Licenciamiento Online Plan Llamadas / Presencia	Secretaria General	Secretaria General	Nube	Correo Electrónico de la EPS	Secretaria General	2	1	1	2
16	Software	Exchange Online Plan 2 Open	Licenciamiento Online Plan Presencia	Secretaria General	Secretaria General	Nube	Correo Electrónico de la EPS con Telefonía	Secretaria General	2	1	1	2
17	Software	Project Professional	Licenciamiento Client Paquete Office Project	Secretaria General	Secretaria General	Nube	Paquete office de administración de proyectos	Secretaria General	2	1	1	2
18	Software	Visio Standard	Licenciamiento Paquete Office Visio	Secretaria General	Secretaria General	Nube	Paquete office de dibujo vectorial para Microsoft Windows	Secretaria General	2	1	1	2
19	Software	Project Server - Device CAL	Licenciamiento Server Paquete Office Project	Secretaria General	Secretaria General	Nube	Software de administración de proyectos	Secretaria General	2	1	1	2
20	Software	SQL Server Enterprise	Licenciamiento Bases de Datos SQL Server	Secretaria General	Secretaria General	Nube	Herramienta de bases de Bases de Datos para: Gestión de Infraestructura Portal Web telefonía y presencia	Secretaria General	2	1	1	2
21	Software	SQL Server Enterprise Core	Licenciamiento Core Bases de Datos SQL Server	Secretaria General	Secretaria General	Nube	Herramienta de bases de Bases de Datos para: Gestión de Infraestructura Portal Web telefonía y presencia	Secretaria General	2	1	1	2
22	Software	System Center Endpoint Protection	Licenciamiento CAL System Center End Point Protection	Secretaria General	Secretaria General	Nube	Gestión de administración para protección antivirus	Secretaria General	2	1	1	2
23	Software	Acrobat	Licenciamiento Acrobat Standard	Secretaria General	Secretaria General	Puesto de Trabajo (Equipo)	Sistemas diseñados para visualizar, crear y modificar archivos	Secretaria General	2	1	1	2
24	Software	SAS	Licenciamiento SAS	Secretaria General	Secretaria General	Puesto de Trabajo (Equipo)	software especializado en estadísticas sobre el sistema de Historias Clínicas	Dirección de Gestión de Información	2	1	1	2
25	Software	Eagle Ware	Licenciamiento Eagle Control	Secretaria General	Secretaria General	Puesto de Trabajo (Equipo)	Sistema de administración Telefónica	Secretaria General	2	1	1	2
26	Software	ITS- GESTIÓN	Licenciamiento ITS GESTION	Secretaria General	Secretaria General	Puesto de Trabajo (Equipo)	Sistema de gestión de calidad	Planeación	2	1	1	2
27	Software	Fuentes de HC Especialistas	Producción	Dirección de Gestión de Información	Datacenter Alterno	Gestión del Sistema Único de Información HC Especialistas	Gestión del Sistema Único de Información HC Especialistas	Dirección de Gestión de Información	2	3	3	3
28	Software	Fuentes de Transaccional	Producción	Dirección de Gestión de Información	Datacenter Alterno	Gestión del Sistema Único de Información HC Especialistas	Gestión del Sistema Único de Información HC Especialistas	Dirección de Gestión de Información	2	3	3	3
29	Software	SAS (Paquete Estadístico)	Estadística	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información HC Especialistas	Dirección de Gestión de Información	2	2	1	2

Fuente: autores

Anexo A.3 Activos de información tipo Información

Información activo de información							Información proceso / actividad		Clasificación de activos de información			
ítem	**Tipo de activo**	**Información física / digital**	**Nombre de activo**	**Contenedor**	**Propietario del activo**	**Custodio del activo/ nombre propietario**	**Proceso**	**Dueño del proceso**	**C**	**I**	**D**	**Valor final**
1	Documento	Digital	Guías	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Oficina Asesora de Planeación	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
2	Documento	Digital	Indicadores de Gestión y de Producto	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
3	Documento	Digital	Informe de Gestión	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
4	Documento	Digital	Informe Rendición de Cuentas	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
5	Documento	Digital	Informe de seguimiento a la Gestión Institucional	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
6	Documento	Digital	Plan de Acción Anual	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
7	Documento	Digital	Plan de Acción Cuatrienal	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
8	Documento	Digital	Política de Desarrollo Administrativo	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
9	Documento	Digital	Protocolos	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
10	Documento	Digital	Seguimiento a Planes	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
11	Documento	Digital	Seguimiento a Planes de inversión	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
12	Documento	Digital	Informe de Gestión	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Gestión con grupos de Interés	Dirección General	1	1	1	1
13	Documento	Digital	Informe entes de control	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Gestión con grupos de Interés	Dirección General	1	1	1	1
14	Documento	Digital	Matriz estratégica-DE-F-22	Aplicativo SIGI o página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
15	Documento	Digital	Plan estratégico cuatrienal Aprobado	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
16	Documento	Digital	Plan de Acción Institucional-DE-F-21	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
17	Documento	Digital	Planes Operativos Anuales-DE-F-19	Sistema Integrado de Gestión Institucional	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
18	Documento	Digital	Proyectos de inversión actualizados y/o formulados	Sistema Integrado de Gestión Institucional, página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1

Anexo A.3 (Continuación)

Información activo de información							Información proceso / actividad		Clasificación de activos de información			
ítem	**Tipo de activo**	**Información física / digital**	**Nombre de activo**	**Contenedor**	**Propietario del activo**	**Custodio del activo/ nombre propietario**	**Proceso**	**Dueño del proceso**	**C**	**I**	**D**	**Valor final**
19	Documento	Digital	Plan Estratégico Cuatrienal aprobado	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
20	Documento	Digital	Formato Informe trimestral avances Plan Operativo Anual-DE-F-19	Sistema Integrado de Gestión Institucional, Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
21	Documento	Digital	Formato Solicitud a ajuste a Plan de Acción Anual-DE-F-07	Sistema Integrado de Gestión Institucional, página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Direccionamiento Estratégico	Oficina Asesora de Planeación	1	1	1	1
22	Documento	Digital	Planeación, seguimiento e informes	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	2	2	2	2
23	Documento	Digital	Conciliación - soportes	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	2	2	2	2
24	Documento	Digital	Conciliación - Productos finales	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	1	2	2	2
25	Documento	Digital	Estudios empíricos - Soportes	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	2	2	2	2
26	Documento	Digital	Estudios empíricos - Productos Finales	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	1	2	2	2
27	Documento	Digital	Estudios jurisprudenciales - Soportes	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	2	2	2	2
28	Documento	Digital	Estudios jurisprudenciales- Productos Finales	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	1	2	2	2
29	Documento	Digital	Guías metodológicas- Soportes	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	2	2	2	2
30	Documento	Digital	Guías metodológicas - Productos Finales	Carpeta pública dirección de políticas y estrategias en servidor de Archivos	Dirección de Políticas y Estrategias	Oficina de sistemas	Gestión de Prevención del Daño Antijurídico Gestión del conflicto jurídico	Dirección de Políticas y Estrategias	1	2	2	2
31	Documento	Digital	Actas de eliminación de Documentos	Sistema de Gestión Documental Orfeo	Secretaria General, Gestión Documental	Gestión de Tecnologías de Información	Gestión Documental	Gestión Documental	1	1	1	1

Anexo A.3 (Continuación)

Información activo de información							Información proceso / actividad		Clasificación de activos de información			
ítem	**Tipo de activo**	**Información física / digital**	**Nombre de activo**	**Contenedor**	**Propietario del activo**	**Custodio del activo/ nombre propietario**	**Proceso**	**Dueño del proceso**	**C**	**I**	**D**	**Valor final**
32	Documento	Digital	Actas de anulación del Consecutivo General de Comunicaciones	Sistema de Gestión Documental Orfeo	Secretaria General, Gestión Documental	Gestión de Tecnologías de Información	Gestión Documental	Gestión Documental	1	1	1	1
33	Documento	Digital	Consecutivo General de Comunicaciones	Sistema de Gestión Documental Orfeo	Secretaria General, Gestión Documental	Gestión de Tecnologías de Información	Gestión Documental	Gestión Documental	3	3	3	3
34	Sistema de Gestión Documental	Digital	Información Personal registrada en el Sistema de Gestión Documental	Sistema de Gestión Documental Orfeo	Secretaria General, Gestión Documental	Gestión de Tecnologías de Información	Gestión Documental	Gestión Documental	3	3	3	3
35	Documento	Digital	Informe de Gestión	Página web	Oficina Asesora de Planeación	Gestión de Tecnologías de Información	Mejora Continua	Oficina Asesora de Planeación	1	1	1	1
36	Documento	Digital	Reportes de información del Sistema	File server de DGI, Correo electrónico, computadores del grupo de validación	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3
37	Documento	Digital	Piezas procesales	Correo electrónico, File server de DGI	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	2	2	3	3
38	Documento	Digital	Información de Gestión de la Dirección	Google Drive (asesores), DropBox, Equipos de la DGI	Dirección de Gestión de Información	PROVEEDORES EXTERNOS GOOGLE Y DROPBOX	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3
39	Documento	Digital	INFORMACIÓN SCANEADA EN LA DGI	FILE SERVER DGI/ SCANDGI	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	2	1	3
40	Documento	Digital	Bases diarias de procesos judiciales y extrajudiciales	SERVIDORES HC Especialistas / Equipos de la DGI	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3
41	Base de datos	Digital	Información de procesos Judiciales ya gestionados en el Sistema Transaccional	SERVIDORES HC Especialistas	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3
42	Base de datos	Digital	Solicitudes de Conciliación ya gestionados en el Sistema Transaccional	SERVIDORES HC Especialistas	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3
43	Base de datos	Digital	Acciones de Tutela ya gestionados en el Sistema Transaccional	SERVIDORES HC Especialistas	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3
44	Base de datos	Digital	Trámites Arbitrales ya relacionados en base de datos	SERVIDORES HC Especialistas	Dirección de Gestión de Información	Gestión de Tecnologías de Información	Gestión del Sistema Único de Información de Historias Clínicas	Dirección de Gestión de Información	3	3	3	3

Fuente: autores

Anexo B. Amenazas clasificadas por su tipo y su nivel de probabilidad

	Amenaza	Descripción	NP	Razón de la calificación
A1	Fuego	Un incendio puede dejar una parte o la totalidad de las instalaciones inservibles.	1	El edificio es antiguo y no cuenta con los controles de seguridad para incendios, no se tiene evidencia de eventos de incendio
A2	Desastres Naturales	Terremotos, rayos, inundaciones, cambios en la temperatura y humedad, de impacto considerable que puedan afectar las operaciones de la Entidad.	1	La zona es de bajo riesgo frente a los eventos mencionados y no se tiene registro de ocurrencia en los últimos 3 años.
A3	Intrusión en la red y ataques de ingeniería social	Intrusos en la red, hace referencia a la actividad de ingresar en un sistema ya sea un ordenador o a la red con una intención maliciosa para robar o dañar la información, y obstaculizar el buen funcionamiento de las operaciones de la Entidad. Los intrusos en la red pueden ser externos o internos. Incluso una intrusión no intencional en la red de la Entidad podría ser denominada como intrusos, ya que expone la vulnerabilidad de los sistemas de defensa de Entidad. Se considera dentro de esta categoría, los ataques de virus, intentos de hackers y ataques de denegación de servicio. Así mismo los ataques de Spam y de ingeniería social.	3	Se han presentado eventos de seguridad y se tiene evidencia de ataques en la EPS.
A4	Daños por agua	Fugas de agua o inundaciones, debido a filtraciones de agua a través de grietas en las paredes / techos, ventanas rotas, tuberías de agua rotas, etc., generado por factores como construcciones defectuosas, tuberías dañadas, desgaste e inadecuado mantenimiento.	1	El edificio es antiguo pero cuenta con los controles de seguridad para daños por agua, no se tiene evidencia de eventos de inundación.
A5	Robo y sabotaje	Retiro de activos de la Entidad no autorizados se considera como robo. Los activos de información se pueden clasificar para este caso en las siguientes categorías: hardware, software, documentos físicos y propiedad intelectual (Propiedad intelectual hace referencia a software de la EPS).	3	Se han presentado el robo de equipos, y existe un nivel de riesgo frente a los activos de la EPS
A6	Mal uso del software	El uso de software no autorizado y sin licencia en los sistemas de la entidad, ya sea por los administradores, funcionarios o contratistas de la EPS, serán considerados como mal uso del software.	2	No se han presentado eventos, sin embargo existe alta probabilidad de que ocurran.
A7	Fallas en infraestructura y en las redes.	Fallas en los equipos de infraestructura y en las redes afectando la disponibilidad de los servicios de la EPS y la comunicación con otras sedes y entidades.	3	Se han presentado eventos que han afectado la infraestructura, como caídas de sistemas e infraestructura, debido a fallas de los proveedores.
A8	Errores humanos	Los errores humanos pueden ser causados por negligencia o falta de información/conocimiento por parte del personal de la EPS, causando una interrupción de las actividades normales de trabajo.	2	No se han presentado eventos, sin embargo existe la probabilidad de que ocurran.
A9	Terrorismo	Un ataque terrorista podría afectar la disponibilidad de las actividades de la EPS.	1	No se tiene evidencia que haya ocurrido.
A10	Amenazas legales	Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la EPS.	3	Las entidades del estado o mixtas constantemente se ven impactadas por nueva normatividad o nuevos decretos, los cuales afectan directamente a la EPS.

Fuente: autores

Anexo C. Matriz de impacto potencial y riesgo potencial

Anexo C.1 Impacto Potencial

Tipo de activo	Código amenaza	Amenaza	Impacto
Hardware	A1	Fuego	5
	A2	Desastres Naturales	4
	A3	Intrusión en la red y ataques de ingeniería social	5
	A4	Daños por agua	5
	A5	Robo y sabotaje	5
	A6	Mal uso del software	4
	A7	Fallas en infraestructura y en las redes	3
	A8	Errores humanos	3
	A9	Terrorismo	5
	A10	Amenazas legales	1
Software	A1	Fuego	5
	A2	Desastres Naturales	5
	A3	Intrusión en la red y ataques de ingeniería social	5
	A4	Daños por agua	5
	A5	Robo y sabotaje	5
	A6	Mal uso del software	4
	A7	Fallas en infraestructura y en las redes	3
	A8	Errores humanos	3
	A9	Terrorismo	2
	A10	Amenazas legales	4
Información	A1	Fuego	5
	A2	Desastres Naturales	5
	A3	Intrusión en la red y ataques de ingeniería social	5
	A4	Daños por agua	5
	A5	Robo y sabotaje	5
	A6	Mal uso del software	4
	A7	Fallas en infraestructura y en las redes	4
	A8	Errores humanos	3
	A9	Terrorismo	4
	A10	Amenazas legales	4

Fuente: autores

Anexo C.2 Riesgo potencial

Tipo de activo	Código amenaza	Amenaza	Impacto	Nivel de probabilidad	Riesgo potencial	Zona de riesgo
Hardware	A1	Fuego	5	1	5	M
	A2	Desastres Naturales	4	1	4	B
	A3	Intrusión en la red y ataques de ingeniería social	5	3	15	E
	A4	Daños por agua	5	1	5	M
	A5	Robo y sabotaje	5	3	15	E
	A6	Mal uso del software	4	2	8	A
	A7	Fallas en infraestructura y en las redes.	3	3	9	A
	A8	Errores humanos	3	2	6	M
	A9	Terrorismo	5	1	5	M
	A10	Amenazas legales	1	3	3	B
Software	A1	Fuego	5	1	5	M
	A2	Desastres Naturales	5	1	5	M
	A3	Intrusión en la red y ataques de ingeniería social	5	3	15	E
	A4	Daños por agua	5	1	5	M
	A5	Robo y sabotaje	5	3	15	E
	A6	Mal uso del software	4	2	8	A
	A7	Fallas en infraestructura y en las redes.	3	3	9	A
	A8	Errores humanos	3	2	6	M
	A9	Terrorismo	2	1	2	B
	A10	Amenazas legales	4	3	12	E
Información	A1	Fuego	5	1	5	M
	A2	Desastres Naturales	5	1	5	M
	A3	Intrusión en la red y ataques de ingeniería social	5	3	15	E
	A4	Daños por agua	5	1	5	M
	A5	Robo y sabotaje	5	3	15	E
	A6	Mal uso del software	4	2	8	A
	A7	Fallas en infraestructura y en las redes.	4	3	12	E
	A8	Errores humanos	3	2	6	M
	A9	Terrorismo	4	1	4	B
	A10	Amenazas legales	4	3	12	E

Fuente: autores

Anexo D. Controles implementados según el activo, la amenaza y su nivel de efectividad

Anexo D.1 Amenaza fuego

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, Información	Proximidad a plantas de producción de Petróleo, Gasolina y Químicos Inflamables Proximidad a áreas de alta combustión o áreas de almacenamiento de material inflamable	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de Petróleo, Gasolina y Químicos Inflamables.	Minimizadoras	SI	3	El datacenter principal y Alterno no se encuentra cerca de líquidos inflamables.
	Interiores construidos con material combustible. Equipos y circuitos eléctricos de baja calidad	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura.	Minimizadoras	SI	3	El datacenter se encuentra alejado de cualquier objeto que pueda generar cortos circuitos. Se encuentra herramientas contra incendios.
Hardware	Manejo inadecuado de cilindros de gas, etc.	Definir directrices para el manejo de cilindros de gas, etc.	Administrativas	SI	3	No se encuentra ningún cilindro inflamable cerca o dentro del datacenter.
Hardware, Software, Información.	Ausencia de un sistema de detección de incendios. Ausencia de equipo contra incendios. Se permite fumar dentro de las instalaciones Exteriores hechos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura. Establecer directrices para comer, beber y fumar en proximidad a las instalaciones de procesamiento de información.	Minimizadoras	PARCIAL	2	No existe sistema detección de incendios, se encuentra el cilindro contra incendios, no está documentado a nivel de datacenter. La edificación cuenta con mecanismos contra incendios.
	La falta de mecanismos alternos en caso de destrucción total por fuego.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	PARCIAL	2	Datacenter Alterno: por contrato se tiene establecido todo el plan de continuidad de negocio. Datacenter que se encuentra en el edificio: no cuenta con ningún plan de continuidad.
Hardware, Software, Información	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Recuperación	NO	1	Actualmente no existe un backup que se encuentre alojado en un lugar externo a la organización, pero están trabajando en el proyecto de implementación de backup en cintas en un lugar alterno.

Fuente: autores

Anexo D.2 Amenaza Desastres Naturales

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Información	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un área propensa a inundaciones.	Minimizadoras	SI	3	El datacenter de los sistemas de soporte se encuentran en una zona no riesgosa de inundaciones, al igual el datacenter alterno se encuentra en una zona con un grado bajo de inundaciones, éste cuenta con los controles como pisos elevados para prevenir inundaciones.
	Ausencia de pisos elevados.	Se debe implementar protección contra inundaciones.	Minimizadoras	SI	3	Los Datacenter están ubicados en pisos elevados para prevenir inundaciones, así mismo se cuenta con piso falso.
	Calidad baja en la construcción de los edificios.	La construcción del edificio debe ser resistente a fugas de agua.	Minimizadoras	SI	3	Los edificios cumplen con los requerimientos de construcción.
	Incapacidad para absorber rayos	Sistemas para rayos y sistemas de polo a tierra	Minimizadoras	SI	3	Los edificios cumplen con los requerimientos de construcción.
	Sistema de drenaje débil.	Se debe implementar protección en contra de inundaciones y fugas de agua.	Minimizadoras	SI	3	Se cuenta con sistemas de drenaje para los datacenter.
	Ausencia de control de temperatura y humedad adecuada	Sistema de monitoreo adecuado para temperatura y humedad	Monitorización	PARCIAL	2	A nivel del datacenter se tiene todos los controles de Nivel 3, a nivel del centro de datos se tienen controles temperatura a través de dos sistemas de aire, se está implementando el sensor de temperatura.
		Las condiciones ambientales, tales como temperatura y humedad, deben ser monitorizados para detectar condiciones anormales.	Monitorización	PARCIAL	2	A nivel del datacenter se tiene todos los controles de Nivel 3, a nivel del centro de datos se tienen controles temperatura a través de dos sistemas de aire, se está implementando el sensor de temperatura.
	Incapacidad para controlar la temperatura y la humedad dentro del centro de datos	Los equipos de control de humedad y temperatura deben mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Administrativas	PARCIAL	2	A nivel del datacenter Alterno se tienen contratos de soporte para los sistemas de humedad y temperatura que están a cargo del proveedor. A nivel del datacenter principal no cuenta con sensores de temperatura y humedad
Hardware	Incapacidad para controlar la entrada de humos venenosos / aire / humo a través de los conductos de aire	El manejo adecuado de apertura / cierre de los conductos de aire durante eventos como vientos fuertes, uso de pesticidas o fuego.	Administrativas	SI	3	Se tiene sistema de Aire independiente para el centro de datos Principal, el cual no es compartido con las instalaciones de EPS. El sistema de aire para el edificio es de refrigeración por lo tanto no se ve impactado por eventos externos.

Anexo D.2 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, Información.	Ubicado en una zona de alto nivel sísmico	Las instalaciones deben ubicarse en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	SI	3	El edificio es antiguo y no cuenta con los estándares de construcción anti-sísmica, por otra parte el datacenter de alterno cuenta con las medidas de protección sísmica.
	Estructura de la construcción y techos de baja calidad	La infraestructura debe ser resistente a terremotos si se encuentra ubicada en una zona de medio o alto nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	SI	3	El edificio es antiguo y no cuenta con los estándares de construcción anti-sísmica, por otra parte el datacenter de alterno cuenta con las medidas de protección sísmica.
Hardware, Software, Información	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Administrativas	PARCIAL	2	A nivel del centro de datos principal no se cuenta con un sistema de backup en un lugar diferente, actualmente se está contratando la implementación del sistema de backups con custodia de cintas. En el datacenter de Alterno tiene un contrato de backup y custodia de cintas externo
Hardware, Software, Información.	La falta de mecanismos alternos en caso de destrucción total por desastres naturales.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	PARCIAL	2	A nivel del centro de datos principal no se cuenta con un sistema de backup en un lugar diferente, actualmente se está contratando la implementación del sistema de backups con custodia de cintas. En el datacenter de Alterno tiene un contrato de backup y custodia de cintas externo

Fuente: autores

Anexo D.3 Amenaza Intrusión en la red

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
transaccional Aplicación	Acceso no autorizado a información confidencial del sistema Transaccional	Validar y hacer los ajustes requeridos en la aplicación Web del sitio www.transacional.gov.co, para que siempre exija autenticación a los usuarios y no pueda ser accedida por personal no autorizado desde Internet	Prevención	NO	1	Fue posible obtener acceso a información de los procesos almacenados en el sitio web de la aplicación Transaccional, sin necesidad de autenticación con un usuario y contraseña válidos. Referencia documento Informe – Amenazas y Códigos Maliciosos, Ethical Hacking
calidad.eps.com.co	PHP < 5.3.x Múltiples Vulnerabilidades	Actualizar el sitio web a la versión más reciente y estable disponible de PHP.	Prevención	NO	1	Está utilizando una versión de PHP anterior a 5.3.29, y esta versión está afectada por diversas vulnerabilidades como por ejemplo divulgación de información, buffer overflow, vulnerabilidades en OpenSSL y posibilidad de denegación de servicio. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
Transaccional Aplicación Mantis HC Especialistas Aplicación intranet.eps.com.co, eps.com.co intranet.eps.com.co, eps.com.co orfeo.eps.com.co calidad.eps.com.co	Servicios de autenticación Web a través de protocolos inseguros (HTTP)	Implementar servicios seguros de autenticación web como HTTPS, de tal forma que la información confidencial (usuarios y contraseñas) sea transmitida de forma cifrada, impidiendo que puedan ser interceptados y usados por terceros no autorizados.	Prevención	NO	1	El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo 'contraseña' y que transmiten su información a un servidor web remoto en texto plano. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
calidad.eps.com.co orfeo.eps.com.co	Divulgación de información de PHP (expose_php)	En el archivo de configuración de PHP 'php.ini', configurar el valor de para el parámetro 'expose_php' en 'Off' para deshabilitar este comportamiento. Finalmente, reiniciar el servicio 'daemon' del servidor web para que este cambio tenga efecto.	Prevención	NO	1	La instalación de PHP en los servidores web remotos está configurada de tal forma que permite la divulgación de información potencialmente sensitiva a un atacante a través de un URL especial. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
orfeo.eps.com.co	Divulgación de información '.svn/entries' por el servidor Web	Configure los permisos en el servidor web para denegar el acceso al directorio '.svn'.	Prevención	PARCIAL	2	El servidor web en el host remoto permite acceso de lectura a los archivos 'svn/entries'.Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
Mantis	Página por Defecto	Configurar una página de inicio del sitio web en lugar de la página por defecto de IIS. Una página de "En construcción" se puede utilizar.	Prevención	NO	1	Fue posible detectar la página por defecto del servidor Web. Esta situación puede indicar que el servidor estaría configurado con las opciones por defecto o que, en la mayoría de los casos, puede indicar que tiene vulnerabilidades que podrían ser utilizadas para obtención de acceso indebido al sistema. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
Transaccional Aplicación HC Especialistas	CGI Generic SQL Injection	Implementar mecanismos de control para filtrar caracteres peligrosos. Únicamente se debería permitir el ingreso de caracteres válidos tales como: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789@.-	Prevención	NO	1	Un ataque de tipo SQL Injection permite a un atacante insertar órdenes a nivel de la base de datos para obtener o modificar información de manera no autorizada. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*

Anexo D.3 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
calidad.eps.com.co	CGI Generic XSS	Restringir el acceso a la aplicación vulnerable. Póngase en contacto con el proveedor para obtener un parche o actualización	Prevención	NO	1	Cross-site scripting es un tipo de agujero de seguridad típico de las aplicaciones Web. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
SWITCH / 10.10.10.6						
SWITCH / 10.10.10.10						
SWITCH / 10.10.10.2						
SWITCH / 10.10.10.12						
SWITCH / 10.10.10.11						
SWITCH / 10.10.10.13						
HC Especialistas						
intranet.eps.com.co, eps.com.co	El certificado SSL no es de confianza	Adquirir un certificado digital de una entidad certificadora abierta, para que cualquier usuario que deba conectarse al servidor pueda confiar en el servicio al cual se está conectando. Si el servicio solo se accede desde la red interna, es posible generar un certificado por una entidad certificadora interna	Prevención	PARCIAL	2	El certificado SSL no ha sido firmado por una entidad certificadora abierta, la cual permite verificar la integridad del mismo. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
calidad.eps.com.co						
SWITCH / 10.10.10.1						
SWITCH / 10.10.10.12						
SWITCH / 10.10.10.13						
SWITCH / 10.10.10.11						
Transaccional BD						
HC Especialistas Base de Datos - Pruebas						
HC Especialistas Aplicación - Pruebas						
HC Especialistas						
Transaccional Aplicación						
SWITCH / 10.10.10.10	Certificado SSL expirado.	Genere un nuevo certificado SSL para el servicio.	Prevención	PARCIAL	2	El uso de este tipo de certificados SSL puede permitir que un atacante realice la suplantación del certificado con el fin de capturar el tráfico generado entre el servidor y los clientes. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
SWITCH / 10.10.10.6						
SWITCH / 10.10.10.5						
SWITCH / 10.10.10.12						
SWITCH / 10.10.10.13						
SWITCH / 10.10.10.11						
SWITCH / 10.10.10.2						
SWITCH / 10.10.10.10	Negación de servicio por renegociación de sesiones SSL / TLS	Dependiendo del servicio y la implementación de SSL, cada fabricante puede tener un parche para cada servicio.	Prevención	PARCIAL	2	Estas versiones antiguas tienen problemas como niveles de cifrado débiles para la actualidad, menores de 128bits, tener activada la renegociación de la conexión puede hacer que sea víctima de un ataque DoS. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
SWITCH / 10.10.10.12						
SWITCH / 10.10.10.13						
SWITCH / 10.10.10.11						
SWITCH / 10.10.10.12	Certificado SSL Firmado con un Algoritmo de Hash Débil	Reexpida el certificado usando SHA-1.	Prevención	PARCIAL	2	Algunos certificados SSL usan un algoritmo de hashing criptológicamente débil como MD2, MD4, MD5. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
SWITCH / 10.10.10.13						
SWITCH / 10.10.10.11						
SWITCH / 10.10.10.1						

Anexo D.3 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
SWITCH / 10.10.10.12 SWITCH / 10.10.10.13 SWITCH / 10.10.10.11	Soporte en Cifrados SSL Débiles	Reconfigure el servicio afectado para que no soporte el uso de estos algoritmos.	Prevención	PARCIAL	2	Estos algoritmos son conocidos por ser vulnerables a ataques de colisión. Un atacante puede ser capaz de usar esta debilidad para generar otro certificado con la misma firma digital. Referencia documento Informe – Amenazas y Códigos Maliciosos, Ethical Hacking
intranet.eps.com.co, eps.com.co calidad.eps.com.co Transaccional BD HC Especialistas Base de Datos - Pruebas HC Especialistas Aplicación - Pruebas HC Especialistas Transaccional Aplicación	Firmas del protocolo SMB deshabilitadas	Evaluar y configurar en los servidores afectados las recomendaciones de firmas SMB que se listan en la siguiente web: http://support.microsoft.com/kb/887429	Prevención	PARCIAL	2	Las firmas del protocolo SMB se encuentran deshabilitadas, lo cual puede ser utilizado por un atacante para ejecutar ataques tipo "hombre en el medio" en el tráfico de la red a través del protocolo SMB. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
Transaccional BD HC Especialistas Base de Datos - Pruebas	Debilidad Microsoft Windows Remote Desktop Protocol Servidor Man-in-the-Middle	Forzar el uso de SSL como capa de transporte por este servicio si es compatible, y /o seleccione la opción 'Permitir sólo las conexiones desde equipos que ejecuten escritorio remoto con autenticación a nivel de red', si está disponible.	Prevención	PARCIAL	2	NLA utiliza el proveedor de soporte de seguridad de credenciales de protocolo (CredSSP) para realizar la autenticación del servidor, ya sea a través mecanismos de TLS / SSL o mecanismos de Kerberos, que protegen contra ataques man-in-the-middle. Referencia documento Informe – Amenazas y Códigos Maliciosos, Ethical Hacking
Transaccional BD HC Especialistas Base de Datos - Pruebas	Los Servicios de Terminal Server no utilizan autenticación a nivel de red de autenticación (NLA)	Habilitar Autenticación a nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la ficha 'Remote' de los ajustes del 'Sistema' en Windows.	Prevención	PARCIAL	2	Los servicios del terminal remoto no están configurados en autenticación a nivel de red de autenticación (NLA). Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
Transaccional BD HC Especialistas Base de Datos - Pruebas	Nivel de Cifrado Bajo o Medio Terminal Services	Cambie el nivel de cifrado a alto o conforme a Federal Information Processing Standards (FIPS).	Prevención	PARCIAL	2	El servicio de escritorio remoto no está configurado para el uso de un nivel de ciframiento alto, lo que le da oportunidades al atacante de descifrar la comunicación. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
SWITCH / 10.10.10.1	Habilitada versión 1 del protocolo SSH	Deshabilitar la versión 1 del protocolo, del servidor ssh.	Prevención	PARCIAL	2	La versión de Open SSH instalada en algunos servidores es vulnerable a los siguientes ataques: El servidor acepta conexiones tipo SSH versión 1, el cual no es criptográficamente seguro. Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*
orfeo.eps.com.co SWITCH / 10.10.10.10 SWITCH / 10.10.10.12 SWITCH / 10.10.10.13 SWITCH / 10.10.10.11 HC Especialistas Aplicación	El servidor web utiliza texto claro como forma de autenticación	Asegúrese de que todas las formas sensibles de contenido se transmiten a través de HTTPS.	Prevención	NO	1	El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo 'contraseña' y que transmiten su información a un servidor web remoto en texto plano. Referencia documento Informe – Amenazas y Códigos Maliciosos, Ethical Hacking
SWITCH / 10.10.10.1	servidor Telnet no cifrado	Deshabilitar este servicio y utilizar SSH en su lugar	Prevención	NO	1	El servidor telnet se está ejecutando sobre un canal no cifrado, no se recomienda este uso ya que los nombres de usuario, contraseñas y los comandos se transfieren en texto plano. .Referencia documento Informe – *Amenazas y Códigos Maliciosos, Ethical Hacking*

Fuente: autores

Anexo D.4 Amenaza Daños por Agua

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Información.	Ausencia de pisos elevados.	Se debe implementar protección contra inundaciones.	Minimizadoras	SI	3	Los Datacenter están ubicados en pisos elevados para prevenir inundaciones, así mismo se cuenta con piso falso.
	Calidad baja en la construcción de los edificios.	La construcción del edificio debe ser resistente a fugas de agua.	Minimizadoras	SI	3	Los edificios cumplen con los requerimientos de construcción.
	Sistema de drenaje débil.	Se debe implementar protección en contra de inundaciones y fugas de agua.	Minimizadoras	SI	3	Se cuenta con sistemas de drenaje para los datacenter.

Fuente: autores

Anexo D.5 Amenaza Robo y Sabotaje

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, Información	Falta de protección física.	Perímetros de seguridad (barreras como: paredes, entradas con uso de tarjetas) deben ser usadas para proteger áreas que contienen información y proteger instalaciones que procesan información.	disuasión	SI	3	Se cuenta con perímetros físicos para la protección de los activos, a nivel de los centros de datos Principal y Alterno se cuenta con protección biométrica, protección de perímetros.
		Las áreas seguras deben estar protegidas apropiadamente por controles que garanticen el acceso de personal autorizado.	prevención	PARCIAL	2	Las áreas donde se procesa información como centro de datos y los archivos de gestión documental se encuentran protegidos con puertas, actualmente se está implementando el sistema de control de acceso por tarjetas para toda la EPS.
		Seguridad física debe ser diseñada y aplicada para oficinas, salas, y demás recursos.	disuasión	PARCIAL	2	Actualmente se está implementando el sistema de control de acceso por tarjetas para toda la EPS Se cuenta con la seguridad del edificio y celadores para el acceso a los pisos.
		Protección física y directrices deben ser diseñadas y aplicadas para trabajar en áreas seguras.	disuasión	NO	1	No se cuentan con guías o procedimientos para protección física y trabajos en áreas seguras.
		Puntos de acceso como áreas de entrega y de carga, en donde personas no autorizadas pueden entrar, deben ser controlados y de ser posible, deben ser aisladas de salas de procesamiento de información, con el fin de evitar accesos no autorizados.	prevención	SI	3	Se cuentan con áreas separadas para el acceso de proveedores, áreas de carga y atención de ciudadanos. Las áreas de protección de información están aisladas de zonas con acceso a personal que no pertenece a la EPS.
		Los usuarios deben garantizar que un equipo no atendido tenga la protección adecuada.	prevención	PARCIAL	2	Actualmente se tiene las políticas de DA, para bloqueo de sesión de usuario, no se cuenta con una política para el bloqueo de aplicaciones desatendidas.
	No existe una supervisión del trabajo de personal externo o de limpieza.	Establecer mecanismos de control sobre el personal externo y de aseo, como: Términos y condiciones de seguridad de la información en los contratos cuyo personal acceda a las instalaciones de la EPS Incorporar en el programa de concientización en seguridad un contenido dirigido a personal externo que labora en las instalaciones de la EPS como requerimiento o condicionamiento para el inicio de sus labores.	disuasión	PARCIAL	2	Se realizan inducciones y reinducciones a todo el personal a nivel de operación tecnológica, al no existir un programa de capacitación de seguridad de la información no se ha establecido un plan enfocado a seguridad de la información.
	Ausencia o insuficiencia de procedimientos para el manejo y almacenamiento de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información para proteger la información contra la divulgación no autorizada o mal uso de la misma.	administración	NO	1	No se ha establecido un procedimiento de manejo y almacenamiento de información sensible de las áreas. Actualmente no se identifican herramientas para manejo seguro de información sensible.
		La documentación de los sistemas debe estar protegido contra el acceso no autorizado.	prevención	PARCIAL	2	Se tienen carpetas compartidas para el área de TI y DGI, donde se maneja información técnica de las aplicaciones, sin embargo esta información puede ser accedida por cualquier usuario de las áreas de TI y DGI.

Anexo D.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, Información	Ausencia o insuficiencia de procedimientos para la clasificación de la información.	Todos los activos deben estar claramente identificados y clasificados en un inventario de acuerdo a su importancia. El inventario debe ser actualizado constantemente.	administración	NO	1	Se está ejecutando el inventario de activos de información.
		Toda la información y los activos asociados con el proceso de información deben poseer un propietario en la entidad.	administración	NO	1	Se está ejecutando el inventario de activos de información.
	La clasificación de activos es insuficiente.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	administración	NO	1	Se está ejecutando el inventario de activos de información.
	Etiquetado de información insuficiente	Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por EPS.	administración	PARCIAL	2	No se cuenta con procedimientos de clasificación y etiquetado de información. Sin embargo en el área de ASD de gestión documental, se encargan de recibir la información física y digital de procesos jurídicos de la EPS para posteriormente realizar la clasificación del nivel de privacidad que deben manejar cada uno de los procesos.
	Existe un inadecuado entendimiento acerca de las implicaciones y consecuencias debido a la divulgación de información confidencial.	Identificar, documentar y revisar regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la EPS para la protección de la información.	administración	NO	1	No se cuenta con un procedimiento para la identificación, documentación y revisión regular de requisitos de seguridad de la información que reflejen las necesidades de la EPS.
		Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la entidad para la seguridad de la información.	disuasión	PARCIAL	2	Se cuenta con un acuerdo de confidencialidad estándar en los contratos de funcionarios de planta y contratistas, sin embargo no existe una política de seguridad de la información para generar el cumplimiento de responsabilidades frente a seguridad de la información.
		Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de información.	disuasión	PARCIAL	2	Se cuenta con procesos disciplinarios para funcionarios y contratistas sin embargo este proceso no contempla violaciones frente a seguridad de la información.
		El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados.	disuasión	NO	1	No se cuenta con un procedimiento que establezca mecanismos para capacitar y sensibilizar a los usuarios acerca del uso inadecuado de los recursos de tratamiento de información.
	Procedimientos inadecuados de contratación de personal.	Se debe realizar pruebas de verificación de los antecedentes sobre todos los candidatos a empleados, contratistas, y usuarios de terceras partes, de acuerdo con las leyes, reglas y éticas pertinentes, y de forma proporcional a los requisitos de negocio, la clasificación de la información a la que se accede, y a los riesgos observados.	disuasión	SI	3	El área de talento humano y contratos realiza las actividades de contratación de personal de acuerdo a los procedimientos de contratación, los cuales incluyen actividades de verificaciones de seguridad y antecedentes de los candidatos.
	Inadecuada e insegura reutilización o eliminación de los equipos	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.	monitorización	PARCIAL	2	A través del proveedor Avante realizan un procedimiento de borrado seguro en los equipos de usuario en los casos que se requiera cambio de equipo o formateo de equipos de usuario. A nivel de servidores no se cuenta con un procedimiento de borrado seguro en el caso que se requiera retirar un equipo.
		El equipo, información o software no debe ser sacado fuera de la Entidad sin autorización.	prevención	SI	3	El retiro de equipos solo es autorizado por el Ing. Ernesto Fuerte para que puedan ser retirados de las instalaciones del Datacenter, la autorización se da por medio de un formato que guarda en la oficina de TI. No se cuenta con un procedimiento documentado pero se tienen actividades definidas. A nivel de la portería no se permite sacar un equipo sin la autorización de la EPS.
		Debería haber procedimientos para la gestión de los medios informáticos removibles	monitorización	NO	1	No se cuenta con un procedimiento para gestión de medios removibles.
		Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	monitorización	PARCIAL	2	No se cuenta con un procedimiento de destrucción segura para todos los medios de almacenamiento de información. Sin embargo a través del proveedor Avante realizan un procedimiento de borrado seguro en los equipos de usuario en los casos que se requiera cambio de equipo o formateo de equipos de usuario.

Anexo D.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
	Existe una inadecuada segregación de funciones para asignar accesos físicos.	Implementar una adecuada segregación para las actividades de mantenimiento y administración de tarjetas de identificación y acceso.	administración	PARCIAL	2	Se cuenta con un sistema de gestión de acceso para instalaciones de la EPS A nivel del área de TI el sistema de acceso al datacenter es autorizado por el gerente de TI y es creado por el área de TI. A nivel del datacenter de Level3 se cuenta con un proceso de autorización para el acceso al datacenter de Level3
	Medidas inadecuadas cuando el contrato de empleados y personal externo finaliza.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir y comunicar al empleado o contratista.	disuasión	PARCIAL	2	En el área de TI se conoce el procedimiento para el retiro de un empleado o tercero de la organización, se entrega equipo, se realiza backup, pero esto se deja registro por medio de correo, no existe un procedimiento formal para la aprobación. No existe política de deberes y responsabilidades con seguridad de la información.
		Todos los empleados, contratistas y terceros deben retornar todos los activos de la entidad que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.	administración	SI	3	El área de recursos físicos se tiene un formato de paz y salvo para la devolución de activos físicos el cual es necesario para generar la liquidación de un funcionario.
Información	Inadecuado retiro de los derechos de acceso cuando el contrato de empleados y personal externo finaliza.	Los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información deben ser removidos hasta la culminación del empleo, contrato o acuerdo, o debe ser ajustada en caso de cambio.	disuasión	PARCIAL	2	No está documentado el procedimiento de disponer de los permisos de los usuarios, pero se conoce el procedimiento con los líderes, se realiza un backup periódico de la documentación del empleado, y con un tiempo máximo de 20 días la información almacenada del empleado se elimina.
	Ausencia o inadecuados mecanismos de prevención de fuga de información.	Se deberían establecer políticas, procedimientos y controles formales de intercambio de información con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación.	disuasión	PARCIAL	2	Existe una carpeta compartida por cada área, el líder cuenta con permisos de todo, cuando se requiere un permiso, se solicita por medio de correo. No existe documentación y/o procedimiento para la solicitud o retiro de permisos.
		La información implicada con la mensajería electrónica debe ser protegida apropiadamente.	monitorización	SI	3	Se tiene protección con certificados SSL en la comunicación de los web services, también el correo electrónico y Lync están funcionando con autenticación con el Directorio Activo y SharePoint.
		Las oportunidades de fuga de información deben ser prevenidas.	monitorización	NO	1	No se han establecido mecanismos de control para prevenir la fuga de información.
	Ausencia de controles para el control de dispositivos móviles	Se debería adoptar una política y unas medidas de seguridad de soporte, para gestionar el uso de dispositivos móviles.	disuasión	NO	1	No se ha establecido política acerca del uso y control de dispositivos móviles.
Hardware, Software, información	Insuficiente seguridad de los equipos fuera de las instalaciones	Se debe aplicar seguridad a los equipos que se encuentran fuera de las instalaciones de la entidad tomando en cuenta los diversos riesgos a los que se está expuesto.	minimización del impacto / limitación del impacto	NO	1	Los gerentes son los únicos que tienen permiso para sacar portátiles de la organización, esto debería ser controlado y registrado por los celadores, pero pocas veces se controla ese procedimiento. No existe documentación.
Hardware, Software, información	Ausencia de gestión de incidentes de seguridad.	Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada.	administración	PARCIAL	2	Actualmente no existe un canal directo para gestión de incidentes, se comunica normalmente por correo o por chat empresarial. No existe un procedimiento de para escalar los eventos de seguridad. Las personas conocen con qué departamento se deben comunica pero no está documentado.
	Ausencia de procedimientos para el reporte sobre incidentes de seguridad.	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.	administración	NO	1	Se informa por correo del incidente, no existe procedimiento para tal fin. Ni para terceros ni para empleados.
	Insuficiente identificación y definición de las responsabilidades para la gestión de incidentes de seguridad	Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.	administración	NO	1	No se encuentra segmentado los roles y responsabilidades, no existe documentación de los procedimientos de escalamiento frente a la gestión de seguridad. Los empleados saben que Camilo es el encargado de seguridad, pero no está documentado.

Anexo D.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
	Insuficiente monitoreo de incidentes de seguridad	Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.	administración	PARCIAL	2	Se encuentran monitoreados los sistemas, pero no existe algún procedimiento ni formato para el seguimiento a los mismos.
		Cuando una acción de seguimiento contra una persona u entidad, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.	administración	PARCIAL	2	No hay un procedimiento de recolección de evidencia formal, se hace seguimiento de acuerdo al monitoreo de modificaciones que se tiene, pero no existe documentación para esto, actualmente se escala enviando correo al líder del grupo.
Software, Información	Ausencia de políticas de seguridad y procedimientos completos cuando se trata de partes externas, clientes y terceros.	Los riesgos a la información de la entidad y a las instalaciones del procesamiento de información desde los procesos del negocio que impliquen a terceros deben ser identificados y se debe implementar controles apropiados antes de conceder el acceso.	prevención	PARCIAL	2	Se realiza por medio de una solicitud vía mail al líder, no se encuentra documentado el procedimiento, pero el personal de la EPS conoce las actividades, estas políticas son comunicadas a los terceros.
		Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activos de la entidad.	prevención	PARCIAL	2	Se conoce el procedimiento para gestión y habilitación a los sistemas a terceros, pero esto no está documentado, por lo cual no está comunicado a los mismos. Se maneja por correo, pero no está formal.
Información		Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la entidad o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, debe cubrir todos los requisitos de seguridad relevantes.	disuasión	PARCIAL	2	Se tiene establecido por medio del contrato el acceso a la información, pero no existe documentación formal acerca de la gestión de información con terceros.
		Los acuerdos deben ser establecidos para el intercambio de información y software entre la entidad y terceros.	disuasión	NO	1	Existe política de seguridad de la información, no se comunica con terceros.
		Los medios que almacenan información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la Entidad.	prevención	NO	1	No se existe control para el almacenamiento de medios extraíbles.
Información	Ausencia de protección para la información transmitida a través de comercio electrónico	La información envuelta en el comercio electrónico pasando a través de redes públicas, debe ser protegida de actividad fraudulenta, disputas de contratos y de acceso y modificación no autorizada.	prevención	SI	3	No se maneja comercio electrónico, se usa el sistema SIIF el cual es administrado por el Gobierno Nacional, se instala el certificado en el equipo cliente de la organización y un token, esto está protegido.
		Se debe proteger la información implicada en transacciones en línea para evitar transmisiones incompletas, enrutamiento erróneo, alteración no autorizada de mensajes, divulgación no autorizada, reproducción o duplicación no autorizada de mensajes.	prevención	PARCIAL	2	Se cuenta con la protección del firewall, pero no existe ningún otro mecanismo de seguridad implementado a nivel de transporte de información. Lo que se encuentra implementado no está documentado.
		La integridad de la información que se ha hecho disponible en un sistema público debe ser protegido para prevenir modificaciones no autorizadas.	prevención	SI	3	Los sistemas que están públicos son el mail y el sitio web. Estos están soportados por Microsoft, el sitio web fue implementado por un tercero (micro sitios), cuenta con certificados SSL esto se encuentra documentado.
Información	Insuficiente protección a los registros de los sistemas (Logs)	Las herramientas de registro y los registros de información deben estar protegidos contra la manipulación y acceso no autorizado.	prevención	PARCIAL	2	Se hace backup de los logs de los sistemas, pero esto no se tiene documentado.
Hardware, Software, Información	Ausencia de concienciación sobre la seguridad de la información	Todos los empleados de la entidad y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	SI	3	Se hace seminarios de capacitación semestral a todos los empleados de la EPS y contratistas, de concientización de seguridad de la información, uso de equipos, seguridad social.
	Insuficiente revisión de las políticas de seguridad de la información	La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad.	concienciación	NO	1	No se revisa ni actualiza la política de seguridad.

Anexo D.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
	Falta de compromiso de la dirección a nivel de seguridad de la información	La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	concienciación	PARCIAL	2	Los líderes de cada área comunican los cambios en los sistemas, pero no hay formalmente una política que se comunique.
		La gerencia debe apoyar activamente en la seguridad dentro de la entidad a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de la información.	administración	NO	1	No existen roles ni responsabilidades claras acerca de seguridad de la información
		La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la entidad con roles relevantes y funciones de trabajo.	concienciación	NO	1	El rol de los líderes de cada área esta desde el punto informativo. No están definidas actividades para la seguridad de la información.
		Deberían definirse claramente las responsabilidades. Incluye la asignación de responsables de los activos de información.	administración	PARCIAL	2	Se conoce los propietarios de los activos de información como también el custodio, pero esto no se encuentra documentado.
Información	Inexistencia del proceso de sanatización en un ambiente de prueba de datos	Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.	monitorización	NO	1	Los datos que se encuentran en el ambiente de pruebas son exactos a los de producción, pero no se tiene ningún control sobre estos datos.

Fuente: autores

Anexo D.6 Amenaza Mal Uso del Software

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Software	Falta de medidas de restricción contra acceso no autorizado	Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	prevención	PARCIAL	2	Se tiene definido que los únicos autorizados para solicitar privilegios de acceso son los líderes de área a través de correo, sin embargo, no se tiene definido un procedimiento de revisión de usuarios y sus privilegios. Actualmente no se encuentra con una matriz de roles y perfiles definida para las aplicaciones de la EPS.
		Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados).	prevención	PARCIAL	2	A nivel del datacenter se restringe el acceso a los ambientes productivos para su administración a Level3, el acceso a los sistemas de información s e restringe a través de usuarios y contraseña.
	Ausencia de conciencia de seguridad Insuficiente capacitación a los usuarios	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	NO	1	No se ha establecido un plan de capacitación frente a seguridad de la información.
	Transferencia/almacenamiento de contraseñas en texto claro	La asignación de contraseñas debe controlarse a través de un proceso de gestión formal. Las contraseñas temporales se deben entregar a los usuarios de forma segura. Se debe evitar el uso de mensajes electrónicos desprotegidos (texto sin cifrar). Las contraseñas nunca deben ser almacenadas en sistemas informáticos de forma desprotegida.	administración	PARCIAL	2	Se tiene actividades de entrega de contraseñas por parte del área de TI y DGI, sin embargo, no se tiene un procedimiento formalizado para la gestión de contraseñas. Existen herramientas de almacenamiento de software libre sin embargo esto no es algo mandatorio en toda la EPS.

Anexo D.6 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
	Ausencia de controles para la instalación de software	Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales.	administración	SI	3	Se tiene restricciones a nivel de privilegios a nivel de usuarios, adicionalmente se cuenta con System center para el control de aplicaciones.
	Ausencia de control de accesos al código fuente de las aplicaciones	El acceso a los códigos de programas fuente debe ser restringido.	prevención	PARCIAL	2	Se encuentra restringido para solo ingenieros de desarrollo, sin embargo se encuentra en un repositorio en la web.
	Falta de mecanismos de monitoreo y supervisión periódicos.	Los procedimientos para el uso y el monitoreo de las instalaciones de procesamiento de información deben ser establecidos. Los resultados de las actividades de monitoreo deben ser revisadas regularmente.	administración	SI	3	Actualmente se tiene el sistema System Center para el monitorear la disponibilidad y capacidad de servidores y redes. El proveedor del centro de datos alterno es responsable del monitoreo de los servidores en el datacenter.
	Insuficiente auditoría sobre las operaciones de los administradores	Las actividades del administrador y de los operadores del sistema deben ser registradas.	prevención	NO	1	No se tiene un procedimiento de gestión y monitoreo de actividades de los administradores.
	Ausencia de controles para el cierre o bloqueo de sesión de usuario o del sistema.	Las sesiones se deberían desactivar tras un periodo definido de inactividad.	prevención	PARCIAL	2	A nivel de Directorio activo se cuenta con un control de bloqueo, sin embargo, para servidores internos se cuenta con configuraciones de contraseñas por defecto, a nivel de las aplicaciones no se identificó un estándar de configuraciones para el cierre automático.
	Daño en la integridad de la información registrada en los sistemas de información.	Se deberían incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados. Como un control preventivo se debería instalar y actualizar herramientas para la detección de código y software malicioso.	monitorización	PARCIAL	2	Se tienen restricciones a nivel de acceso a la información, para evitar modificaciones en la comunicación se usan certificados SSL. Se realizan validaciones sobre cambios a sistemas en el ambiente de pruebas. Se mantiene actualizado el antivirus de los endpoints. No existe un procedimiento formal ni documentado para la detección de software malicioso.
Información	Procedimientos insuficientes para verificar el cumplimiento de las políticas y estándares de seguridad.	Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.	administración	PARCIAL	2	Se han generado por parte del área de planeación auditorías a los sistemas a nivel de seguridad, sin embargo no se tiene establecida una política de seguridad de la información a nivel de la EPS que dicte los lineamientos de cumplimiento de seguridad. No se identificaron actividades de plantillas para el aseguramiento de las plataformas tecnológicas.
		Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información.	monitorización	NO	1	No se identificaron actividades de plantillas para el aseguramiento de las plataformas tecnológicas. No se ha establecido formalmente actividades de revisión de las configuraciones de seguridad de la información.
	Ausencia de mecanismos de control y política de uso de software de almacenamiento en la nube.	Se debería definir y comunicar la política para la transferencia segura de información del negocio entre la organización y las partes externas (Google, Dropbox, OneDrive)	concienciación	NO		No se tiene una política y/o procedimiento para el uso de almacenamiento en la nube
	Procedimientos insuficientes para la auditoría de controles en los sistemas de información.	Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.	administración	SI	3	Se hace cada año una auditoría externa de todas las plataformas, se tiene actualmente el primer reporte y van a realizar los controles pertinentes, esto se encuentra documentado.
		Se deberían proteger los accesos a las herramientas de auditoría de sistemas con el fin de prever cualquier posible mal uso o daño.	monitorización	SI	3	No existe herramienta de auditoría de sistemas. Se hacen las pruebas con los usuarios finales. El usuario define cuánto tiempo va a realizar la prueba
Hardware, Software, Información	Falta de documentación para procedimientos operativos.	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.	administración	PARCIAL	2	Se cuenta con la documentación de la operación de tecnología y manuales de los proveedores, sin embargo no se cuenta con la totalidad de la documentación de las operaciones de TI.

Anexo D.6 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Software, Información	Software de monitoreo insuficiente para prevenir los accesos no autorizados así como el acceso a información sensible	La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restringa y se mantenga fuertemente controlado.	monitorización	PARCIAL	2	Se tienen restricciones de a nivel de instalación de software operativo sin embargo no se identifican procedimientos de monitoreo de accesos no autorizados o herramientas para prevenir el acceso no autorizado
Software, Información	Cambios no autorizados en los paquetes de software	No se recomiendan modificaciones a los paquetes de software. Se debería limitar a cambios necesarios y todos estos deben ser estrictamente controlados.	prevención	NO	1	No se han realizado actualizaciones sobre software alterno, por lo cual no se tiene control, esto no está documentado.

Fuente: autores

Anexo D.7 Amenaza Fallas en Infraestructura y Redes

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, Información	Ausencia de procesos de autorización	Debería establecerse un proceso de autorización cuando se va a realizar la instalación de un nuevo recurso en los centros de tratamiento de la información.	Administración	PARCIAL	2	No se tienen procedimientos pero se está haciendo de forma controlada en el datacenter principal y en el datacenter alterno
	La falta de procedimientos formales para la gestión de cambios de terceros.	Los cambios en la provisión de servicios (incluido el mantenimiento y mejoras de las políticas, procedimientos y controles de seguridad de la información) teniendo en cuenta la criticidad de los sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos	Administración	PARCIAL	2	No se tienen procedimientos, pero se está haciendo de forma controlada con los proveedores a través de correos y programación de actividades de mantenimiento para el datacenter principal y en el datacenter alterno
Hardware	Sistema sobrecargados / planificación de la capacidad inadecuada	Se monitoriza y ajusta el uso de recursos, y se hacen pronósticos de los requisitos de capacidad futuros, para asegurar las prestaciones requeridas del sistema	Monitorización	NO	1	No se tiene implementado un control, no se encuentra formal, sin embargo cuando se implementa un nuevo componente de infraestructura se realiza una proyección de la capacidad de manera informal.
Software	Ausencia de una metodología adecuada de desarrollo de software	La introducción de nuevos sistemas y cambios importantes en los sistemas existentes deberían seguir un proceso formal de la documentación, especificaciones, pruebas, control de calidad y gestión de la implementación.	Administración	PARCIAL	2	Actualmente no usan ninguna metodología para nuevos cambios, se documenta el cambio, se hacen pruebas, se aprueba el cambio.
		Outsourcing de desarrollo de software deben ser supervisados y controlados por la entidad.	Monitorización	PARCIAL	2	El proveedor realiza el desarrollo, se controlan los cambios sobre los sistemas, se documentan, pero el sistema se encuentra bajo la custodia del proveedor del datacenter alterno este envía reportes mensualmente sobre disponibilidad y monitoreo de los sistemas. No existe un procedimiento formal para esto.
	Ausencia de pruebas de aceptación	Establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones así como las pruebas adecuadas del sistema (s) llevadas a cabo durante el desarrollo y antes de su aceptación.	Administración	NO	1	No hay criterio de aceptación, el requerimiento funcional solicitado al tercero se valida únicamente con la funcionalidad.
	Instalaciones y configuraciones defectuosas	Se debe asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.	prevención	SI	3	Los niveles de servicios son contractuales con los terceros, esto se mantienen monitoreados por el tercero los cuales envían periódicamente un informe de SLA, hay una persona que se encarga de revisar estos informes y validarlos.

Anexo D.7 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware	Baja calidad en los equipos de hardware	Establecer requerimientos de la entidad para nuevos sistemas de información o para la mejora de los ya existentes, que especifiquen los controles de seguridad requeridos.	administración	PARCIAL	2	No se tiene un control establecido formalmente, sin embargo durante los años de operación de la EPS se han contratado expertos para generar los lineamientos y arquitectura de hardware necesaria para soportar la operación de la EPS. Para nuevas adquisiciones no se tiene un control.
	Uso de periféricos y repuestos incompatibles			PARCIAL	1	A nivel de equipos de hardware de equipos se tiene un contrato de soporte a través de la empresa que alquila los equipos de la EPS quien provee los repuestos compatibles para los equipos. A nivel de servidores se tienen contratos con los fabricantes para la adquisición de repuestos.
Hardware, Software, Información	Ausencia de monitoreo regular	Se debe asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa. Se recomienda realizar informes periódicos según la norma internacional ISAE 3402 para el control de servicios de terceros.	monitorización	PARCIAL	2	Se tiene un interventor del contrato con el proveedor de datacenter alterno para realizar el monitoreo de acuerdos de servicio que se definieron con el proveedor, pero no está documentado la metodología de seguimiento y control
Hardware, Software	Ausencia de sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo	prevención	PARCIAL	2	La mayor parte de los equipos están conectados al directorio activo, el cual provee una sincronización de los relojes, sin embargo no se tiene un procedimiento para que el 100% de los equipos este sincronizado.
	Debilidades en las medidas de restricción de acceso no autorizado (física y lógica)	Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	prevención	PARCIAL	1	Se cuentan con sistemas biométricos a los centros de datos, más los procedimientos de acceso físico. A nivel de servidores se restringe el acceso a través de políticas de directorio a los administradores de TI de la EPS, en los sistemas de producción ubicados en el datacenter alterno se tiene un contrato de administración sobre los servidores en el cual ellos son los únicos que puede tener la administración.
Hardware	Ausencia de equipos adecuados para la protección de fallas de energía	Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas a través de los equipos de apoyo.	prevención	PARCIAL	2	A nivel del datacenter principal se tiene una UPS para toda la EPS así como una planta de energía para todo el edificio. A nivel del datacenter de alterno se tiene controles de nivel TIER3
	Ausencia de medidas adecuadas para el control de la temperatura y humedad	El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.	minimización del impacto / limitación del impacto	PARCIAL	2	A nivel del datacenter se tiene todos los controles de Nivel 3, a nivel del centro de datos se tienen controles temperatura a través de dos sistemas de aire, se está implementando el sensor de temperatura.
	Ineficaz / insuficiente formación de los usuarios	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	NO	1	Se está implementando un plan de capacitación, sin embargo el personal que opera no tiene todas las competencias técnicas para la operación de la plataforma actual. A nivel del personal que opera los ambientes de producción el proveedor del datacenter alterno es el encargado, sin embargo no existe un control que garantice que asigna el perfil de profesionales adecuado para la operación.
Hardware, información	Líneas de comunicación desprotegidas	Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.	prevención	SI	3	Se tiene cableado estructurado bajo estándares aunque es un edificio antiguo, a nivel de comunicaciones los equipos se encuentran en el datacenter. A nivel del proveedor alterno se cuentan con los controles de seguridad para el cableado según el estándar TIAR3
	Uniones incorrectas del cableado e insuficiente seguridad para el cableado					
	Inadecuada seguridad de la red	Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito.	prevención	SI	3	Se tienen controles de seguridad como Firewalls, sin embargo, no se tienen controles para la detección de eventos, seguridad proactivo, en los equipos de apoyo. A nivel del datacenter de Alterno se cuenta con equipos de seguridad como IPS
Hardware	Ausencia de mantenimiento periódico	Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.	prevención	SI	3	Se tienen contratos, con los fabricantes y proveedores de los equipos, y los vendedores de los equipos.

Anexo D.7 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, información	La falta de soporte del proveedor adecuado	Mantener con el proveedores adecuados contratos de soporte y mantenimiento	administración	SI	3	Se tienen contratos, con los fabricantes y proveedores de los equipos, y los vendedores de los equipos.
	Falta de proveedores expertos	La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.	administración	PARCIAL	2	Se han solicitado a nivel de contratos los perfiles adecuados, sin embargo se ha visto que el soporte de proveedores a sistemas de información, no ha sido el adecuado.
	Fallas de los proveedores					
	Un único punto de fallo en la arquitectura, ausencia de disponibilidad de enlaces de respaldo	La incorporación de redundancia en la red, hacer uso de los servicios públicos (energía y las líneas de comunicación locales) de más de una fuente / proveedor de servicios	prevención	PARCIAL	2	A nivel del datacenter principal no se tiene alta disponibilidad, se tiene alta disponibilidad en canal de internet, a nivel de red de los servidores de alterno se garantiza alta disponibilidad

Fuente: autores

Anexo D.8 Amenaza Errores Humanos

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Información	Insuficiente definición de roles y responsabilidades en materia de seguridad de la información	Las funciones y responsabilidades de los empleados, contratistas y terceros deben ser definidas y documentadas en concordancia con la política de seguridad de la organización.	administración	PARCIAL	2	No se cuenta con una política de seguridad de la información que defina lineamientos para establecer funciones y responsabilidades, sin embargo se cuenta con un manual de funciones para funcionarios de planta y contratistas.
Hardware, Información	La ausencia o ineficacia / insuficiente capacitación de los usuarios	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	NO	1	Se cuenta con actividades de entrega de puesto al iniciar el vínculo laboral. No se cuenta con un plan de capacitación para cada una de las áreas. Se ejecutan planea de actualización e inducción peor no existe un plan de estudios o de profundización.

Fuente: autores

Anexo D.9 Amenaza Terrorismo

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Hardware, Software, Información	Disturbios civiles	Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.	prevención	SI	3	Se cuenta con planes de evacuación frente de disturbios y eventos de malestar social, se han realizado simulacros de evacuación. El área donde se encuentra ubicada la EPS no es propensa a disturbios. El área encargada de la coordinación de actividades de evacuación es Talento Humano. En el caso que no se pueda ingresar a las instalaciones las aplicaciones críticas se encuentran en el datacenter de Alterno.
Hardware, Software, información	Insuficiente conocimiento de las autoridades correspondientes.	Deben ser mantenidos contactos apropiados con autoridades relevantes.	administración	SI	3	Se tiene establecido contactos con los organismos de emergencia, a nivel de alarmas de incendio y alarmas de intrusión. En el plan de evacuación se contempla un árbol de llamadas de acuerdo al tipo de emergencia.

Fuente: autores

Anexo D.10 Amenaza Legal

Activos afectados	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Comentarios
Información, Software	Comprensión insuficiente de las nuevas leyes y reglamentos y la identificación de la legislación aplicable	Se debería establecer política de tratamiento de la información de alojada en el registro nacional de base de datos fundamentado con el Decreto 886 de 2014	administración	NO	1	No existe política de tratamiento de base de datos.
		Se deberían definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información. Se debería establecer política de cumplimiento de la Ley 1712 de 2014 para la transparencia y acceso a la información pública nacional.	administración	PARCIAL	2	Los empleados de la EPS, los conocen por medio de los seminarios internos que se realizan, también por las noticias internas acerca de la reglamentación aplicable. Pero esto no se encuentra documentado.
	Procedimiento insuficiente para el cumplimiento de los requisitos de propiedad intelectual	Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.	administración	PARCIAL	2	A nivel de contratos se establecen las restricciones legales y contractuales. Pero no existe un procedimiento ni documentación formal para conocer cuáles son aplicables.
	Protección insuficiente de los registros de la organización	Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio	recuperación	PARCIAL	2	Algunas áreas cuentan con los controles de protección de la información, se encuentran bajo llave, se guardan registros de modificación.
	Insuficiente protección y privacidad de información personal	La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales. Se debería implementar una política de protección de datos en base a la Ley 1581 de 2012 y el decreto 1377 de 2013.	administración	NO	1	No existe un procedimiento y/o proceso formal para el tratamiento de los datos personales de los empleados y clientes. Conocen el requerimiento legal pero no es aplicable.
	Reglamento de los controles criptográficos	Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.	prevención	NO	1	No existe ninguna implementación sobre esto.

Fuente: autores

Anexo E. Matriz de impacto residual y riesgo residual

Anexo E.1 Amenaza Fuego

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Proximidad a plantas de producción de Petróleo, Gasolina y Químicos Inflamables	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de Petróleo, Gasolina y Químicos Inflamables.	Minimizadoras	3	5	1,7	1	1,7	B
	Proximidad a áreas de alta combustión o áreas de almacenamiento de material inflamable			3	5	1,7	1	1,7	B
	Interiores construidos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura.	Minimizadoras	3	5	1,7	1	1,7	B
	Equipos y circuitos eléctricos de baja calidad			3	5	1,7	1	1,7	B
	Manejo inadecuado de cilindros de gas, etc.	Definir directrices para el manejo de cilindros de gas, etc.	Administrativas	3	5	1,7	1	1,7	B
	Ausencia de un sistema de detección de incendios.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura. Establecer directrices para comer, beber y fumar en proximidad a las instalaciones de procesamiento de información.	Minimizadoras	2	5	2,5	1	2,5	B
	Ausencia de equipo contra incendios.			2	5	2,5	1	2,5	B
	Se permite fumar dentro de las instalaciones			2	5	2,5	1	2,5	B
	Exteriores hechos con material combustible.			2	5	2,5	1	2,5	B
	La falta de mecanismos alternos en caso de destrucción total por fuego.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	2	5	2,5	1	2,5	B
	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Recuperación	1	5	5,0	1	5,0	M

Anexo E.1 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Proximidad a plantas de producción de Petróleo, Gasolina y Químicos Inflamables	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de Petróleo, Gasolina y Químicos Inflamables.	Minimizadoras	3	5	1,7	1	1,7	B
	Proximidad a áreas de alta combustión o áreas de almacenamiento de material inflamable			3	5	1,7	1	1,7	B
	Interiores construidos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura.	Minimizadoras	3	5	1,7	1	1,7	B
	Equipos y circuitos eléctricos de baja calidad			3	5	1,7	1	1,7	B
	Manejo inadecuado de cilindros de gas, etc.	Definir directrices para el manejo de cilindros de gas, etc.	Administrativas	3	5	1,7	1	1,7	B
	Ausencia de un sistema de detección de incendios.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura. Establecer directrices para comer, beber y fumar en proximidad a las instalaciones de procesamiento de información.	Minimizadoras	2	5	2,5	1	2,5	B
	Ausencia de equipo contra incendios.			2	5	2,5	1	2,5	B
	Se permite fumar dentro de las instalaciones			2	5	2,5	1	2,5	B
	Exteriores hechos con material combustible.			2	5	2,5	1	2,5	B
	La falta de mecanismos alternos en caso de destrucción total por fuego.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	2	5	2,5	1	2,5	B
	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Recuperación	1	5	5,0	1	5,0	M

Anexo E.1 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Proximidad a plantas de producción de Petróleo, Gasolina y Químicos Inflamables	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de Petróleo, Gasolina y Químicos Inflamables.	Minimizadoras	3	5	1,7	1	1,7	B
	Proximidad a áreas de alta combustión o áreas de almacenamiento de material inflamable			3	5	1,7	1	1,7	B
	Interiores construidos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura.	Minimizadoras	3	5	1,7	1	1,7	B
	Equipos y circuitos eléctricos de baja calidad			3	5	1,7	1	1,7	B
	Manejo inadecuado de cilindros de gas, etc.	Definir directrices para el manejo de cilindros de gas, etc.	Administrativas	3	5	1,7	1	1,7	B
	Ausencia de un sistema de detección de incendios.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente. Materiales inflamables o peligrosos deberán almacenarse a una distancia segura. Establecer directrices para comer, beber y fumar en proximidad a las instalaciones de procesamiento de información.	Minimizadoras	2	5	2,5	1	2,5	B
	Ausencia de equipo contra incendios.			2	5	2,5	1	2,5	B
	Se permite fumar dentro de las instalaciones			2	5	2,5	1	2,5	B
	Exteriores hechos con material combustible.			2	5	2,5	1	2,5	B
	La falta de mecanismos alternos en caso de destrucción total por fuego.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	administrativas	2	5	2,5	1	2,5	B
	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Recuperación	1	5	5,0	1	5,0	M

Fuente: autores

Anexo E.2 Amenaza Desastres Naturales

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un área propensa a inundaciones.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de pisos elevados.	Se debe implementar protección contra inundaciones.	Minimizadoras	3	5	1,7	1	1,7	B
	Calidad baja en la construcción de los edificios.	La construcción del edificio debe ser resistente a fugas de agua.	Minimizadoras	3	5	1,7	1	1,7	B
	Incapacidad para absorber rayos	Sistemas para rayos y sistemas de polo a tierra	Minimizadoras	3	5	1,7	1	1,7	B
	Sistema de drenaje débil.	Se debe implementar protección en contra de inundaciones y fugas de agua.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de control de temperatura y humedad adecuada	Sistema de monitoreo adecuado para temperatura y humedad	Monitorización	2	5	2,5	1	2,5	B
		Las condiciones ambientales, tales como temperatura y humedad, deben ser monitorizados para detectar condiciones anormales.	Monitorización	2	5	2,5	1	2,5	B
	Incapacidad para controlar la temperatura y la humedad dentro del centro de datos	Los equipos de control de humedad y temperatura deben mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Administrativas	2	5	2,5	1	2,5	B
	Incapacidad para controlar la entrada de humos venenosos / aire / humo a través de los conductos de aire	El manejo adecuado de apertura / cierre de los conductos de aire durante eventos como vientos fuertes, uso de pesticidas o fuego.	Administrativas	3	5	1,7	1	1,7	B
	Ubicado en una zona de alto nivel sísmico	Las instalaciones deben ubicarse en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	3	5	1,7	1	1,7	B
	Estructura de la construcción y techos de baja calidad	La infraestructura debe ser resistente a terremotos si se encuentra ubicada en una zona de medio o alto nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Administrativas	2	5	2,5	1	2,5	B
	La falta de mecanismos alternos en caso de destrucción total por desastres naturales.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	2	5	2,5	1	2,5	B

Anexo E.2 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Ubicado en una zona de alto nivel sísmico	Las instalaciones deben ubicarse en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	3	5	1,7	1	1,7	B
	Estructura de la construcción y techos de baja calidad	La infraestructura debe ser resistente a terremotos si se encuentra ubicada en una zona de medio o alto nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Administrativas	2	5	2,5	1	2,5	B
	La falta de mecanismos alternos en caso de destrucción total por desastres naturales.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	2	5	2,5	1	2,5	B
Información	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un área propensa a inundaciones.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de pisos elevados.	Se debe implementar protección contra inundaciones.	Minimizadoras	3	5	1,7	1	1,7	B
	Calidad baja en la construcción de los edificios.	La construcción del edificio debe ser resistente a fugas de agua.	Minimizadoras	3	5	1,7	1	1,7	B
	Incapacidad para absorber rayos	Sistemas para rayos y sistemas de polo a tierra	Minimizadoras	3	5	1,7	1	1,7	B
	Sistema de drenaje débil.	Se debe implementar protección en contra de inundaciones y fugas de agua.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de control de temperatura y humedad adecuada	Sistema de monitoreo adecuado para temperatura y humedad	Monitorización	2	5	2,5	1	2,5	B
		Las condiciones ambientales, tales como temperatura y humedad, deben ser monitorizados para detectar condiciones anormales.	Monitorización	2	5	2,5	1	2,5	B

Anexo E.2 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
	Incapacidad para controlar la temperatura y la humedad dentro del centro de datos	Los equipos de control de humedad y temperatura deben mantenerse correctamente para asegurar su continua disponibilidad e integridad.	Administrativas	2	5	2,5	1	2,5	B
	Ubicado en una zona de alto nivel sísmico	Las instalaciones deben ubicarse en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	3	5	1,7	1	1,7	B
	Estructura de la construcción y techos de baja calidad	La infraestructura debe ser resistente a terremotos si se encuentra ubicada en una zona de medio o alto nivel sísmico. Se debe implementar una protección apropiada contra terremotos.	Minimizadoras	3	5	1,7	1	1,7	B
	Ausencia de backup en un lugar diferente o lugar alterno.	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información.	Administrativas	2	5	2,5	1	2,5	B
	La falta de mecanismos alternos en caso de destrucción total por desastres naturales.	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones en los procesos de negocio, junto con la probabilidad y el impacto de estas interrupciones así como sus consecuencias para la seguridad de la información. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos de negocio críticos. Mantener una estructura única de planes de continuidad de negocio para asegurar que todos los planes son consistentes, considerando los requerimientos de seguridad de la información de manera coherente así como identificar las prioridades para pruebas y mantenimiento. Los planes de continuidad de negocio deben ser revisados periódicamente para garantizar su actualización y eficacia.	Administrativas	2	5	2,5	1	2,5	B

Fuente: autores

Anexo E.3 Amenaza Intrusión en la red

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Transaccional aplicación	Acceso no autorizado a información confidencial del sistema transaccional	Validar y hacer los ajustes requeridos en la aplicación web del sitio www.transacional.gov.co, para que siempre exija autenticación a los usuarios y no pueda ser accedida por personal no autorizado desde internet	Prevención	1	5	5,00	3	15,0	E
Calidad.eps.com.co	Php < 5.3.x múltiples vulnerabilidades	Actualizar el sitio web a la versión más reciente y estable disponible de php.	Prevención	1	5	5,00	3	15,0	E
Transaccional aplicación	Servicios de autenticación web a través de protocolos inseguros (http)	Implementar servicios seguros de autenticación web como https, de tal forma que la información confidencial (usuarios y contraseñas) sea transmitida de forma cifrada, impidiendo que puedan ser interceptados y usados por terceros no autorizados.	Prevención	1	5	5,00	3	15,0	E
Mantis				1	5	5,00	3	15,0	E
Hc especialistas aplicación				1	5	5,00	3	15,0	E
Intranet.eps.com.co, eps.com.co				1	5	5,00	3	15,0	E
Intranet.eps.com.co, eps.com.co				1	5	5,00	3	15,0	E
Orfeo.eps.com.co				1	5	5,00	3	15,0	E
Calidad.eps.com.co				1	5	5,00	3	15,0	E
Calidad.eps.com.co	Divulgación de información de php (expose_php)	En el archivo de configuración de php 'php.ini', configurar el valor de para el parámetro 'expose_php' en 'off' para deshabilitar este comportamiento. Finalmente, reiniciar el servicio 'daemon' del servidor web para que este cambio tenga efecto.	Prevención	1	5	5,00	3	15,0	E
Orfeo.eps.com.co				1	5	5,00	3	15,0	E
Orfeo.eps.com.co	Divulgación de información '.svn/entries' por el servidor web	Configure los permisos en el servidor web para denegar el acceso al directorio '.svn'.	Prevención	2	5	2,50	3	7,5	A
Mantis	Página por defecto	Configurar una página de inicio del sitio web en lugar de la página por defecto de iis. Una página de "en construcción" se puede utilizar.	Prevención	1	5	5,00	3	15,0	E
Transaccional aplicación	Cgi generic sql injection	Implementar mecanismos de control para filtrar caracteres peligrosos. Únicamente se debería permitir el ingreso de caracteres válidos tales como: abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz0123456789@.-	Prevención	1	5	5,00	3	15,0	E
Hc especialistas				1	5	5,00	3	15,0	E
Calidad.eps.com.co	Cgi generic xss	Restringir el acceso a la aplicación vulnerable. Póngase en contacto con el proveedor para obtener un parche o actualización	Prevención	1	5	5,00	3	15,0	E
Switch / 10.10.10.6				1	5	5,00	3	15,0	E
Switch / 10.10.10.10				1	5	5,00	3	15,0	E
Switch / 10.10.10.2				1	5	5,00	3	15,0	E
Switch / 10.10.10.12				1	5	5,00	3	15,0	E
Switch / 10.10.10.11				1	5	5,00	3	15,0	E
Switch / 10.10.10.13				1	5	5,00	3	15,0	E
Hc especialistas				1	5	5,00	3	15,0	E
Intranet.eps.com.co, eps.com.co	El certificado ssl no es de confianza	Adquirir un certificado digital de una entidad certificadora abierta, para que cualquier usuario que deba conectarse al servidor pueda confiar en el servicio al cual se está conectando. Si el servicio solo se accede desde la red interna, es posible generar un certificado por una entidad certificadora interna	Prevención	2	5	2,50	3	7,5	A
Calidad.eps.com.co				2	5	2,50	3	7,5	A
Switch / 10.10.10.1				2	5	2,50	3	7,5	A
Switch / 10.10.10.12				2	5	2,50	3	7,5	A
Switch / 10.10.10.13				2	5	2,50	3	7,5	A
Switch / 10.10.10.11				2	5	2,50	3	7,5	A
Transaccional bd				2	5	2,50	3	7,5	A
Hc especialistas base de datos - pruebas				2	5	2,50	3	7,5	A
Hc especialistas aplicación - pruebas				2	5	2,50	3	7,5	A
Hc especialistas				2	5	2,50	3	7,5	A
Transaccional aplicación				2	5	2,50	3	7,5	A

Anexo E.3 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Switch / 10.10.10.10	Certificado ssl expirado.	Genere un nuevo certificado ssl para el servicio.	Prevención	2	5	2,50	3	7,5	A
Switch / 10.10.10.6				2	5	2,50	3	7,5	A
Switch / 10.10.10.5				2	5	2,50	3	7,5	A
Switch / 10.10.10.12				2	5	2,50	3	7,5	A
Switch / 10.10.10.13				2	5	2,50	3	7,5	A
Switch / 10.10.10.11				2	5	2,50	3	7,5	A
Switch / 10.10.10.2				2	5	2,50	3	7,5	A
Switch / 10.10.10.10	Negación de servicio por renegociación de sesiones ssl / tls	Dependiendo del servicio y la implementación de ssl, cada fabricante puede tener un parche para cada servicio.	Prevención	2	5	2,50	3	7,5	A
Switch / 10.10.10.12				2	5	2,50	3	7,5	A
Switch / 10.10.10.13				2	5	2,50	3	7,5	A
Switch / 10.10.10.11				2	5	2,50	3	7,5	A
Switch / 10.10.10.12	Certificado ssl firmado con un algoritmo de hash débil	Reexpida el certificado usando sha-1.	Prevención	2	5	2,50	3	7,5	A
Switch / 10.10.10.13				2	5	2,50	3	7,5	A
Switch / 10.10.10.11				2	5	2,50	3	7,5	A
Switch / 10.10.10.1				2	5	2,50	3	7,5	A
Switch / 10.10.10.12	Soporte en cifrados ssl débiles	Reconfigure el servicio afectado para que no soporte el uso de estos algoritmos.	Prevención	2	5	2,50	3	7,5	A
Switch / 10.10.10.13				2	5	2,50	3	7,5	A
Switch / 10.10.10.11				2	5	2,50	3	7,5	A
Intranet.eps.com.co, eps.com.co	Firmas del protocolo smb deshabilitadas	Evaluar y configurar en los servidores afectados las recomendaciones de firmas smb que se listan en la siguiente web: http://support.microsoft.com/kb/887429	Prevención	2	5	2,50	3	7,5	A
Calidad.eps.com.co				2	5	2,50	3	7,5	A
Transaccional bd				2	5	2,50	3	7,5	A
Hc especialistas base de datos - pruebas				2	5	2,50	3	7,5	A
Hc especialistas aplicación - pruebas				2	5	2,50	3	7,5	A
Hc especialistas				2	5	2,50	3	7,5	A
Transaccional aplicación				2	5	2,50	3	7,5	A
Transaccional bd	Debilidad microsoft windows remote desktop protocol servidor man-in-the-middle	Forzar el uso de ssl como capa de transporte por este servicio si es compatible, y /o seleccione la opción 'permitir sólo las conexiones desde equipos que ejecuten escritorio remoto con autenticación a nivel de red', si está disponible.	Prevención	2	5	2,50	3	7,5	A
hc especialistas base de datos - pruebas				2	5	2,50	3	7,5	A
Transaccional bd	Los servicios de terminal server no utilizan autenticación a nivel de red de autenticación (nla)	Habilitar autenticación a nivel de red (nla) en el servidor rdp remoto. Esto se hace generalmente en la ficha 'remote' de los ajustes del 'sistema' en windows.	Prevención	2	5	2,50	3	7,5	A
hc especialistas base de datos - pruebas				2	5	2,50	3	7,5	A
Transaccional bd	Nivel de cifrado bajo o medio terminal services	Cambie el nivel de cifrado a alto o conforme a federal information processing standards (fips).	Prevención	2	5	2,50	3	7,5	A
hc especialistas base de datos - pruebas				2	5	2,50	3	7,5	A
Switch / 10.10.10.1	Habilitada versión 1 del protocolo ssh	Deshabilitar la versión 1 del protocolo, del servidor ssh.	Prevención	2	5	2,50	3	7,5	A
Orfeo.eps.com.co	El servidor web utiliza texto claro como forma de autenticación	Asegurarse de que todas las formas sensibles de contenido se transmiten a través de https.	Prevención	1	5	5,00	3	15,0	E
Switch / 10.10.10.10				1	5	5,00	3	15,0	E
Switch / 10.10.10.12				1	5	5,00	3	15,0	E
Switch / 10.10.10.13				1	5	5,00	3	15,0	E
Switch / 10.10.10.11				1	5	5,00	3	15,0	E
Hc especialistas aplicación				1	5	5,00	3	15,0	E
Switch / 10.10.10.1	Servidor telnet no cifrado	Deshabilitar este servicio y utilizar ssh en su lugar	Prevención	1	5	5,00	3	15,0	E

Fuente: autores

Anexo E.4 Amenaza Daños por Agua

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware, Información.	Ausencia de pisos elevados.	Se debe implementar protección contra inundaciones.	Minimizadoras	3	5	1,67	1	1,7	B
	Calidad baja en la construcción de los edificios.	La construcción del edificio debe ser resistente a fugas de agua.	Minimizadoras	3	5	1,67	1	1,7	B
	Sistema de drenaje débil.	Se debe implementar protección en contra de inundaciones y fugas de agua.	Minimizadoras	3	5	1,67	1	1,7	B

Fuente: autores

Anexo E.5 Amenaza Robo y Sabotaje

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Falta de protección física.	Perímetros de seguridad (barreras como: paredes, entradas con uso de tarjetas) deben ser usadas para proteger áreas que contienen información y proteger instalaciones que procesan información.	disuasión	3	5	1,67	3	5,0	M
		Las áreas seguras deben estar protegidas apropiadamente por controles que garanticen el acceso de personal autorizado.	prevención	2	5	2,50	3	7,5	A
		Seguridad física debe ser diseñada y aplicada para oficinas, salas, y demás recursos.	disuasión	2	5	2,50	3	7,5	A
		Protección física y directrices deben ser diseñadas y aplicadas para trabajar en áreas seguras.	disuasión	1	5	5,00	3	15,0	E
		Puntos de acceso como áreas de entrega y de carga, en donde personas no autorizadas pueden entrar, deben ser controlados y de ser posible, deben ser aisladas de salas de procesamiento de información, con el fin de evitar accesos no autorizados.	prevención	3	5	1,67	3	5,0	M
		Los usuarios deben garantizar que un equipo no atendido tenga la protección adecuada.	prevención	2	5	2,50	3	7,5	A
	No existe una supervisión del trabajo de personal externo o de limpieza.	Establecer mecanismos de control sobre el personal externo y de aseo, como: Términos y condiciones de seguridad de la información en los contratos cuyo personal acceda a las instalaciones de la EPS Incorporar en el programa de concientización en seguridad un contenido dirigido a personal externo que labora en las instalaciones de la EPS como requerimiento o condicionamiento para el inicio de sus labores.	disuasión	2	5	2,50	3	7,5	A
	Ausencia o insuficiencia de procedimientos para el manejo y almacenamiento de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información para proteger la información contra la divulgación no autorizada o mal uso de la misma.	administración	1	5	5,00	3	15,0	E
		La documentación de los sistemas debe estar protegido contra el acceso no autorizado.	prevención	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Ausencia o insuficiencia de procedimientos para la clasificación de la información.	Todos los activos deben estar claramente identificados y clasificados en un inventario de acuerdo a su importancia. El inventario debe ser actualizado constantemente.	administración	1	5	5,00	3	15,0	E
		Toda la información y los activos asociados con el proceso de información deben poseer un propietario en la entidad.	administración	1	5	5,00	3	15,0	E
	La clasificación de activos es insuficiente.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	administración	1	5	5,00	3	15,0	E
	Etiquetado de información insuficiente	Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por EPS.	administración	2	5	2,50	3	7,5	A
	Existe un inadecuado entendimiento acerca de las implicaciones y consecuencias debido a la divulgación de información confidencial.	Identificar, documentar y revisar regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la EPS para la protección de la información.	administración	1	5	5,00	3	15,0	E
		Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la entidad para la seguridad de la información.	disuasión	2	5	2,50	3	7,5	A
		Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de información.	disuasión	2	5	2,50	3	7,5	A
		El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados.	disuasión	1	5	5,00	3	15,0	E
	Procedimientos inadecuados de contratación de personal.	Se debe realizar pruebas de verificación de los antecedentes sobre todos los candidatos a empleados, contratistas, y usuarios de terceras partes, de acuerdo con las leyes, reglas y éticas pertinentes, y de forma proporcional a los requisitos de negocio, la clasificación de la información a la que se accede, y a los riesgos observados.	disuasión	3	5	1,67	3	5,0	M
	Inadecuada e insegura reutilización o eliminación de los equipos	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.	monitorización	2	5	2,50	3	7,5	A
		El equipo, información o software no debe ser sacado fuera de la Entidad sin autorización.	prevención	3	5	1,67	3	5,0	M
		Debería haber procedimientos para la gestión de los medios informáticos removibles	monitorización	1	5	5,00	3	15,0	E
		Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	monitorización	2	5	2,50	3	7,5	A
	Existe una inadecuada segregación de funciones para asignar accesos físicos.	Implementar una adecuada segregación para las actividades de mantenimiento y administración de tarjetas de identificación y acceso.	administración	2	5	2,50	3	7,5	A
	Medidas inadecuadas cuando el contrato de empleados y personal externo finaliza.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir y comunicar al empleado o contratista.	disuasión	2	5	2,50	3	7,5	A
		Todos los empleados, contratistas y terceros deben retornar todos los activos de la entidad que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.	administración	3	5	1,67	3	5,0	M

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Insuficiente seguridad de los equipos fuera de las instalaciones	Se debe aplicar seguridad a los equipos que se encuentran fuera de las instalaciones de la entidad tomando en cuenta los diversos riesgos a los que se está expuesto.	minimización del impacto / limitación del impacto	1	5	5,00	3	15,0	E
	Ausencia de gestión de incidentes de seguridad.	Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada.	administración	2	5	2,50	3	7,5	A
	Ausencia de procedimientos para el reporte sobre incidentes de seguridad.	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.	administración	1	5	5,00	3	15,0	E
	Insuficiente identificación y definición de las responsabilidades para la gestión de incidentes de seguridad	Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.	administración	1	5	5,00	3	15,0	E
	Insuficiente monitoreo de incidentes de seguridad	Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.	administración	2	5	2,50	3	7,5	A
		Cuando una acción de seguimiento contra una persona u entidad, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.	administración	2	5	2,50	3	7,5	A
	Ausencia de concienciación sobre la seguridad de la información	Todos los empleados de la entidad y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	3	5	1,67	3	5,0	M
	Insuficiente revisión de las políticas de seguridad de la información	La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad.	concienciación	1	5	5,00	3	15,0	E
	Falta de compromiso de la dirección a nivel de seguridad de la información	La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	concienciación	2	5	2,50	3	7,5	A
		La gerencia debe apoyar activamente en la seguridad dentro de la entidad a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de la información.	administración	1	5	5,00	3	15,0	E
		La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la entidad con roles relevantes y funciones de trabajo.	concienciación	1	5	5,00	3	15,0	E
		Deberían definirse claramente las responsabilidades. Incluye la asignación de responsables de los activos de información.	administración	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Falta de protección física.	Perímetros de seguridad (barreras como: paredes, entradas con uso de tarjetas) deben ser usadas para proteger áreas que contienen información y proteger instalaciones que procesan información.	disuasión	3	5	1,67	3	5,0	M
		Las áreas seguras deben estar protegidas apropiadamente por controles que garanticen el acceso de personal autorizado.	prevención	2	5	2,50	3	7,5	A
		Seguridad física debe ser diseñada y aplicada para oficinas, salas, y demás recursos.	disuasión	2	5	2,50	3	7,5	A
		Protección física y directrices deben ser diseñadas y aplicadas para trabajar en áreas seguras.	disuasión	1	5	5,00	3	15,0	E
		Puntos de acceso como áreas de entrega y de carga, en donde personas no autorizadas pueden entrar, deben ser controlados y de ser posible, deben ser aisladas de salas de procesamiento de información, con el fin de evitar accesos no autorizados.	prevención	3	5	1,67	3	5,0	M
		Los usuarios deben garantizar que un equipo no atendido tenga la protección adecuada.	prevención	2	5	2,50	3	7,5	A
	No existe una supervisión del trabajo de personal externo o de limpieza.	Establecer mecanismos de control sobre el personal externo y de aseo, como: Términos y condiciones de seguridad de la información en los contratos cuyo personal acceda a las instalaciones de la EPS Incorporar en el programa de concientización en seguridad un contenido dirigido a personal externo que labora en las instalaciones de la EPS como requerimiento o condicionamiento para el inicio de sus labores.	disuasión	2	5	2,50	3	7,5	A
	Ausencia o insuficiencia de procedimientos para el manejo y almacenamiento de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información para proteger la información contra la divulgación no autorizada o mal uso de la misma.	administración	1	5	5,00	3	15,0	E
		La documentación de los sistemas debe estar protegido contra el acceso no autorizado.	prevención	2	5	2,50	3	7,5	A
	Ausencia o insuficiencia de procedimientos para la clasificación de la información.	Todos los activos deben estar claramente identificados y clasificados en un inventario de acuerdo a su importancia. El inventario debe ser actualizado constantemente.	administración	1	5	5,00	3	15,0	E
		Toda la información y los activos asociados con el proceso de información deben poseer un propietario en la entidad.	administración	1	5	5,00	3	15,0	E
	La clasificación de activos es insuficiente.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	administración	1	5	5,00	3	15,0	E
	Etiquetado de información insuficiente	Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por EPS.	administración	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Existe un inadecuado entendimiento acerca de las implicaciones y consecuencias debido a la divulgación de información confidencial.	Identificar, documentar y revisar regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la EPS para la protección de la información.	administración	1	5	5,00	3	15,0	E
		Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la entidad para la seguridad de la información.	disuasión	2	5	2,50	3	7,5	A
		Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de información.	disuasión	2	5	2,50	3	7,5	A
		El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados.	disuasión	1	5	5,00	3	15,0	E
	Procedimientos inadecuados de contratación de personal.	Se debe realizar pruebas de verificación de los antecedentes sobre todos los candidatos a empleados, contratistas, y usuarios de terceras partes, de acuerdo con las leyes, reglas y éticas pertinentes, y de forma proporcional a los requisitos de negocio, la clasificación de la información a la que se accede, y a los riesgos observados.	disuasión	3	5	1,67	3	5,0	M
	Inadecuada e insegura reutilización o eliminación de los equipos	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.	monitorización	2	5	2,50	3	7,5	A
		El equipo, información o software no debe ser sacado fuera de la Entidad sin autorización.	prevención	3	5	1,67	3	5,0	M
		Debería haber procedimientos para la gestión de los medios informáticos removibles	monitorización	1	5	5,00	3	15,0	E
		Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	monitorización	2	5	2,50	3	7,5	A
	Existe una inadecuada segregación de funciones para asignar accesos físicos.	Implementar una adecuada segregación para las actividades de mantenimiento y administración de tarjetas de identificación y acceso.	administración	2	5	2,50	3	7,5	A
	Medidas inadecuadas cuando el contrato de empleados y personal externo finaliza.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir y comunicar al empleado o contratista.	disuasión	2	5	2,50	3	7,5	A
		Todos los empleados, contratistas y terceros deben retornar todos los activos de la entidad que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.	administración	3	5	1,67	3	5,0	M
	Insuficiente seguridad de los equipos fuera de las instalaciones	Se debe aplicar seguridad a los equipos que se encuentran fuera de las instalaciones de la entidad tomando en cuenta los diversos riesgos a los que se está expuesto.	minimización del impacto / limitación del impacto	1	5	5,00	3	15,0	E
	Ausencia de gestión de incidentes de seguridad.	Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada.	administración	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Ausencia de procedimientos para el reporte sobre incidentes de seguridad.	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.	administración	1	5	5,00	3	15,0	E
	Insuficiente identificación y definición de las responsabilidades para la gestión de incidentes de seguridad	Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.	administración	1	5	5,00	3	15,0	E
	Insuficiente monitoreo de incidentes de seguridad	Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.	administración	2	5	2,50	3	7,5	A
		Cuando una acción de seguimiento contra una persona u entidad, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.	administración	2	5	2,50	3	7,5	A
	Ausencia de políticas de seguridad y procedimientos completos cuando se trata de partes externas, clientes y terceros.	Los riesgos a la información de la entidad y a las instalaciones del procesamiento de información desde los procesos del negocio que impliquen a terceros deben ser identificados y se debe implementar controles apropiados antes de conceder el acceso.	prevención	2	5	2,50	3	7,5	A
		Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activos de la entidad.	prevención	2	5	2,50	3	7,5	A
	Ausencia de concienciación sobre la seguridad de la información	Todos los empleados de la entidad y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	3	5	1,67	3	5,0	M
	Insuficiente revisión de las políticas de seguridad de la información	La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad.	concienciación	1	5	5,00	3	15,0	E
	Falta de compromiso de la dirección a nivel de seguridad de la información	La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	concienciación	2	5	2,50	3	7,5	A
		La gerencia debe apoyar activamente en la seguridad dentro de la entidad a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de la información.	administración	1	5	5,00	3	15,0	E
		La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la entidad con roles relevantes y funciones de trabajo.	concienciación	1	5	5,00	3	15,0	E
		Deberían definirse claramente las responsabilidades. Incluye la asignación de responsables de los activos de información.	administración	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Falta de protección física.	Perímetros de seguridad (barreras como: paredes, entradas con uso de tarjetas) deben ser usadas para proteger áreas que contienen información y proteger instalaciones que procesan información.	disuasión	3	5	1,67	3	5,0	M
		Las áreas seguras deben estar protegidas apropiadamente por controles que garanticen el acceso de personal autorizado.	prevención	2	5	2,50	3	7,5	A
		Seguridad física debe ser diseñada y aplicada para oficinas, salas, y demás recursos.	disuasión	2	5	2,50	3	7,5	A
		Protección física y directrices deben ser diseñadas y aplicadas para trabajar en áreas seguras.	disuasión	1	5	5,00	3	15,0	E
		Puntos de acceso como áreas de entrega y de carga, en donde personas no autorizadas pueden entrar, deben ser controlados y de ser posible, deben ser aisladas de salas de procesamiento de información, con el fin de evitar accesos no autorizados.	prevención	3	5	1,67	3	5,0	M
		Los usuarios deben garantizar que un equipo no atendido tenga la protección adecuada.	prevención	2	5	2,50	3	7,5	A
	No existe una supervisión del trabajo de personal externo o de limpieza.	Establecer mecanismos de control sobre el personal externo y de aseo, como: Términos y condiciones de seguridad de la información en los contratos cuyo personal acceda a las instalaciones de la EPS Incorporar en el programa de concientización en seguridad un contenido dirigido a personal externo que labora en las instalaciones de la EPS como requerimiento o condicionamiento para el inicio de sus labores.	disuasión	2	5	2,50	3	7,5	A
	Ausencia o insuficiencia de procedimientos para el manejo y almacenamiento de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información para proteger la información contra la divulgación no autorizada o mal uso de la misma.	administración	1	5	5,00	3	15,0	E
		La documentación de los sistemas debe estar protegido contra el acceso no autorizado.	prevención	2	5	2,50	3	7,5	A
	Ausencia o insuficiencia de procedimientos para la clasificación de la información.	Todos los activos deben estar claramente identificados y clasificados en un inventario de acuerdo a su importancia. El inventario debe ser actualizado constantemente.	administración	1	5	5,00	3	15,0	E
		Toda la información y los activos asociados con el proceso de información deben poseer un propietario en la entidad.	administración	1	5	5,00	3	15,0	E
	La clasificación de activos es insuficiente.	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	administración	1	5	5,00	3	15,0	E
	Etiquetado de información insuficiente	Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por EPS.	administración	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Existe un inadecuado entendimiento acerca de las implicaciones y consecuencias debido a la divulgación de información confidencial.	Identificar, documentar y revisar regularmente los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la EPS para la protección de la información.	administración	1	5	5,00	3	15,0	E
		Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la entidad para la seguridad de la información.	disuasión	2	5	2,50	3	7,5	A
		Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de información.	disuasión	2	5	2,50	3	7,5	A
		El personal debe ser disuadido de utilizar los recursos de tratamiento de la información para propósitos no autorizados.	disuasión	1	5	5,00	3	15,0	E
	Procedimientos inadecuados de contratación de personal.	Se debe realizar pruebas de verificación de los antecedentes sobre todos los candidatos a empleados, contratistas, y usuarios de terceras partes, de acuerdo con las leyes, reglas y éticas pertinentes, y de forma proporcional a los requisitos de negocio, la clasificación de la información a la que se accede, y a los riesgos observados.	disuasión	3	5	1,67	3	5,0	M
	Inadecuada e insegura reutilización o eliminación de los equipos	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.	monitorización	2	5	2,50	3	7,5	A
		El equipo, información o software no debe ser sacado fuera de la Entidad sin autorización.	prevención	3	5	1,67	3	5,0	M
		Debería haber procedimientos para la gestión de los medios informáticos removibles	monitorización	1	5	5,00	3	15,0	E
		Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	monitorización	2	5	2,50	3	7,5	A
	Existe una inadecuada segregación de funciones para asignar accesos físicos.	Implementar una adecuada segregación para las actividades de mantenimiento y administración de tarjetas de identificación y acceso.	administración	2	5	2,50	3	7,5	A
	Medidas inadecuadas cuando el contrato de empleados y personal externo finaliza.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir y comunicar al empleado o contratista.	disuasión	2	5	2,50	3	7,5	A
		Todos los empleados, contratistas y terceros deben retornar todos los activos de la entidad que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.	administración	3	5	1,67	3	5,0	M
	Inadecuado retiro de los derechos de acceso cuando el contrato de empleados y personal externo finaliza.	Los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información deben ser removidos hasta la culminación del empleo, contrato o acuerdo, o debe ser ajustada en caso de cambio.	disuasión	2	5	2,50	3	7,5	A

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Ausencia o inadecuados mecanismos de prevención de fuga de información.	Se deberían establecer políticas, procedimientos y controles formales de intercambio de información con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación.	disuasión	2	5	2,50	3	7,5	A
		La información implicada con la mensajería electrónica debe ser protegida apropiadamente.	monitorización	3	5	1,67	3	5,0	M
		Las oportunidades de fuga de información deben ser prevenidas.	monitorización	1	5	5,00	3	15,0	E
	Ausencia de controles para el control de dispositivos móviles	Se debería adoptar una política y unas medidas de seguridad de soporte, para gestionar el uso de dispositivos móviles.	disuasión	1	5	5,00	3	15,0	E
	Insuficiente seguridad de los equipos fuera de las instalaciones	Se debe aplicar seguridad a los equipos que se encuentran fuera de las instalaciones de la entidad tomando en cuenta los diversos riesgos a los que se está expuesto.	minimización del impacto / limitación del impacto	1	5	5,00	3	15,0	E
	Ausencia de gestión de incidentes de seguridad.	Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada.	administración	2	5	2,50	3	7,5	A
	Ausencia de procedimientos para el reporte sobre incidentes de seguridad.	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.	administración	1	5	5,00	3	15,0	E
	Insuficiente identificación y definición de las responsabilidades para la gestión de incidentes de seguridad	Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información.	administración	1	5	5,00	3	15,0	E
	Insuficiente monitoreo de incidentes de seguridad	Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.	administración	2	5	2,50	3	7,5	A
		Cuando una acción de seguimiento contra una persona u entidad, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.	administración	2	5	2,50	3	7,5	A
	Ausencia de políticas de seguridad y procedimientos completos cuando se trata de partes externas, clientes y terceros.	Los riesgos a la información de la entidad y a las instalaciones del procesamiento de información desde los procesos del negocio que impliquen a terceros deben ser identificados y se debe implementar controles apropiados antes de conceder el acceso.	prevención	2	5	2,50	3	7,5	A
		Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activos de la entidad.	prevención	2	5	2,50	3	7,5	A
		Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la entidad o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, debe cubrir todos los requisitos de seguridad relevantes.	disuasión	2	5	2,50	3	7,5	A
		Los acuerdos deben ser establecidos para el intercambio de información y software entre la entidad y terceros.	disuasión	1	5	5,00	3	15,0	E
		Los medios que almacenan información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la Entidad.	prevención	1	5	5,00	3	15,0	E

Anexo E.5 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Ausencia de protección para la información transmitida a través de comercio electrónico	La información envuelta en el comercio electrónico pasando a través de redes públicas, debe ser protegida de actividad fraudulenta, disputas de contratos y de acceso y modificación no autorizada.	prevención	3	5	1,67	3	5,0	M
		Se debe proteger la información implicada en transacciones en línea para evitar transmisiones incompletas, enrutamiento erróneo, alteración no autorizada de mensajes, divulgación no autorizada, reproducción o duplicación no autorizada de mensajes.	prevención	2	5	2,50	3	7,5	A
		La integridad de la información que se ha hecho disponible en un sistema público debe ser protegido para prevenir modificaciones no autorizadas.	prevención	3	5	1,67	3	5,0	M
	Insuficiente protección a los registros de los sistemas (Logs)	Las herramientas de registro y los registros de información deben estar protegidos contra la manipulación y acceso no autorizado.	prevención	2	5	2,50	3	7,5	A
	Ausencia de concienciación sobre la seguridad de la información	Todos los empleados de la entidad y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	3	5	1,67	3	5,0	M
	Insuficiente revisión de las políticas de seguridad de la información	La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad.	concienciación	1	5	5,00	3	15,0	E
	Falta de compromiso de la dirección a nivel de seguridad de la información	La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	concienciación	2	5	2,50	3	7,5	A
		La gerencia debe apoyar activamente en la seguridad dentro de la entidad a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de la información.	administración	1	5	5,00	3	15,0	E
		La información de las actividades de seguridad deben ser coordinadas por representantes de diferentes partes de la entidad con roles relevantes y funciones de trabajo.	concienciación	1	5	5,00	3	15,0	E
		Deben definirse claramente las responsabilidades. Incluye la asignación de responsables de los activos de información.	administración	2	5	2,50	3	7,5	A
	Inexistencia del proceso de sanatización en un ambiente de prueba de datos	Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.	monitorización	1	5	5,00	3	15,0	E

Fuente: autores

Anexo E.6 Amenaza Mal Uso del Software

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Falta de documentación para procedimientos operativos.	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.	administración	2	4	2,00	2	4,0	B
Software	Falta de medidas de restricción contra acceso no autorizado	Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	prevención	2	4	2,00	2	4,0	B
		Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados).	prevención	2	4	2,00	2	4,0	B
	Ausencia de conciencia de seguridad	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	1	4	4,00	2	8,0	A
	Insuficiente capacitación a los usuarios			1	4	4,00	2	8,0	A
	Transferencia/almacenamiento de contraseñas en texto claro	La asignación de contraseñas debe controlarse a través de un proceso de gestión formal. Las contraseñas temporales se deben entregar a los usuarios de forma segura. Se debe evitar el uso de mensajes electrónicos desprotegidos (texto sin cifrar). Las contraseñas nunca deben ser almacenadas en sistemas informáticos de forma desprotegida.	administración	2	4	2,00	2	4,0	B
	Ausencia de controles para la instalación de software	Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales.	administración	3	4	1,33	2	2,7	B
	Ausencia de control de accesos al código fuente de las aplicaciones	El acceso a los códigos de programas fuente debe ser restringido.	prevención	2	4	2,00	2	4,0	B
	Falta de mecanismos de monitoreo y supervisión periódicos.	Los procedimientos para el uso y el monitoreo de las instalaciones de procesamiento de información deben ser establecidos. Los resultados de las actividades de monitoreo deben ser revisadas regularmente.	administración	3	4	1,33	2	2,7	B
	Insuficiente auditoría sobre las operaciones de los administradores	Las actividades del administrador y de los operadores del sistema deben ser registradas.	prevención	1	4	4,00	2	8,0	A
	Ausencia de controles para el cierre o bloqueo de sesión de usuario o del sistema.	Las sesiones se deberían desactivar tras un periodo definido de inactividad.	prevención	2	4	2,00	2	4,0	B
	Daño en la integridad de la información registrada en los sistemas de información.	Se deberían incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados. Como un control preventivo se debería instalar y actualizar herramientas para la detección de código y software malicioso.	monitorización	2	4	2,00	2	4,0	B
	Falta de documentación para procedimientos operativos.	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.	administración	2	4	2,00	2	4,0	B
	Software de monitoreo insuficiente para prevenir los accesos no autorizados así como el acceso a información sensible	La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restringa y se mantenga fuertemente controlado.	monitorización	2	4	2,00	2	4,0	B
	Cambios no autorizados en los paquetes de software	No se recomiendan modificaciones a los paquetes de software. Se debería limitar a cambios necesarios y todos estos deben ser estrictamente controlados.	prevención	1	4	4,00	2	8,0	A

Anexo E.6 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Procedimientos insuficientes para verificar el cumplimiento de las políticas y estándares de seguridad.	Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.	administración	2	4	2,00	2	4,0	B
		Se debería comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información.	monitorización	1	4	4,00	2	8,0	A
	Ausencia de mecanismos de control y política de uso de software de almacenamiento en la nube.	Se debería definir y comunicar la política para la transferencia segura de información del negocio entre la organización y las partes externas (Google, Dropbox, OneDrive)	concienciación		4	4,00	2	8,0	A
	Procedimientos insuficientes para la auditoría de controles en los sistemas de información.	Se deberían planificar cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.	administración	3	4	1,33	2	2,7	B
		Se deberían proteger los accesos a las herramientas de auditoría de sistemas con el fin de prever cualquier posible mal uso o daño.	monitorización	3	4	1,33	2	2,7	B
	Falta de documentación para procedimientos operativos.	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.	administración	2	4	2,00	2	4,0	B
	Software de monitoreo insuficiente para prevenir los accesos no autorizados así como el acceso a información sensible	La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restringa y se mantenga fuertemente controlado.	monitorización	2	4	2,00	2	4,0	B
	Cambios no autorizados en los paquetes de software	No se recomiendan modificaciones a los paquetes de software. Se debería limitar a cambios necesarios y todos estos deben ser estrictamente controlados.	prevención	1	4	4,00	2	8,0	A

Fuente: autores

Anexo E.7 Amenaza Fallas en Infraestructura y Redes

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Ausencia de procesos de autorización	Debería establecerse un proceso de autorización cuando se va a realizar la instalación de un nuevo recurso en los centros de tratamiento de la información.	administración	2	3	1,50	3	4,5	M
	La falta de procedimientos formales para la gestión de cambios de terceros.	Los cambios en la provisión de servicios (incluido el mantenimiento y mejoras de las políticas, procedimientos y controles de seguridad de la información) teniendo en cuenta la criticidad de los sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos	administración	2	3	1,50	3	4,5	M
	Sistema sobrecargados / planificación de la capacidad inadecuada	Se monitoriza y ajusta el uso de recursos, y se hacen pronósticos de los requisitos de capacidad futuros, para asegurar las prestaciones requeridas del sistema	monitorización	1	3	3,00	3	9,0	A
	Baja calidad en los equipos de hardware	Establecer requerimientos de la entidad para nuevos sistemas de información o para la mejora de los ya existentes, que especifiquen los controles de seguridad requeridos.	administración	2	3	1,50	3	4,5	M
	Uso de periféricos y repuestos incompatibles			1	3	3,00	3	9,0	A

Anexo E.7 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Ausencia de monitoreo regular	Se debe asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluida en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa. Se recomienda realizar informes periódicos según la norma internacional ISAE 3402 para el control de servicios de terceros.	monitorización	2	3	1,50	3	4,5	M
	Ausencia de sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo	prevención	2	3	1,50	3	4,5	M
	Debilidades en las medidas de restricción de acceso no autorizado (física y lógica)	Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	prevención	1	3	3,00	3	9,0	A
	Ausencia de equipos adecuados para la protección de fallas de energía	Se deberían proteger los equipos contra fallos de energía u otras anomalías eléctricas a través de los equipos de apoyo.	prevención	2	3	1,50	3	4,5	M
	Ausencia de medidas adecuadas para el control de la temperatura y humedad	El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.	minimización del impacto / limitación del impacto	2	3	1,50	3	4,5	M
	Ineficaz / insuficiente formación de los usuarios	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	1	3	3,00	3	9,0	A
	Líneas de comunicación desprotegidas	Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.	prevención	3	3	1,00	3	3,0	B
	Uniones incorrectas del cableado e insuficiente seguridad para el cableado			3	3	1,00	3	3,0	B
	Inadecuada seguridad de la red	Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito.	prevención	3	3	1,00	3	3,0	B
	Ausencia de mantenimiento periódico	Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.	prevención	3	3	1,00	3	3,0	B
	La falta de soporte del proveedor adecuado	Mantener con el proveedores adecuados contratos de soporte y mantenimiento	administración	3	3	1,00	3	3,0	B
	Falta de proveedores expertos	La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.	administración	2	3	1,50	3	4,5	M
	Fallas de los proveedores			2	3	1,50	3	4,5	M
	Un único punto de fallo en la arquitectura, ausencia de disponibilidad de enlaces de respaldo	La incorporación de redundancia en la red, hacer uso de los servicios públicos (energía y las líneas de comunicación locales) de más de una fuente / proveedor de servicios	prevención	2	3	1,50	3	4,5	M

Anexo E.7 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Ausencia de procesos de autorización	Debería establecerse un proceso de autorización cuando se va a realizar la instalación de un nuevo recurso en los centros de tratamiento de la información.	administración	2	3	1,50	3	4,5	M
	La falta de procedimientos formales para la gestión de cambios de terceros.	Los cambios en la provisión de servicios (incluido el mantenimiento y mejoras de las políticas, procedimientos y controles de seguridad de la información) teniendo en cuenta la criticidad de los sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos	administración	2	3	1,50	3	4,5	M
	Ausencia de una metodología adecuada de desarrollo de software	La introducción de nuevos sistemas y cambios importantes en los sistemas existentes deberían seguir un proceso formal de la documentación, especificaciones, pruebas, control de calidad y gestión de la implementación.	administración	2	3	1,50	3	4,5	M
		Outsourcing de desarrollo de software deben ser supervisados y controlados por la entidad.	monitorización	2	3	1,50	3	4,5	M
	Ausencia de pruebas de aceptación	Establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones así como las pruebas adecuadas del sistema (s) llevadas a cabo durante el desarrollo y antes de su aceptación.	administración	1	3	3,00	3	9,0	A
	Instalaciones y configuraciones defectuosas	Se debe asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluida en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.	prevención	3	3	1,00	3	3,0	B
	Ausencia de monitoreo regular	Se debe asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluida en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa. Se recomienda realizar informes periódicos según la norma internacional ISAE 3402 para el control de servicios de terceros.	monitorización	2	3	1,50	3	4,5	M
	Ausencia de sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo	prevención	2	3	1,50	3	4,5	M
	Debilidades en las medidas de restricción de acceso no autorizado (física y lógica)	Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	prevención	1	3	3,00	3	9,0	A
	La falta de soporte del proveedor adecuado	Mantener con el proveedores adecuados contratos de soporte y mantenimiento	administración	3	3	1,00	3	3,0	B
	Falta de proveedores expertos	La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.	administración	2	3	1,50	3	4,5	M
	Fallas de los proveedores			2	3	1,50	3	4,5	M
	Un único punto de fallo en la arquitectura, ausencia de disponibilidad de enlaces de respaldo	La incorporación de redundancia en la red, hacer uso de los servicios públicos (energía y las líneas de comunicación locales) de más de una fuente / proveedor de servicios	prevención	2	3	1,50	3	4,5	M

Anexo E.7 (Continuación)

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Ausencia de procesos de autorización	Debería establecerse un proceso de autorización cuando se va a realizar la instalación de un nuevo recurso en los centros de tratamiento de la información.	administración	2	4	2,00	3	6,0	M
	La falta de procedimientos formales para la gestión de cambios de terceros.	Los cambios en la provisión de servicios (incluido el mantenimiento y mejoras de las políticas, procedimientos y controles de seguridad de la información) teniendo en cuenta la criticidad de los sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos	administración	2	4	2,00	3	6,0	M
	Ausencia de monitoreo regular	Se debe asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluida en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa. Se recomienda realizar informes periódicos según la norma internacional ISAE 3402 para el control de servicios de terceros.	monitorización	2	4	2,00	3	6,0	M
	Líneas de comunicación desprotegidas	Se debería proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.	prevención	3	4	1,33	3	4,0	B
	Uniones incorrectas del cableado e insuficiente seguridad para el cableado			3	4	1,33	3	4,0	B
	Inadecuada seguridad de la red	Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito.	prevención	3	4	1,33	3	4,0	B
	La falta de soporte del proveedor adecuado	Mantener con el proveedores adecuados contratos de soporte y mantenimiento	administración	3	4	1,33	3	4,0	B
	Falta de proveedores expertos	La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.	administración	2	4	2,00	3	6,0	M
	Fallas de los proveedores			2	4	2,00	3	6,0	M
	Un único punto de fallo en la arquitectura, ausencia de disponibilidad de enlaces de respaldo	La incorporación de redundancia en la red, hacer uso de los servicios públicos (energía y las líneas de comunicación locales) de más de una fuente / proveedor de servicios	prevención	2	4	2,00	3	6,0	M

Fuente: autores

Anexo E.8 Amenaza Errores Humanos

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Información	Insuficiente definición de roles y responsabilidades en materia de seguridad de la información	Las funciones y responsabilidades de los empleados, contratistas y terceros deben ser definidas y documentadas en concordancia con la política de seguridad de la organización.	Administración	2	3	1,50	2	3,0	B
	La ausencia o ineficacia / insuficiente capacitación de los usuarios	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	1	3	3,00	2	6,0	M
Hardware	La ausencia o ineficacia / insuficiente capacitación de los usuarios	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	concienciación	1	3	3,00	2	6,0	M

Fuente: autores

Anexo E.9 Amenaza Terrorismo

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Disturbios civiles	Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.	Prevención	3	5	1,67	1	1,7	B
	Insuficiente conocimiento de las autoridades correspondientes.	Deben ser mantenidos contactos apropiados con autoridades relevantes.	Administración	3	5	1,67	1	1,7	B
Software	Disturbios civiles	Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.	Prevención	3	2	0,67	1	0,7	B
	Insuficiente conocimiento de las autoridades correspondientes.	Deben ser mantenidos contactos apropiados con autoridades relevantes.	Administración	3	2	0,67	1	0,7	B
Información	Disturbios civiles	Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.	Prevención	3	4	1,33	1	1,3	B
	Insuficiente conocimiento de las autoridades correspondientes.	Deben ser mantenidos contactos apropiados con autoridades relevantes.	Administración	3	4	1,33	1	1,3	B

Fuente: autores

Anexo E.10 Amenaza Legal

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Software	Comprensión insuficiente de las nuevas leyes y reglamentos y la identificación de la legislación aplicable	Se debería establecer política de tratamiento de la información de alojada en el registro nacional de base de datos fundamentado con el Decreto 886 de 2014	Administración	1	4	4,00	3	12,0	E
		Se deberían definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información. Se debería establecer política de cumplimiento de la Ley 1712 de 2014 para la transparencia y acceso a la información pública nacional.	Administración	2	4	2,00	3	6,0	M
	Procedimiento insuficiente para el cumplimiento de los requisitos de propiedad intelectual	Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.	Administración	2	4	2,00	3	6,0	M
	Protección insuficiente de los registros de la organización	Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio	Recuperación	2	4	2,00	3	6,0	M
	Insuficiente protección y privacidad de información personal	La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales. Se debería implementar una política de protección de datos en base a la Ley 1581 de 2012 y el decreto 1377 de 2013.	Administración	1	4	4,00	3	12,0	E
	Reglamento de los controles criptográficos	Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.	Prevención	1	4	4,00	3	12,0	E
Información	Comprensión insuficiente de las nuevas leyes y reglamentos y la identificación de la legislación aplicable	Se debería establecer política de tratamiento de la información de alojada en el registro nacional de base de datos fundamentado con el Decreto 886 de 2014	Administración	1	4	4,00	3	12,0	E
		Se deberían definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información. Se debería establecer política de cumplimiento de la Ley 1712 de 2014 para la transparencia y acceso a la información pública nacional.	Administración	2	4	2,00	3	6,0	M
	Procedimiento insuficiente para el cumplimiento de los requisitos de propiedad intelectual	Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.	Administración	2	4	2,00	3	6,0	M
	Protección insuficiente de los registros de la organización	Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio	Recuperación	2	4	2,00	3	6,0	M
	Insuficiente protección y privacidad de información personal	La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales. Se debería implementar una política de protección de datos en base a la Ley 1581 de 2012 y el decreto 1377 de 2013.	Administración	1	4	4,00	3	12,0	E
	Reglamento de los controles criptográficos	Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.	Prevención	1	4	4,00	3	12,0	E

Fuente: autores