AUTORES	**EDUARDO ANDRES OSPINO MORON**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS**
DIRECTOR	**Esp. MAGRETH ROSSIO SANGUINO REYES**
TÍTULO DE LA TESIS	**AUDITORIA AL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013**

RESUMEN

(70 palabras aproximadamente)

EL PRESENTE PROYECTO DE PASANTÍA SURGE A PARTIR DE LA NECESIDAD Y OBSERVACIÓN REALIZADA EN LA E.S.E.- HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA, CUYOS ACTIVOS SON DE GRAN IMPORTANCIA, LOS CUALES SE MANTIENEN EN CONDICIONES POCO CONFIABLES, YA QUE NO CUENTAN CON LAS POLÍTICAS, PROCEDIMIENTOS, MANUALES, PLANES DE CONTINGENCIAS, ETC.

LA AUDITORÍA REALIZADA SE ENFOCÓ EN LA EVALUACIÓN A LA SEGURIDAD LÓGICA DEL SISTEMA DE INFORMACIÓN ADMINISTRATIVO Y HOSPITALARIO MYPROCESS, BAJO EL ESTÁNDAR ISO/IEC: 27002 DEL 2013.

CARACTERÍSTICAS

PÁGINAS: 97	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

AUDITORÍA AL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

EDUARDO ANDRES OSPINO MORON

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERIA DE SISTEMAS
OCAÑA
2015

AUDITORÍA AL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

EDUARDO ANDRES OSPINO MORON

Trabajo de grado modalidad pasantía presentado para obtener el título de Ingeniero de Sistemas

Directora
Ingeniera Esp. MAGRETH ROSSIO SANGUINO REYES

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERA DE SISTEMAS
OCAÑA
2015

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El presente proyecto de pasantía surge a partir de la necesidad y observación realizada en la E.S.E.- Hospital Emiro Quintero Cañizares de Ocaña, cuyos activos son de gran importancia, en este caso la información, base de datos, dispositivos de red, sistemas de información, aplicaciones etc., se mantienen en condiciones poco confiables, ya que no cuentan con las políticas, procedimientos, manuales, planes de contingencias formales para el resguardo de la información y la protección de la misma. La auditoría realizada se enfocó en la evaluación a la seguridad lógica del sistema de información administrativo y hospitalario myProcess, bajo el estándar ISO/IEC: 27002 del 2013, evaluando los siguientes dominios: control de acceso, seguridad en la operativa y algunos ítems de adquisición, desarrollo y mantenimiento de sistemas de información.

INTRODUCCIÓN

El propósito de este informe es la realización del trabajo de grado modalidad pasantía, desarrollada en la E.S.E Hospital Emiro Quintero Cañizares, donde se identificó la necesidad de realizar una auditoría al sistema de información administrativo y hospitalario myProcess, bajo el estándar ISO 27002/2013.

Si se tiene en cuenta que la información es uno de los activos más importantes de la Empresa, y que la infraestructura informática (hardware, software y elementos complementarios) son indispensables para mantener un adecuado almacenamiento de la información o datos críticos para prestar un servicio con calidad a los usuarios, se crea la necesidad de realizar un análisis de los posibles riesgos y diagnóstico del sistema de información que permitan cumplir e implementar el código de buenas prácticas como lo es la ISO 27002 del 2013 el cual es una guía para el mejoramiento de la seguridad de la información.

Por tanto es de vital importancia mantener el control, políticas, y procedimientos que proporcionen un nivel seguridad de la información con menos riegos de ataques informáticos, robo de información, y demás delitos informáticos que afectan a cualquier sistema de información.

La auditoría realizada al sistema de información mencionado contribuirá al logro de metas y objetivos de la Empresa mejorando la imagen y credibilidad del Hospital Emiro Quintero Cañizares, donde los usuarios que manejan el sistema y los que se benefician de él se sientan respaldados con la seguridad de la información.

AUDITORIA AL SISTEMA DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

1.1. DESCRIPCIÓN DE LA EMPRESA.

E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES (HEQC)

La Empresa Social del Estado Hospital Emiro Quintero Cañizares es una institución de larga trayectoria y experiencia demostrada en toda la Provincia de Ocaña. Se consolida como institución de primer y segundo nivel de complejidad para brindar los servicios de salud a la población vinculada, subsidiada, contributiva y regímenes especiales.
Gracias a su actual infraestructura cuenta con cómodas instalaciones físicas garantizando un ambiente agradable y personal altamente calificado para ofrecer calidad y oportunidad[1].

RESEÑA HISTORICA

Nuevamente al igual que con la fundación de Ocaña, la Ciudad de Pamplona jugó un papel muy importante en materia de salud con la fundación del primer Hospital denominado SAN JUAN DE DIOS, en 1622 en la ciudad de Pamplona, por la comunidad de los hermanos de San Juan de Dios, se hace necesario fundar uno en la Ciudad de Ocaña, es así que desde Pamplona, se trasladan seis (6) religiosos en el año 1645 y fundan un hospital manicomio que además prestaba los servicios en Medicina General, dicho centro hospitalario funcionó poco tiempo en una casa ubicada en el Barrio San Agustín cerca al convento de la capilla de San Sebastián; este Hospital se terminó debido a las guerras de la época y a la expulsión de los religiosos de la Nueva Granada.

Luego a Mediados del siglo XVIII, se fundó una clínica que también funcionó en el barrio San Agustín, más concretamente en la casa de los COLOBON, donde funcionaba la panadería la INSUPERABLE, y quién fuera propietario el controvertido presbítero padre BUZETA.

En el año 1888 llegó a Ocaña, el pavoroso azote de la FIEBRE AMARILLA, dejando la ciudad reducida a menos de su tercera parte; ante esta epidemia y desolación y ante la ausencia de una Institución Hospitalaria, mediante Decreto Eclesiástico No, 203 de 1890 emanado de la Diócesis de Santa Marta se autorizaba al Párroco RAFAEL CELEDÓN de la parroquia de Santa Ana de Ocaña, la creación del Hospital de Caridad SANTA ANA DE OCAÑA, con escritura pública No. 445 del 25 de julio de 1890, el cual inició labores el 1°

[1] E.S.E Hospital Emiro Quintero Cañizares Ocaña N. De S. Información Corporativa (presentación [En línea]. <http://www.hospitaleqc.gov.co/plataforma-estrategica/reseña-historica.html> [citado el 08 de marzo de 2012]

de febrero de 1891 en el sitio denominado "El Llano de Echávez".
La Resolución No. 06 del 16 de marzo de 1937 del Consejo Municipal de Ocaña, cambia su nombre por el del Hospital Civil de Ocaña y faculta al Director del mismo. La Resolución Ejecutiva No.90 del 18 de septiembre de 1939, le concede Personería Jurídica.
Desde diciembre de 1955, ofrece sus servicios en el local donde actualmente funciona, adoptando el nombre de HOSPITAL EMIRO QUINTERO CAÑIZARES, por Resolución No.23 de 1960. El Doctor Emiro Quintero Cañizares, en su condición de Secretario General de Salud hizo posible su construcción y dotación.

El Acuerdo del Concejo Municipal No.27 de 1938 establece los estatutos que posteriormente fueron reformados por la Resolución No. 001 de 1960, emanada de la Junta Directiva y que define claramente su finalidad.

Su nivel de atención se determinó en 1960, cuando Norte de Santander fue tomado como uno de los Departamentos de prueba en la implantación de la regionalización según el plan Piloto estructurado por Min salud, O.P.S., UNICEF, con el fin de descentralizar las cuatro (4) especialidades básicas: Cirugía, Medicina Interna, Pediatría y Gineco-Obstetricia.
En el año de 1990 se inician los trabajos de remodelación que se terminan a finales de 1995.

Se le da vida jurídica como una empresa social del estado según ordenanza 060 del 29 de diciembre de 1995 emanada de la honorable Asamblea del Norte de Santander.
La ESE Hospital Emiro Quintero Cañizares es actualmente Hospital de II Nivel de atención, es Hospital de referencia para los Municipios de Ocaña, Abrego, Hacarí, La Playa, Teorama, San Calixto, Convención, El Tarra, El Carmen, Cáchira, y la Esperanza en el Departamento Norte de Santander, y de los Municipios de Río de Oro y Gonzáles del Departamento del Cesar.
El Hospital, es el centro asistencial más importante de la provincia de Ocaña ya que tiene una cobertura aproximada de 300.000 mil usuarios tiene como misión la prestación de servicios de salud con atención humanizada, dignidad, eficiencia, integridad y calidad a toda la población de Ocaña y municipios vecinos, que además ofrece servicios de promoción y prevención realizando visitas a diferentes zonas del área rural y puestos de salud.
La ESE Hospital Emiro Quintero Cañizares se encuentra en un momento trascendental e importante en su historia siendo el líder en el sector a través de la prestación de servicios, brindando atenciones en salud a miles de ciudadanos en condiciones de eficiencia, oportunidad y calidad, con buen nivel científico y realizando un aporte significativo al desarrollo de la región.
Como ya es sabido ante la permanente generación de cambios y transformación institucional tan profunda en el sector que se desenvuelven las entidades, ya sea jalonadas por la implementación de nuevas normas, la adopción de correctivos oportunos en cumplimiento de la legislación vigente, es de vital importancia para nosotros como IPS trabajar arduamente en la calidad de la prestación de servicios hacia nuestros clientes como

compromiso para satisfacer la población en sus necesidades de salud en todas las fases.[2]

1.1.1 Misión.

Somos una empresa social del Estado que presta servicios de salud de baja, mediana y alta complejidad en la Provincia de Ocaña, con altos estándares de calidad y mejora continua a los usuarios del sistema general de seguridad social en salud en la sede principal y redes integradas; basadas en la participación social, el desarrollo del Talento Humano, la relación docencia – servicio e investigación, con tecnología apropiada y en pro de la sostenibilidad financiera, respetando la dignidad del individuo, con el enfoque diferencial, enfoque de género, enfoque de derechos, logrando satisfacer las necesidades en salud.[3]

1.1.2 Visión.

Para el año 2023 la ESE Hospital Emiro Quintero Cañizares quiere ser reconocida en el Nororiente colombiano como una institución líder en salud, en la prestación de servicios, modelo en la atención, acreditada, promoviendo la gestión del conocimiento a través de la atención humanizada para mejorar la salud de los individuos y comunidad, enfocada a la población materno-infantil.[4]

1.1.3 Objetivo de la empresa.

- Contribuir al desarrollo social de la región mejorando la calidad de vida, y reduciendo la morbilidad, la mortalidad, la incapacidad y la angustia evitables en la población usuaria, en la medida en que esto esté a su alcance.

- Producir servicios de salud eficientes y efectivos, que cumplan con las normas de calidad establecidas de acuerdo con las reglamentaciones que se expida para tal propósito.

- Garantizar, mediante un manejo Gerencial adecuado, la rentabilidad social y financiera de la empresa.

- Ofrecer a las Empresas Promotoras de salud y demás personas naturales o jurídicas que lo demandan, servicios y paquetes de servicios a tarifas competitivas en el mercado.

- Satisfacer los requerimientos del entorno, adecuando continuamente sus servicios y funcionamiento.

- Garantizar los mecanismos de participación ciudadana y comunitaria establecidos por la ley y los reglamentos.

---

[2] ESE Hospital Emiro Quintero Cañizares Ocaña N. De S. Plataforma Estratégica (Reseña histórica) [En línea]. <http://www.hospitaleqc.gov.co/plataforma-estrategica/reseña-historica.html> [citado el 08 de marzo de 2012].
[3]PORTAFOLIO DE SERVICIO ESE Hospital Emiro Quintero Cañizares, 2015 (Misión)
[4]PORTAFOLIO DE SERVICIO ESE Hospital Emiro Quintero Cañizares, 2015 (Visión)

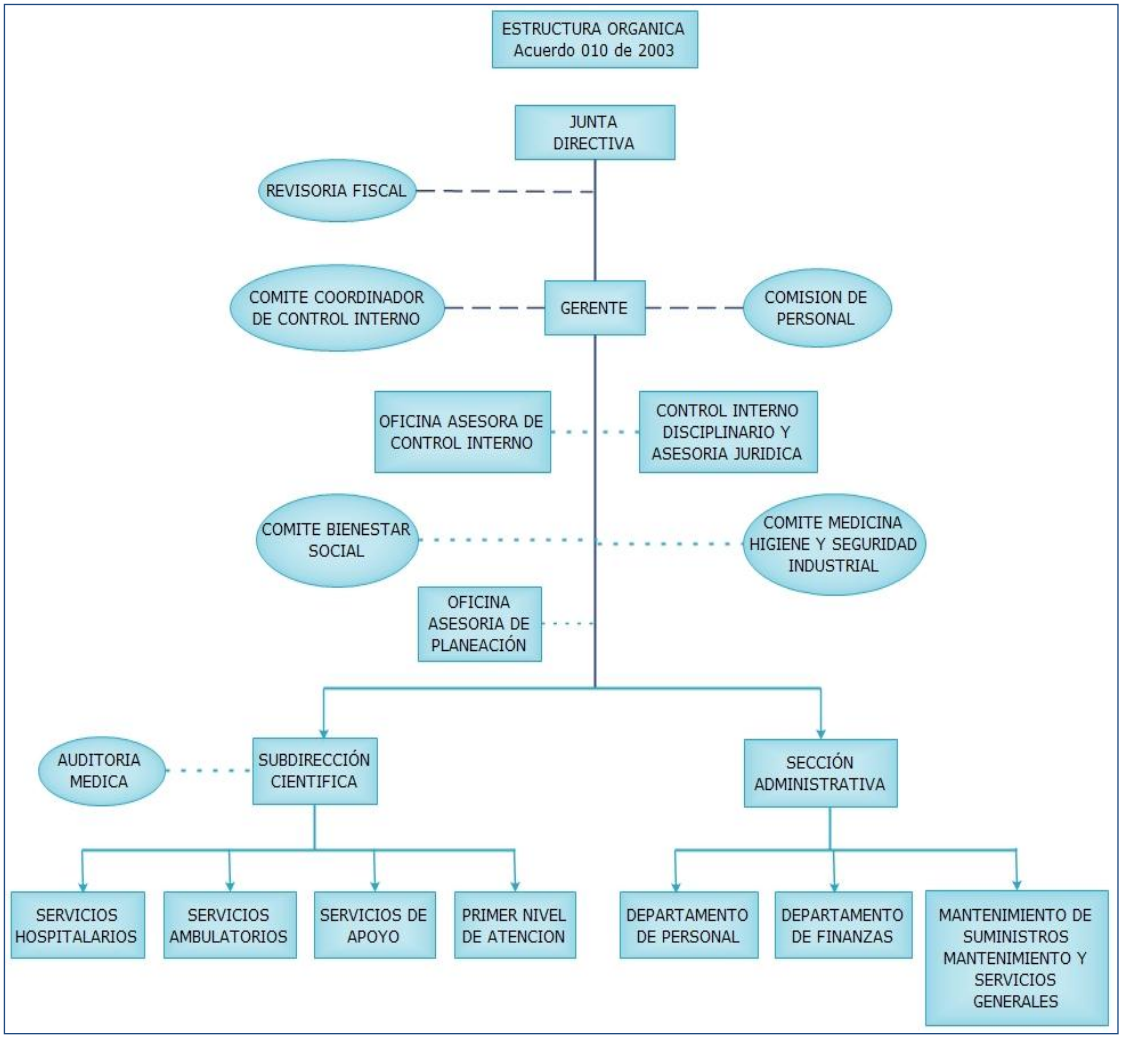
- Prestar servicios de salud que satisfagan de manera óptima las necesidades y expectativas de la población en relación con la promoción, el fomento y la conservación de la salud y la prevención, tratamiento y rehabilitación de la enfermedad.

- Satisfacer las necesidades esenciales y secundarias de salud de la población usuaria a través de acciones gremiales, organizativas, técnico-científicas y técnico-administrativas.

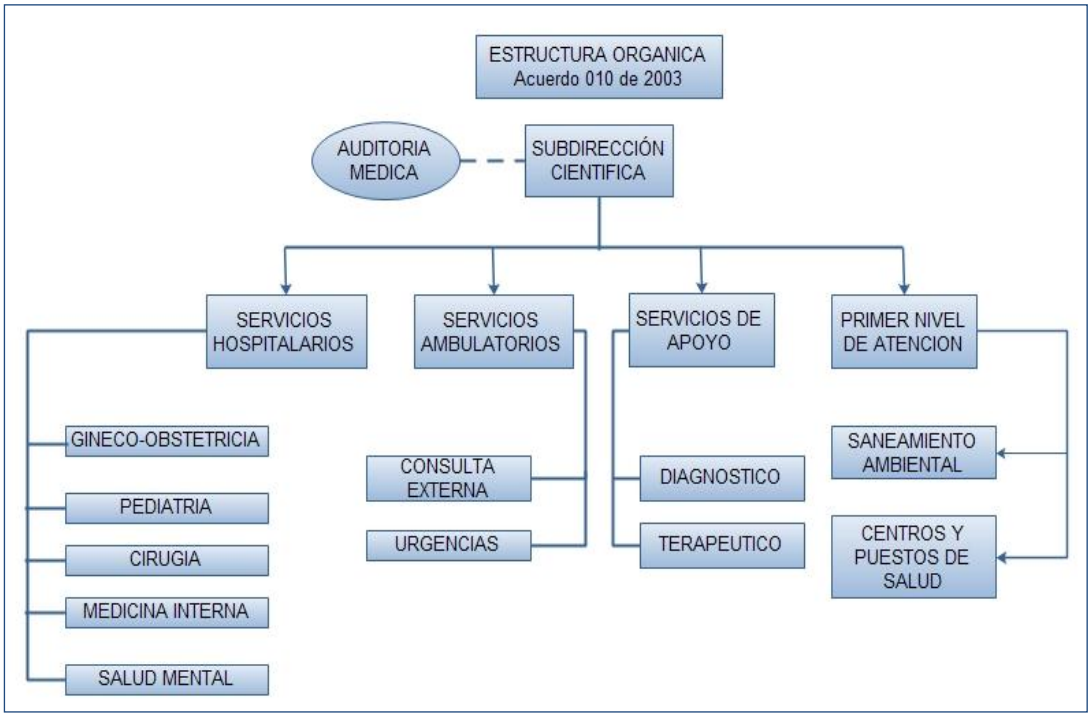
- Desarrollar la estructura y capacidad operativa de la Empresa mediante la aplicación de principios y técnicas gerenciales que aseguren su supervivencia, crecimiento, calidad de sus recursos, capacidad de competir en el mercado y rentabilidad social y financiera.

1.1.4 Estructura orgánica del HEQC Ocaña[5]

Figura No 1. Estructura Orgánica del HEQC.



[5] ESE Hospital Emiro Quintero Cañizares Ocaña N. De S. Información Corporativa (Estructura Orgánica) [En línea]. <http://www.hospitaleqc.gov.co/organigrama.html> [citado el 30 de marzo de 2012].



Gerencia. Encargada de Dirigir, Gestionar todos los planes, programas y proyectos que garanticen la prestación de servicios de salud, tendientes a promover el desarrollo integral.

Oficina Asesoría jurídica. Fortalecer las labores asistenciales de apoyo a los procesos administrativos jurídicos en la E.S.E.

Oficina Asesora de Control Interno. Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten, garantizar la eficacia, la eficiencia y economía en todas las operaciones, promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional, velar porque todas las actividades y recursos de la organización estén dirigidos al cumplimiento de los objetivos del Hospital.

Subdirección Científica. Organizar y coordinar políticas institucionales de atención en salud, planear y controlas los recursos necesarios para el desarrollo de las políticas de salud, dirigir la prestación del servicio conforme a las competencias asignadas por las normas en salud pública.

Servicios Hospitalarios. Fortalecer los procesos que se realizan en el laboratorio Clínico, fisioterapia, radiología, anestesiología, cirugías, gineco-obstetricia, pediatría, para mejorar la calidad de la prestación del servicio en la institución.

Servicios de Apoyo. Fortalecer los procesos de sistemas de información, estadística, archivo y procedimientos que se realizan en trabajo social para mejorar la calidad en la

prestación del servicio en la institución.

Sección Administrativa. Planear, ejecutar, controlar la prestación de los servicios administrativos y velar por el cumplimiento de las políticas financieras de personal, de recursos físicos e información del Hospital.

Departamento de Personal. Fortalecer los procedimientos de programación, coordinación y supervisión de programas que garanticen el buen funcionamiento y desarrollo del Talento Humano en la institución.

Departamento de finanzas. Fortalecer los procedimientos dando cumplimiento a las normas contables generalmente aceptadas y referentes técnicos de la Contaduría general de la Nación y Entes de Control.

Mantenimiento de Suministros y servicios generales. Fortalecer labores de programación, coordinación y supervisión del área de suministros, almacén y controlar las labores técnicas en la oficina de mantenimiento, lavandería y economato.

Servicios Ambulatorios. Fortalecer los procesos y procedimientos que se realizan en medicina interna, traumatología, ortopedia, otorrinolaringología, psiquiatría, para mejorar la calidad de la prestación del servicio en la institución.

1.1.5 Descripción de la dependencia

La dependencia de sistemas en la E.S.E Hospital Emiro Quintero Cañizares (Ocaña) no existe, esta solamente cuenta con dos áreas de trabajo bastante pequeñas las cuales son: Mantenimiento de sistemas que es la encargada de todos los procedimientos técnicos preventivos y correctivos de todos los equipos de cómputo con los que cuenta el hospital actualmente; esta área se encuentra ubicada en la dependencia Mantenimiento de Suministros y servicios generales.

Por otra parte existen sistemas de información, encargados de las agendas médicas, radiología, asignación de citas, facturación, administración, contabilidad y demás procesos de pagos por los servicios prestados, esta actividad está a cargo de la empresa COOTRASMAR CTA, la cual ofrece todos estos servicios garantizando mayor seguridad y viabilidad de la información. Esta se encuentra en comodato con la ESE HEQC, también es llevado a cabo el proceso de estadísticas vitales encargados del manejo de las estadísticas de nacidos vivos y los fallecimientos en las diferentes áreas dentro de la E.S.E.

1.2. DIAGNÓSTICO INICIAL DE LA DEPENDENCIA ASIGNADA

Tabla No 1. Diagnóstico inicial de la Dependencia Asignada.

Fortalezas	Debilidades
• Se cuenta con disposición de la alta gerencia para invertir en pro de mejorar el servicio. • Existencia de oficinas con la tecnología adecuada para la ejecución de los procesos (Hardware, software y equipos de telecomunicaciones). • El Hospital posee a su disposición un equipo de trabajo orientado a mejorar la prestación del servicio y calidad de este.	• No se cuenta con una revisión y evaluación permanente de los Sistemas de información que soporte y mantenga de forma eficiente la información. • No se cuenta con una infraestructura adecuada donde se contemple toda el área de Sistemas, esto hace que no haya integridad laboral del equipo de trabajo y que algunas áreas estén separadas de otras. • El Recurso Humano no es suficiente para atender la demanda en la implementación de nuevos sistemas de información y tecnología. • No se realizan controles a los riesgos tecnológicos a ninguna de las áreas de sistemas. • Poca capacitación al personal del área de Sistemas para poder solucionar problemas a largo plazo.
Amenazas	**Oportunidades**
• Fácil acceso de personal no autorizado a la información permitiendo que se presenten alteraciones, modificaciones o pérdida de la misma. • Desestabilización del sistema por ataques informáticos.	• Posibilidad de mejorar la infraestructura del área de sistema para el mejoramiento de todos los procesos tecnológicos que se llevan a cabo en E.S.E • Implementación de políticas y procedimientos que garanticen la integridad, accesibilidad y disponibilidad de la información. • Competitividad, rentabilidad y buena imagen frente a otras empresas que desempeñen la misma función.

Fuente personal (Entrevista y Observación directa)

1.2.1. Planteamiento del problema

El sistema de información **myProcess** de la E.S.E Hospital Emiro Quintero Cañizares de Ocaña no es evaluado frecuentemente por que no ha sido posible conocer si los controles que se llevan a cabo para mantener la integridad y disponibilidad de la información que se maneja a través de este, son lo suficientemente efectivos o si por el contrario se hace necesario realizar una restructuración de los mismos e implementar otras medidas de seguridad.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que pueden aprovechar cualquiera de las vulnerabilidades existentes para someter activos críticos de información a diversas formas de fraude, espionaje, sabotaje o devastación; Así mismo debe considerarse los riesgos que pueden producirse al no llevar un control adecuado de cada uno de los sistemas de información, ya que de esta manera la calidad del servicio es más eficiente tanto para la comunidad como para el personal de trabajo de la empresa.

La información, junto con los procesos y sistemas que hacen uso de ella, son activos muy importantes para una organización, pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Es evidente además que la empresa en mención, no cuenta con un plan de auditoria continuo, por tal razón, es imperiosa la necesidad de implementar una evaluación y revisión sobre el estado actual del sistema de información mencionado, sugerir controles para manejar los riesgos o inconvenientes que se puedan presentar en este, además establecer objetivos que contribuyan al seguimiento, revisión y control de la información, útil para la toma de decisiones.

1.3. OBJETIVOS

1.3.1. General

Auditar el sistema de información de gestión administrativa y hospitalaria **myProcess** de la E.S.E Emiro Quintero cañizares del municipio de Ocaña**,** Norte de Santander bajo el estándar ISO/IEC 27002:2013

1.3.2. Específicos

- Realizar un diagnóstico de la seguridad del Sistema de Información **myProcess** que da soporte a los servicios que presta el E.S.E Hospital Emiro Quintero Cañizares.

- Realizar una evaluación de riesgos asociados a la seguridad del sistema de Información **myProcess** del Hospital Emiro Quintero Cañizares.

- Elaborar el informe de Auditoria.

1.4. DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR.

Tabla No 2. Descripción de actividades.

Objetivo General	Objetivos Específicos	Actividades a Desarrollar en la empresa para hacer posible el cumplimiento de los Objetivos Específicos
AUDITAR EL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTÁNDAR ISO/IEC 27002:2013	Realizar un diagnóstico del Sistema de Información **myProcess** que da soporte a los servicios que presta el E.S.E Hospital Emiro Quintero Cañizares.	▪ Diseño de instrumentos de recolección de información. ▪ Análisis de los resultados obtenidos. ▪ Elaboración del diagnóstico
	Realizar una evaluación de riesgos asociados a la seguridad del sistema de Información **myProcess** del Hospital Emiro Quintero Cañizares.	▪ Identificación de los activos de información. ▪ Tasación de activos ▪ Identificación de amenazas y vulnerabilidades ▪ Cálculo de amenazas y vulnerabilidades. ▪ Evaluación de variables
	Elaborar el informe de Auditoria.	▪ Elaboración del documento del Informe Final con sus hallazgos y recomendaciones.

2. ENFOQUE REFERENCIAL.

2.1. ENFOQUE CONCEPTUAL

2.1.1. Información.[6]

La información es un activo que representa un gran valor dentro de la organización, sean este tangible o intangible, por tanto requiere una protección adecuada ya sea por diferentes medios o técnicas de seguridad implantada.

2.1.2. Sistemas de Información[7]

Los Sistemas de Información (SI) son conjuntos organizados de elementos que procesan y distribuyen información con el fin de cumplir unos objetivos. No es necesario que estén basados en ordenadores. La utilización de aplicaciones informáticas sobre soportes informáticos da lugar a los Sistemas de Información Automatizados (SIA).

Los Sistemas de Información pretenden proporcionar una información oportuna y exacta para el apoyo en la toma de decisiones de la compañía. Además, garantizan la confiabilidad, la integridad y disponibilidad de la información. El uso de Sistemas de Información automatiza procesos operativos y pretenden conseguir ventajas competitivas en el mercado.

Características de los datos en un sistema de información:

Integridad:

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

Confidencialidad:

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Disponibilidad:

[6]Universidad Politécnica SALESIANA de Ecuador. Seguridad de la Información.ISOIIEC, 2005, 107 P (ISO/IEC 27002:2005 (E)).

[7]Universidad Carlos III de Madrid escuela politécnica superior calidad y seguridad de la información y auditoría informática

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2.1.3. Auditoría.[8]

Control realizado por los empleados de una empresa para garantizar que las operaciones se llevan a cabo de acuerdo con la política general de la entidad, evaluando la eficacia y la eficiencia, y proponiendo soluciones a los problemas detectados.

2.1.3.1. Auditoría a Bases de Datos.[9]

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

– Quién accede a los datos.
– Cuándo se accedió a los datos.
– Desde qué tipo de dispositivo/aplicación.
– Desde que ubicación en la Red.
– Cuál fue la sentencia SQL ejecutada.
– Cuál fue el efecto del acceso a la base de datos.

Es uno de los procesos fundamentales para apoyar la responsabilidad delegada a IT por la organización frente a las regulaciones y su entorno de negocios o actividad.

2.1.3.2. Auditoría a Redes de Datos.[10]

Una Auditoria de Redes es, en esencia, una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información.

2.1.4. Auditoria de Sistemas de información.[11]

La Auditoría de Sistemas de Información es el proceso de recoger y evaluar las evidencias para determinar la seguridad de los sistemas informáticos, la salvaguarda de los activos, la integridad de los datos y conseguirlos objetivos dela organización con eficacia y con consumo de recursos eficiente.

Por tanto, la Auditoría de Sistemas de Información mantiene la obtención de los objetivos de la Auditoría tradicional, que tiene como foco la salvaguarda de los activos y la

[8]Auditoría: conceptos, clases y evolución, Capítulo 1[en línea]Disponible en Internet:< http://www.mcgraw-hill.es/bcv/guide/capitulo/8448178971.pdf>
[9]En Línea http://www.jkmst.com
[10]GIL RIOS, OSCAR; Auditoría a la red de una Empresa.
[11]Universidad Carlos III de Madrid escuela politécnica superior calidad y seguridad de la información y auditoría informática

integridad de los datos, ya demás los objetivos de eficacia y eficiencia. El proceso de la Auditoría de Sistemas de Información se puede concebir como una fuerza que ayuda a las organizaciones a conseguir mejor estos objetivos.

Importancia de realizar auditorías a los sistemas de información:

La Auditoria es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

La Auditoria del Sistema de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que se sustenta.

2.1.4.1 Seguridad Lógica.[12]

Se conoce seguridad lógica como la manera de aplicar procedimientos que se aseguren que solo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlos.

2.1.5 Estándar ISO/IEC 27002.[13]

La ISO 27002 comprende la norma ISO / IEC 17799: 2005 esta consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.
Éstos se hallan distribuidos en diferentes dominios que abarcan de una forma integral todos los aspectos que han de ser tenidos en cuenta por las organizaciones.

Dominios de la ISO 27002

Estos dominios que estructura la ISO 27002 son:

1. La política de seguridad.
2. Los aspectos organizativos de la seguridad de la información.
3. La gestión de activos.
4. La seguridad ligada a los recursos humanos.
5. La seguridad física y ambiental.
6. La gestión de las comunicaciones y de las operaciones.
7. Los controles de acceso a la información.
8. La adquisición, desarrollo y mantenimiento de los sistemas de información.
9. La gestión de incidentes en la seguridad de la información.
10. La gestión de la continuidad del negocio.
11. Los aspectos de cumplimiento legal y normativo.

[12]CERVANTES, ROSALBA; Unidad IV Seguridad Lógica.
[13]ISO/IEC 27002:2013, Information Technology - Security techniques – Code of practice for security management. DisponibleenInternet<http://inicio.ifai.org.mx/DocumentosdeInteres/4-2_ISO-IEC_27002-2013.pdf>

2.1.5.1 Seguridad de la información[14]

La seguridad de la información es la protección de la información de un rango amplio der amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de la inversiones y las oportunidades comerciales.
La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

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

• Integridad:

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad:

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

2.1.6. Análisis de riesgos informáticos.[15]

El análisis del riesgo es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Hay pequeñas variaciones en la terminología utilizada por las tres organizaciones. Sin embargo, las tres organizaciones hermanas consideran el análisis del riesgo como un proceso que consta de cuatro etapas:

- Identificación del peligro
- Evaluación del riesgo
- Gestión del riesgo
- Comunicación del riesgo.

[14]ISO/IEC 27002:2013, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información,DisponibleenInternet<https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf>
[15] Disponible en Línea http://www.wto.org

La **identificación del peligro** consiste en especificar el acontecimiento adverso que es motivo de preocupación.

En la **evaluación del riesgo** se tiene en cuenta la probabilidad (la probabilidad real y no sólo la posibilidad) de que se produzca el peligro, las consecuencias si ocurre y el grado de incertidumbre que supone. (Obsérvese que esta descripción de la evaluación del riesgo es diferente de la definición que figura en el Acuerdo MSF.)

La **gestión del riesgo** consiste en la identificación y aplicación de la mejor opción para reducir o eliminar la probabilidad de que se produzca el peligro.

La **comunicación del riesgo** consiste en el intercambio abierto de información y opiniones aclaratorias que llevan a una mejor comprensión y adopción de decisiones

2.2. ENFOQUE LEGAL.

El presente trabajo tiene como base legal las siguientes normas:

2.2.1 Ley 1273 DE 2009.[16]

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

ELCONGRESO DE COLOMBIA

Decreta:

ARTÍCULO1°. Adiciónese el Código Penal con un Título VIIBIS denominado "De la Protección de la información y de los datos.

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y delos sistemas informáticos

2.2.1.1. Artículo269ª: **Acceso abusivo a un sistema informático**.
El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

[16]ConstituciónpolíticadeColombia.Delaprotecciódelainformaciónydelosdatos,Ley1273de2009[EnLínea]Disponibleeninternet:<http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm>

2.2.1.2. Articulo 269E. Uso de software malicioso.
El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envié, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.2.1.3. Artículo269C: **Interceptación de datos informáticos**.
El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisión es electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

2.2.1.4. Artículo269D: **Daño Informático**.
El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho(48) a noventa y seis (96) meses y en multa de 100 a1.000 salarios mínimos legales mensuales vigentes.

2.2.1.5. Artículo269F: **Violación de datos personales**.
El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

3. INFORME DE CUMPLIMIENTO DE TRABAJO

3.1. PRESENTACION DE RESULTADOS

3.2. ASPECTOS DE LA AUDITORIA.

3.2.1. Objetivo General.

Auditar el sistema de información de gestión administrativa y hospitalaria **myProcess** de la E.S.E Emiro Quintero cañizares del municipio de Ocaña**,** Norte de Santander bajo el estándar ISO/IEC 27002:2013

3.2.2. Objetivos Específicos.

- Evaluar la existencia y eficiencia de procedimientos formales para la gestión de los derechos de acceso de los usuarios que manejan el sistema de información myProcess.
- Evaluar los controles de acceso al sistema myProcess y aplicaciones adicionales.
- Evaluar la protección contra el código malicioso en el sistema de información myProcess.
- Evaluar la existencia de realización de copias de seguridad en el sistema de gestión administrativa y hospitalaria myProcess.
- Evaluar la gestión y monitoreo de las vulnerabilidades técnicas en el sistema de información.
- Evaluar la seguridad y eficiencia en los procesos de desarrollo y soporte brindado al sistema de información myProcess.
- Evaluar controles de acceso a la base de datos del sistema de información myProcess.

3.2.3. Alcances.

Para el presente proyecto, se hizo necesario evaluar los siguientes controles pertenecientes al estándar internacional ISO/IEC 27002:2013: Control de acceso al sistema de información, seguridad en las operaciones realizadas en el sistema y las actividades relacionadas con Adquisición, Desarrollo y mantenimiento de los sistemas de información, aplicándolos en el área de Sistemas de la E.S.E. Emiro Quintero Cañizares del municipio de Ocaña, Norte de Santander.

3.2.4. Restricciones.

Debido a cierto cargo asignado a un nuevo ingeniero para manejar y administrar la base de datos del sistema de información myProcess desde la ciudad de Cúcuta, no fue posible evaluar la integridad de los datos.

3.2.5. Recurso Humano.

EDUARDO ANDRES OSPINO MORON – Auditor
MAGRETH ROSSIO SANGUINO REYES– Directora del Proyecto
YOLIMER AREVALO CLARO – Director de infraestructura Técnica
GEOVANNI ORTIZ SANCHEZ – Administrador de Sistema de Información myProcess.

3.2.6. Criterios.

La auditoría realizada se llevó a cabo bajo el estándar ISO/IEC 27002:2013, teniendo en cuenta los siguientes dominios.

CONTROL DE ACCESOS.

- Requisitos del negocio para el control de acceso.
- Gestión de acceso de usuario
- Responsabilidades del usuario
- Control de acceso a sistemas y aplicaciones.

SEGURIDAD EN LA OPERATIVA.

- Responsabilidades y procedimientos de operación
- Protección contra el código malicioso.
- Copias de seguridad.
- Registro de actividad y supervisión.

ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION.

- Seguridad en los procesos de desarrollo y soporte.

3.3. ORGANIZACIÓN DEL TRABAJO

3.3.1. Plan de Auditoría

Contiene el conjunto de actividades que como equipo auditor, se establecieron para llevar a cabo la realización de la auditoria en la E.S.E. Emiro Quintero Cañizares, así como el lugar y fecha de encuentro con los auditados.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT PLA01

Empresa: **E.S.E. Emiro Quintero Cañizares** — Fecha Inicio: 06/04/2015
Área o Proceso**: Sistemas** — Fecha Final: 10/07/2015

Auditor : **Eduardo Andrés Ospino Morón – E.A.O.M**

Objetivo General
Auditar el sistema de información de gestión administrativa y hospitalaria **myProcess** de la E.S.E Emiro Quintero cañizares del municipio de Ocaña, Norte de Santander bajo el estándar ISO/IEC 27002:2013.

Alcances
La auditoría se llevara a cabo en la E.S.E. Emiro Quintero Cañizares de Ocaña, durante 4 meses se realizara la evaluación mediante el estándar ISO/IEC 27002:2013, contemplando la seguridad lógica, desarrollando diferentes actividades que permitan analizar y verificar los procedimientos que se llevan a cabo al sistema de información myProcess.

No.	ACTIVIDAD	FECHA-HORA	LUGAR	AUDITADO	AUDITOR
1	Reunión con el Ingeniero para definir responsabilidades y tareas.	22/04/2015 2:00 p.m.	AREA DE SISTEMAS E.S.E HEQC	Y.A	E.A.O.M
2	Reunión del equipo auditor para definir los métodos y procedimientos de auditoría	23/04/2015 09:30 a.m.	OFICINA E.S.E-HEQC	Y.A	M.R.S.R. E.A.O.M
3	Socialización del Programa de Auditoría	24/04/2015 4:00 p.m.	E.S.E-HEQC	Y.A	E.A.O.M

4	Reunión para discutir la pertinencia de los instrumentos de recolección de información.	25/04/2015 2:00 p.m.	AREA DE SISTEMAS E.S.E HEQC	Y.A	E.A.O.M
5	Diseño de instrumentos de recolección de información (Entrevistas, Listas de chequeo, Prueba sustantiva...).	11/05/2015 8:00 a.m.	AREA DE SISTEMAS E.S.E HEQC	Y.A	E.A.O.M
6	Aplicación de instrumentos de recolección de información (Entrevistas, Listas de chequeo, Prueba sustantiva...)	20/05/2015 8:00 a.m.	AREA DE SISTEMAS E.S.E HEQC	G.O	E.A.O.M
7	Elaboración del diagnóstico del área auditada.	20/06/2015 09:00 a.m.	OFICINA E.S.E-HEQC	Y.A	M.R.S.R. E.A.O.M
8	Reunión de cierre de la auditoría.	23/06/2015 2:00 p.m.	AREA DE SISTEMAS E.S.E HEQC	Y.A	E.A.O.M
9	Entrega del Informe Final de Auditoría.	10/07/2015 2:00 p.m.	AREA DE SISTEMAS E.S.E HEQC	Y.A	E.A.O.M

EDUARDO ANDRES OSPINO MORON Encargado de Auditoria Auditor Master	**ING. YOLIMER AREVALO CLARO** Directro de Infraestructura Tecnica Auditado

MARCAS O TILDES UTILIZADAS
PLA01: Plan de Trabajo No. 1 **E.A.O.M:** Eduardo Andrés Ospino Morón – Auditor Master. **M.R.S.R.:** Magreth Rossio Sanguino Reyes – Directora del Proyecto. **G.O:** Geovanny Ortiz – Administrador de Software myProcess. **Y.A:** Yolimer Arévalo-Director de Infraestructura Técnica.

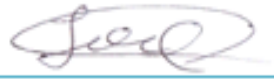
3.3.2. Programa de Auditoría.

Para la evaluación a la seguridad lógica del sistema de información myProcess, se realizó el programa de auditoria con los diferentes objetivos y actividades a realizar en la E.S.E Emiro Quintero Cañizares.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER **FACULTAD DE INGENIERIAS** **PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS** **AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013**	**R/PT PRA01**
Empresa: **E.S.E. Emiro Quintero Cañizares** Área o Proceso**: Sistemas**	Fecha Inicio: 06/04/2015 Fecha Final: 10/07/2015
Auditor**: Eduardo Andrés Ospino Morón – E.A.O.M**	
Objetivo General Auditar el sistema de información de gestión administrativa y hospitalaria myProcess de la E.S.E Emiro Quintero cañizares del municipio de Ocaña, Norte de Santander bajo el estándar ISO/IEC 27002:2013	
Objetivos Específicos. 1. Evaluar la existencia y eficiencia de procedimientos formales para la gestión de los derechos de acceso de los usuarios que manejan el sistema de información myProcess. 2. Evaluar los controles de acceso al sistema myProcess y aplicaciones adicionales. 3. Evaluar la protección contra el código malicioso en el sistema de información myProcess. 4. Evaluar la existencia de realización de copias de seguridad en el sistema de gestión administrativa y hospitalaria myProcess. 5. Evaluar la seguridad y eficiencia en los procesos de desarrollo y soporte brindado al sistema de información myProcess. 6. Evaluar controles de acceso a la base de datos del sistema de información myProcess.	

No.	ACTIVIDAD	AUDITADO	R/PT
1.1	Verificar la existencia de una política de control de acceso a la información y al sistema de información myProcess que soporta las actividades de gestión administrativa y hospitalaria.	G.O	**ENT01**
1.2	Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.	PT-HEQC	**ENT02**
2.1	Verificar la existencia de controles de acceso que dan soporte al buen uso del sistema de información myProcess.	G.O	**ENT03**
3.1	Verificar la existencia de controles preventivos y correctivos contra el código malicioso que pueda afectar al sistema de información.	Y.A.C	**ENT04**
3.2	Realizar comprobación de la eficiencia de los controles implementados para contrarrestar la presencia de código malicioso.	Y.A.C	**CHL01**
4.1	Verificar la existencia de una política de realización de copias de respaldo de la data en el sistema de información myProcess.	G.O	**ENT05**
4.2	Comprobar la eficiencia de los procedimientos de rutina para realización de backups y su restauración.	G.O	**CHL02**
5.1	Verificar la existencia e implementación de procedimientos formales, especificación, prueba y control que dan soporte a la seguridad y desarrollo del sistema de información myProcess.	G.O	**ENT06**

6.1	Verificar la existencia de controles de acceso a la base de datos que dan soporte al sistema de información myProcess.	G.O	**ENT07**

APROBACIÓN	
	
EDUARDO ANDRES OSPINO MORON Encargado de Auditoria Auditor Master	**ING. YOLIMER AREVALO CLARO** Directro de Infraestructura Tecnica Auditado

MARCAS O TILDES UTILIZADAS

PA01: Programa de Auditoría
G.O: Geovanny Ortiz
PT-HEQC: Personal de trabajo del Hospital Emiro Quintero Cañizares.
ENT01: Entrevista No. 1
ENT02: Entrevista No. 2
ENT03: Entrevista No. 3
ENT04: Entrevista No. 4
ENT05: Entrevista No. 5
ENT06: Entrevista No. 6
ENT07: Entrevista No. 7
CHL01: Lista de chequeo No.1
CHL02: Lista de chequeo No.2

3.4. HALLAZGOS DE AUDITORIA

Después de haber realizado una serie actividades e investigación por medio de entrevistas listas de chequeo y demás papeles de trabajo que permitieron visualizar en que situación de seguridad lógica se encuentra el sistema de información myProcess de la entidad de salud, se encontraron los siguientes hallazgos bajo tres dominios de la norma ISO/IEC 27002/2013 los cuales son:

- **CONTROL DE ACCESOS.**

Situaciones encontradas

- No existe una política de control de acceso claramente definida que contenga los requerimientos de seguridad de los activos de información.
- No existen procedimientos formales que enuncien los derechos de acceso a los usuarios que manejan el sistema de información myProcess.
- No existen acuerdos de confidencialidad para los usuarios del sistema de información myProcess.
- Se realizan muy pocas capacitaciones a los usuarios del sistema en el uso de las buenas prácticas de la seguridad de la información.
- Los usuarios que manejan el sistema no reciben formalmente por escrito la información relacionada con el acceso al sistema y las tareas que pueden realizar o no en el mismo.
- Los usuarios no conocen en su totalidad las funciones del módulo que les corresponde, llegando a retrasar sus tareas.
- Muchos usuarios en el momento de su contratación no le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y las sanciones que este acarrea.
- No existen procedimientos formales para manejar el control de acceso a myProcess y aplicaciones necesarias para su funcionamiento.
- Los Usuarios del sistema conocen su usuario y contraseña para entrar al sistema, aplicándola para trabajar en sus tareas.
- A los usuarios se le asignan ciertos privilegios para manejar sus tareas en el sistema de información myProcess.

Recomendaciones.

- Implementar una política de control de acceso que contenga los requerimientos de seguridad de los activos de información.
- Establecer procedimientos formales que enuncien los derechos de acceso a los usuarios que manejan el sistema de información myProcess.
- Establecer acuerdos de confidencialidad para los usuarios que manejan el sistema de información myProcess.
- Aumentar el número de capacitaciones a los usuarios en el uso de las buenas prácticas de la seguridad de la información.
- Implementar documentos formales sobre la información relacionada con el acceso al sistema y las tareas que pueden realizar cada uno de los usuarios que manejan el sistema de información.
- información myProcess.
- Capacitar a los usuarios nuevos en las actividades y responsabilidades sobre el manejo de la información y las sanciones que acarrean su mal uso.
- Establecer procedimientos formales para controlar el acceso al sistema de información myProcess y demás aplicaciones necesarias para su funcionamiento.

- **SEGURIDAD EN LA OPERATIVA.**

Situaciones encontradas

- No existen políticas formales para controlar el uso de software no autorizado al sistema.
- Los usuarios que manejan el sistema de información no conocen estas políticas y no las aplican.
- Se realizan muy pocas capacitaciones de prevención a los usuarios para evitar los ataques por virus, robo de información, malware y demás códigos maliciosos.
- No existen sanciones disciplinarias establecidas para los usuarios que hacen caso omiso al uso de medios informáticos que pueden poner en riesgo la seguridad de la información.
- Se realizan pocos chequeos a los medios electrónicos u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos.
- No existen procedimientos formales para la realización de back-Up en el sistema de información myProcess.
- No existen un lugar externo a las instalaciones del hospital donde se almacenen las copias de seguridad para los casos en que se presente un siniestro.
- Se realizan copias de seguridad todos los días, las cuales son almacenas en el disco duro del servidor y demás medios de almacenamiento.

- Existe un firewall (corta fuegos), el cual no permite que los ataques por virus y demás códigos maliciosos no entren tan fácilmente al sistema.

Recomendaciones.

- Establecer procedimientos formales que restrinjan el uso de software no autorizado al sistema, evitando de esta manera posibles ataques. De igual manera capacitar a los usuarios del sistema de información en el buen uso de los recursos informáticos que tienen bajo su responsabilidad.
- Crear una política de seguridad de la información, que contenga todos los procedimientos para el buen uso de la información que se genera al interior del Hospital, así como las sanciones por omisiones o incumplimiento a la misma.
- Realizar registros exactos y completos de las copias de respaldo y procedimientos documentados de su restauración.
- Almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el área de sistemas las copias de respaldo que se realicen.
- Otorgar el nivel de protección física y ambiental adecuados a las copias de respaldo de la información.
- Probar regularmente los medios de respaldo para asegurar su confiabilidad de tal manera que puedan ser usados en casos de emergencia.
- Probar regularmente los procedimientos de restauración de las copias de respaldo para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.

- **ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION.**

Situaciones encontradas

- No existen procedimientos formales para la realización de cambios en los módulos o aplicaciones del sistema de información myProcess.
- Cuando se realizan cambios al sistema información no son informados al personal de trabajo del HEQC, lo cual provoca confusión y frecuentes errores en el sistema.
- No existe un personal totalmente capacitado para manejar el control de cambios en el sistema de información.

Recomendaciones

- Establecer e implementar procedimientos formales para controlar los cambios que se realizan en los módulos y aplicaciones del sistema de información myProcess.

- Documentar y hacer cumplir los procedimientos formales de control de cambios para minimizar la corrupción de los sistemas de información.
- Establecer un protocolo de comunicación o notificación de los cambios que se realizan a los módulos del sistema de información myProcess, de tal manera que se pueda evitar o reducir la frecuencia de errores en el manejo de los módulos que componen el sistema.
- Designar a personal competente del área de sistemas para que se encargue de la administración, documentación e implementación de los cambios que se realicen al sistema de información.

3.5. ANALISIS DE RIEGOS.

El primer paso en la Gestión de riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

3.5.1. Identificación de Activos.

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

Para el caso particular de la evaluación a la seguridad lógica del sistema de información administrativo y hospitalario myProcess, se identificaron lo siguientes activos:

ACTIVOS

Datos e Información

- Historias Clínicas.
- Bases de datos de los Usuarios.
- Contratos.
- Facturas.
- Registro de vacunas.
- Registros de citología.
- Registros epidemiológicos.
- Certificaciones.
- Lista de contactos de correos.
- Comprobantes.

- Historiales laborales.
- Indicadores.
- Informes.
- Hojas de vida de equipos de cómputo.
- Inventarios.
- Proyectos.
- Reportes.
- Remisiones.
- Cuentas.

Sistemas e Infraestructura

- Licencias de Software.
- Firewall.
- Copias de respaldo.
- Software Antivirus.
- Computadores.
- Servidores.
- Líneas Telefónicas.
- Router.
- Switch.
- Access Point.
- Ups.
- Aires Acondiciones.
- Rack de Comunicaciones.
- Cámaras de vigilancia.
- Proyectores.
- Cableado de red.
- Impresoras.

Personal

- Director de infraestructura Técnica.
- Administrador del sistema myProcess.
- Equipo de Capacitación.
- Equipo de Mantenimientos preventivos y Correctivos de computadores.

3.5.2. Tasación de activos.

La tasación de activos es un factor muy importante en la evaluación del riesgo. La tasación es la asignación apropiada en términos de la importancia que éste tenga para la empresa. Para ello se deberá aplicar una escala de valor a los activos y de esa manera poder relacionarlos apropiadamente.
Para tasar cada uno de los activos se utilizara la siguiente escala.

Tabla No 3. Tasación de Activos.

Insignificante (Ninguna)	No causa ningún tipo de impacto o daño a la organización.
Baja	Causa daño aislado, que no perjudica a ningún componente de la organización.
Mediana	Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
Alto	En el corto plazo desmoviliza o desarticula la organización.

ELEMENTOS DE INFORMACION	CLASIFICACION			MAGNITUD DE DAÑO			
DATOS E INFORMACIÓN	**Confidencial, Privado, Sensitivo**	**Obligación por ley/ Contrato / Convenio**	**Costo de recuperación**	**Insignificante (Ninguno)**	**Bajo**	**Mediano**	**Alto**
Historias Clínicas.	**x**	**x**	**x**			**x**	
Bases de datos de los Usuarios.	**x**		**x**				**x**
Contratos.	**x**	**x**	**x**			**x**	
Facturas.	**x**	**x**			**x**		
Registro de vacunas.	**x**	**x**			**x**		
Registros de citología.	**x**	**x**			**x**		
Registros epidemiológicos.	**x**	**x**			**x**		
Certificaciones.	**x**	**x**	**x**		**x**		
Lista de contactos de correos.	**x**				**x**		
Comprobantes.	**x**				**x**		

Historial laborales	x	x	x			x	
Informes.	x	x	x			x	
Hojas de vida de equipos de cómputo.	x	x	x			x	
Inventarios.	x	x	x			x	
Proyectos.	x		x			x	
Remisiones.	x	x	x			x	
Reportes.	x	x	x			x	
Cuentas.	x	x	x			x	
SISTEMAS E INFRAESTRUCTURA	**Acceso Exclusivo**	**Acceso Ilimitado**	**Costo de Recuperación (Tiempo, económico, material)**	**Insignificante (Ninguno)**	**Bajo**	**Mediano**	**Alto**
Licencias de Software.	x		x			x	
Firewall.	x		x				x
Copias de respaldo.	x		x				x
Software Antivirus.	x		x			x	
Computadores.	x		x			x	
Servidores.	x		x				x
Líneas Telefónicas.	x		x				x
Router.	x		x				x
Switch.	x		x				x
Access Point.	x		x			x	
Ups.	x		x			x	
Aires Acondicionados.	x		x		x		
Rack de Comunicaciones.	x		x				x
Cámaras de vigilancia.	x		x			x	
Proyectores.		x	x		x		
Cableado de red.	x		x				x
Impresoras.		x	x		x		
PERSONAL	**Imagen pública de alto perfil.**	**Perfil medio, experto en su área.**	**Perfil bajo**	**Insignificante (Ninguno)**	**Bajo**	**Mediano**	**Alto**
Director de infraestructura Técnica.		x				x	
Administrador del sistema myProcess.		x				x	

Equipo de Capacitación.		x			x		
Equipo de Mantenimientos preventivos y Correctivos de computadores.		x			x		

3.5.3. Identificación de Amenazas.

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática y los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

En esta etapa se hace una valoración de la probabilidad de ocurrencia de la amenaza y para ello se utilizará la siguiente escala:

Tabla No 4. Identificación de Amenazas.

Insignificante(Ninguna)	No existen condiciones que impliquen riego/ ataque
Baja	Existen condiciones que hacen muy lejana la posibilidad del ataque.
Mediana	Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
Alta	La realización de ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

TIPO DE AMENAZA O ATAQUE	**PROBABILIDAD DE AMENAZA**			
Actos originados por la criminalidad común y motivación política	**Insignificante**	**Baja**	**Mediana**	**Alta**
Sabotaje (ataque físico y electrónico).		**x**		
Robo / Hurto (físico).		**x**		
Robo / Hurto de información electrónica.			**x**	
Intrusión a Red interna.			**x**	

Infiltración.			**x**	
Virus / Ejecución no autorizado de programas.				**x**
Suceso de origen físico	**Insignificante**	**Baja**	**Mediana**	**Alta**
Incendio.		**x**		
Inundación / deslave.		**x**		
Sismo.		**x**		
Daños debidos al polvo.		**x**		
Falta de ventilación.		**x**		
Electromagnetismo.		**x**		
Sobrecarga eléctrica.			**x**	
Falla de corriente (apagones)		**x**		
Falla de sistema /Daño disco duro		**x**		
Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales	**Insignificante**	**Baja**	**Mediana**	**Alta**
Falta de inducción, capacitación y sensibilización sobre riesgos.			**x**	
Mal manejo de sistemas y herramientas.			**x**	
Utilización de programas no autorizados / software 'pirateado'			**x**	
Pérdida de datos		**x**		
Infección de sistemas a través de unidades portables sin escaneo.			**x**	

Unidades portables con información sin cifrado.			**x**	
Transmisión no cifrada de datos críticos.			**x**	
Compartir contraseñas o permisos a terceros no autorizados.			**x**	
Transmisión de contraseñas por teléfono.			**x**	
Exposición o extravío de equipo, unidades de almacenamiento, etc.		**x**		
Falta de definición de perfil, privilegios y restricciones del personal.		**x**		
Falta de mantenimiento físico (proceso, repuestos e insumos).		**x**		
Falta de actualización de software (proceso y recursos)		**x**		
Fallas en permisos de usuarios (acceso a archivos)		**x**		
Acceso electrónico no autorizado a sistemas internos.		**x**		
Red cableada expuesta para el acceso no autorizado.			**x**	
Red inalámbrica expuesta al acceso no autorizado.			**x**	
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)			**x**	

Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control.			**x**	

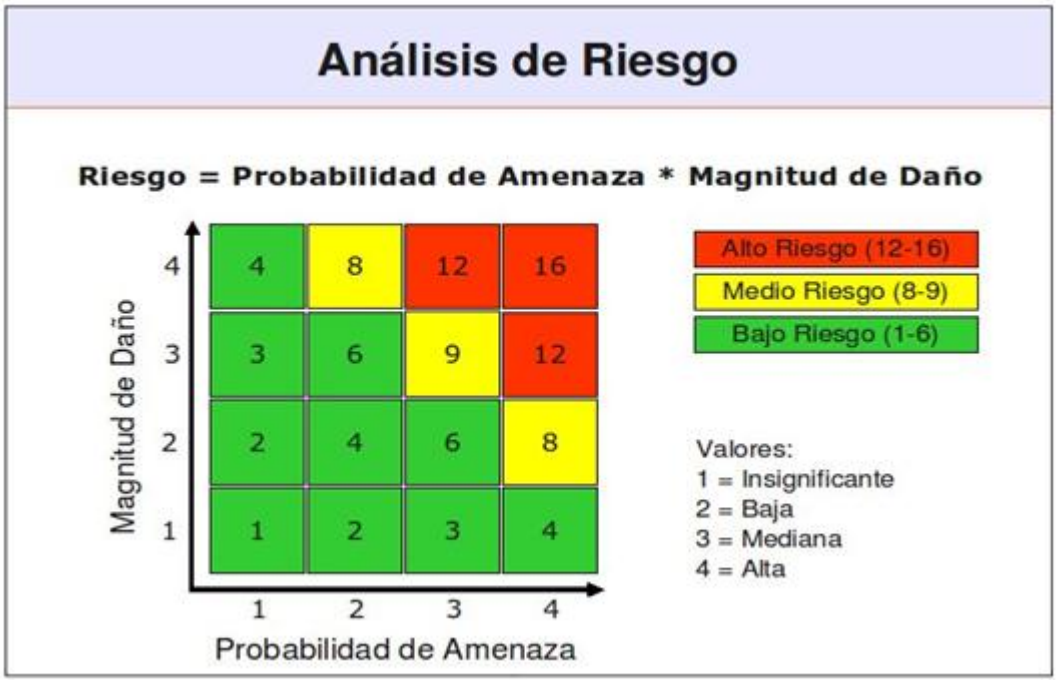
3.5.4. Calculo del Riesgo.

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos -las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo. La valoración del riesgo basada en la fórmula matemática es:

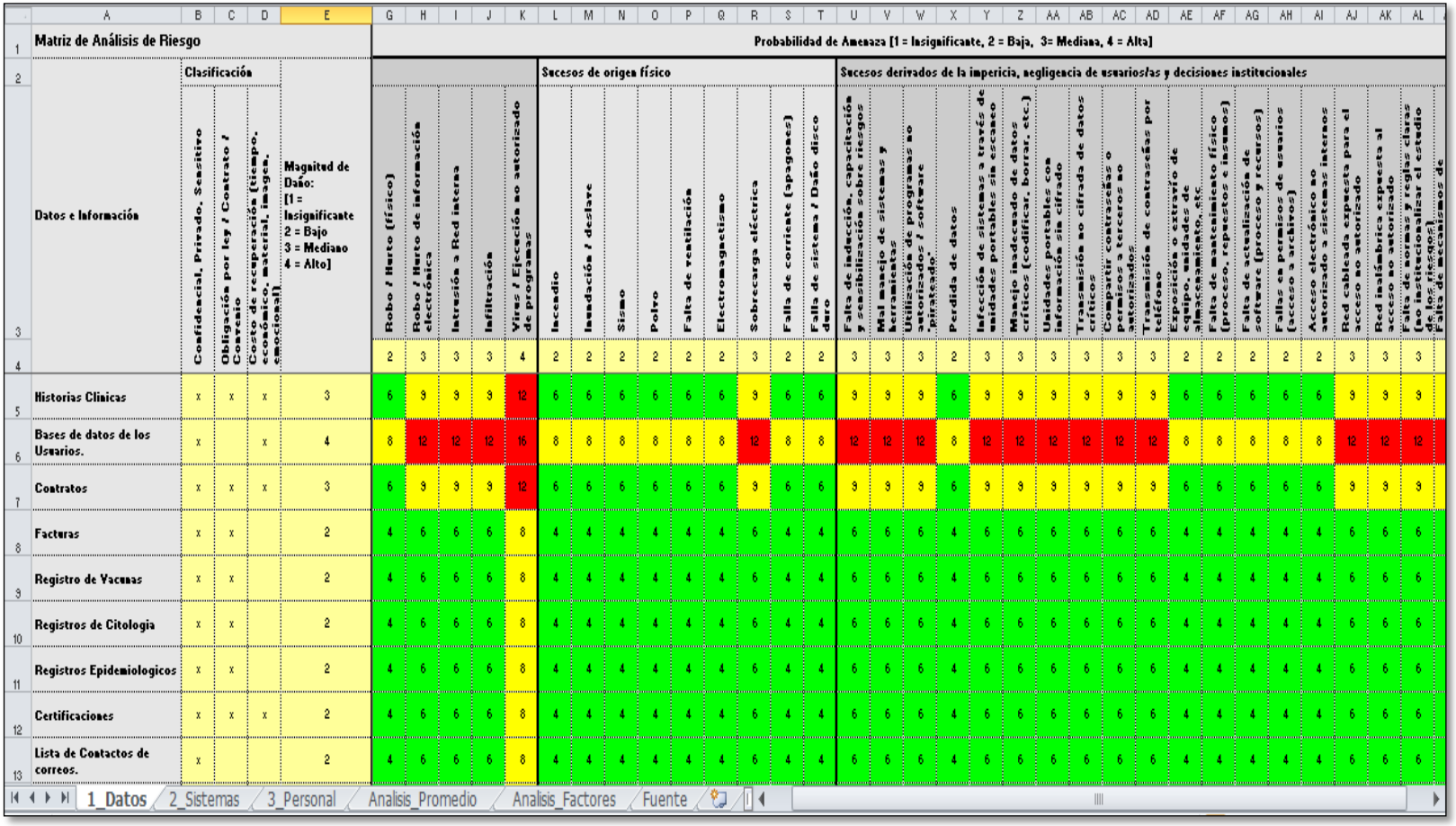
Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Figura No 2. Análisis de Riesgo.



Fuente: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Figura No 3. Datos e **Información**

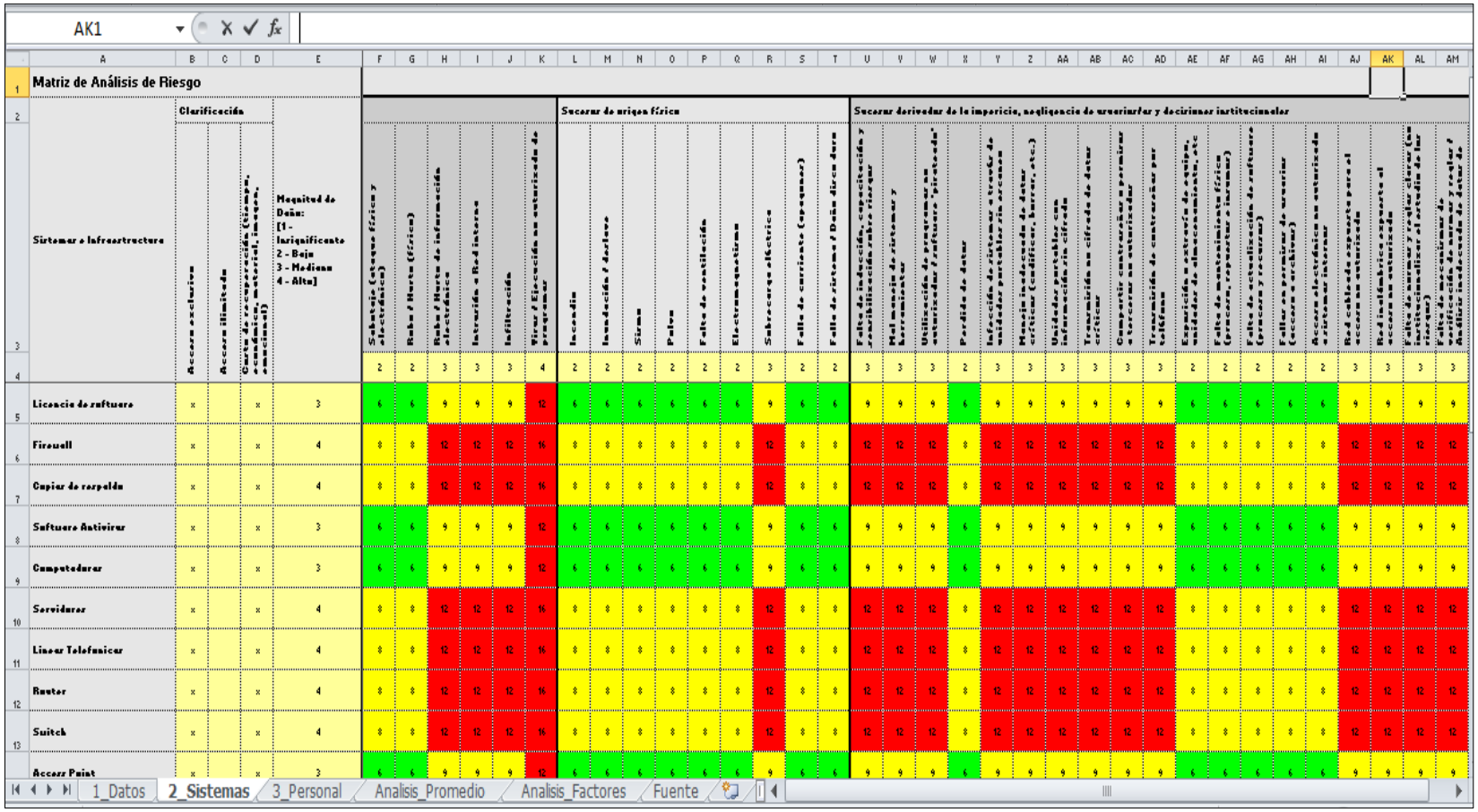


Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																														
	Clasificación										Sucesos de origen físico										Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales														
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de almacenamiento, etc.	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Fallas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas internos	Red cableada expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de
					2	3	3	3	4	2	2	2	2	2	2	3	2	2	3	3	3	2	3	3	3	3	3	3	2	2	2	2	2	3	3	3	
Historias Clinicas	x	x	x	3	6	9	9	9	12	6	6	6	6	6	6	9	6	6	9	9	9	6	9	9	9	9	9	9	6	6	6	6	6	9	9	9	
Bases de datos de los Usuarios.	x		x	4	8	12	12	12	16	8	8	8	8	8	8	12	8	8	12	12	12	8	12	12	12	12	12	12	8	8	8	8	8	12	12	12	
Contratos	x	x	x	3	6	9	9	9	12	6	6	6	6	6	6	9	6	6	9	9	9	6	9	9	9	9	9	9	6	6	6	6	6	9	9	9	
Facturas	x	x		2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4	4	4	4	4	6	6	6	
Registro de Vacunas	x	x		2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4	4	4	4	4	6	6	6	
Registros de Citologia	x	x		2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4	4	4	4	4	6	6	6	
Registros Epidemiologicos	x	x		2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4	4	4	4	4	6	6	6	
Certificaciones	x	x	x	2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4	4	4	4	4	6	6	6	
Lista de Contactos de correos.	x			2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4	4	4	4	4	6	6	6	

1_Datos | 2_Sistemas | 3_Personal | Analisis_Promedio | Analisis_Factores | Fuente

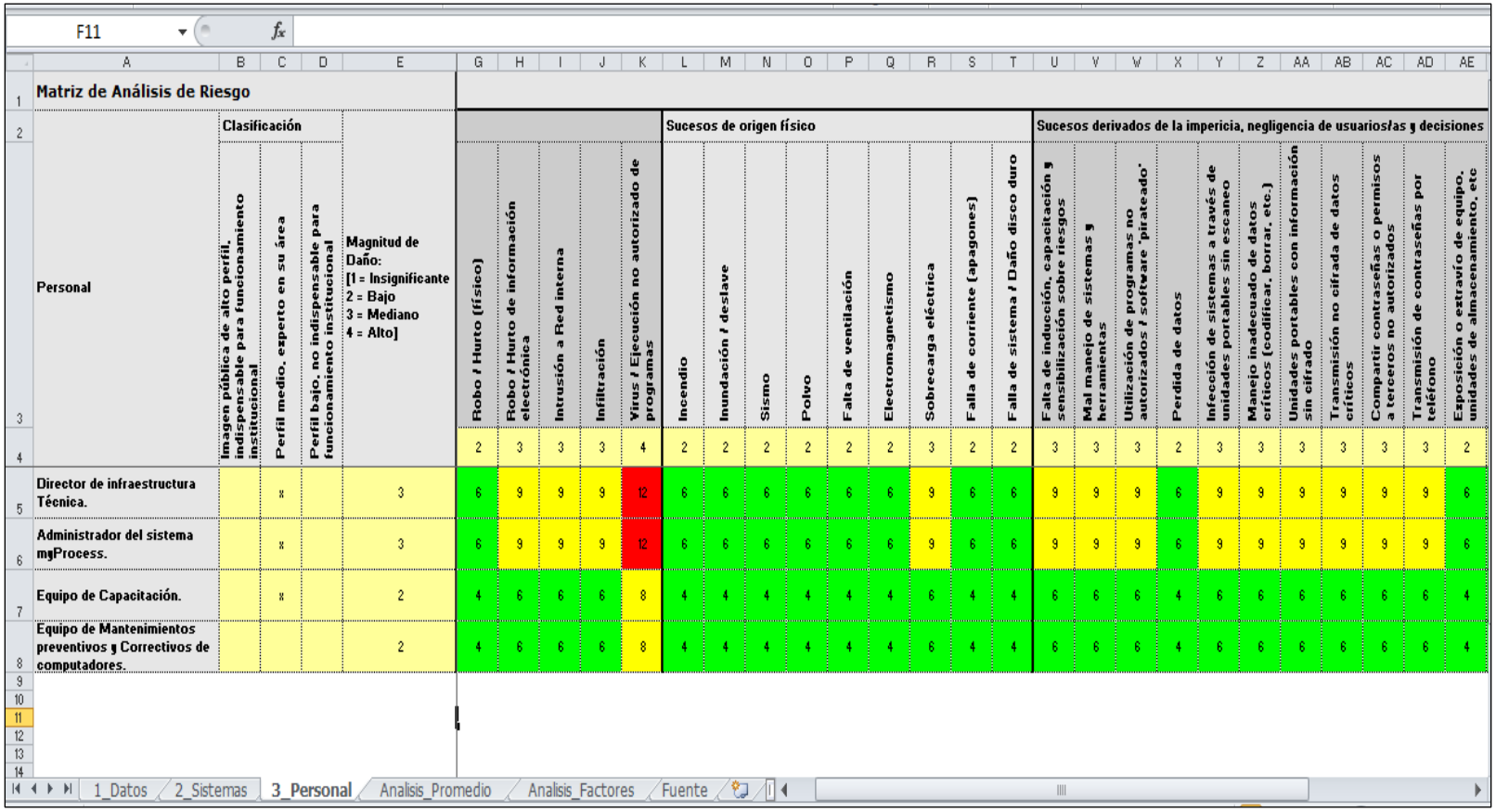
En la **figura No 3**, notamos que hay más puntos verdes que rojo y amarillo, los cual nos indica que el nivel de riesgo es bajo, pero de todas maneras hay que seguir mejorando y emplear mejores controles para mantener un buen sistema de gestión de seguridad.

Figura No 4. Sistemas e Infraestructura



Como vemos en esta matriz donde se evalúa la parte de sistemas e infraestructura hay bastantes puntos rojos, lo cual nos indica que el nivel de riesgo con respecto a las amenazas es bastante alto y puede provocar desarticulación en la entidad, los cuales dan soporte al sistema de información myProcess.

Figura No 5. Personal



	A	B	C	D	E	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE
1	**Matriz de Análisis de Riesgo**																													
2		**Clasificación**									**Sucesos de origen físico**									**Sucesos derivados de la impericia, negligencia de usuarios‡as ¶ decisiones**										
3	**Personal**	**Imagen pública de alto perfil, indispensable para funcionamiento institucional**	**Perfil medio, experto en su área**	**Perfil bajo, no indispensable para funcionamiento institucional**	**Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]**	**Robo ⁄ Hurto (físico)**	**Robo ⁄ Hurto de información electrónica**	**Intrusión a Red interna**	**Infiltración**	**Virus ⁄ Ejecución no autorizado de programas**	**Incendio**	**Inundación ⁄ deslave**	**Sismo**	**Polvo**	**Falta de ventilación**	**Electromagnetismo**	**Sobrecarga eléctrica**	**Falla de corriente (apagones)**	**Falla de sistema ⁄ Daño disco duro**	**Falta de inducción, capacitación ¶ sensibilización sobre riesgos**	**Mal manejo de sistemas ¶ herramientas**	**Utilización de programas no autorizados ⁄ software 'pirateado'**	**Perdida de datos**	**Infección de sistemas a través de unidades portables sin escaneo**	**Manejo inadecuado de datos críticos (codificar, borrar, etc.)**	**Unidades portables con información sin cifrado**	**Transmisión no cifrada de datos críticos**	**Compartir contraseñas o permisos a terceros no autorizados**	**Transmisión de contraseñas por teléfono**	**Exposición o extravío de equipo, unidades de almacenamiento, etc**
4						2	3	3	3	4	2	2	2	2	2	2	3	2	2	3	3	3	2	3	3	3	3	3	3	2
5	**Director de infraestructura Técnica.**		x		3	6	9	9	9	12	6	6	6	6	6	6	9	6	6	9	9	9	6	9	9	9	9	9	9	6
6	**Administrador del sistema mµProcess.**		x		3	6	9	9	9	12	6	6	6	6	6	6	9	6	6	9	9	9	6	9	9	9	9	9	9	6
7	**Equipo de Capacitación.**		x		2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4
8	**Equipo de Mantenimientos preventivos ¶ Correctivos de computadores.**				2	4	6	6	6	8	4	4	4	4	4	4	6	4	4	6	6	6	4	6	6	6	6	6	6	4
9																														
10																														
11																														
12																														
13																														
14																														

1_Datos | 2_Sistemas | 3_Personal | Analisis_Promedio | Analisis_Factores | Fuente

En esta sección de personal notamos solamente dos puntos rojos y varios verdes y amarillos, esto nos indica que el nivel de riesgo es bajo, y que el trabajo que realiza el personal de trabajo con respecto a las amenazas que pueden existirse puede decir que es bueno.

4. DIAGNOSTICO FINAL

Luego de identificar una serie de hallazgos en la auditoría realizada a la seguridad lógica del sistema de información myProcess de la E.S.E. Hospital Emiro Quintero Cañizares, se puede ver que la entidad no está implementando y cumpliendo adecuadamente con los dominios y controles de la norma ISO/IEC 27002 del 2013, la cual establece como se debe manejar un buen sistema de gestión de seguridad de la información y los beneficios que esta trae para una entidad.

Teniendo en cuenta la seguridad de la información y los hallazgos encontrados podemos deducir que en un 80% la empresa no está cumpliendo adecuadamente con la seguridad de la información, se encontraron muchas falencias como:

La entidad de salud del estado hospital Emiro Quintero Cañizares no cuenta con políticas de seguridad para el manejo del sistema de información myProcess, tampoco con políticas para control de acceso a la información, provocando así ataques interno y externos que conlleven a un desastre en el sistema.

Aparte de lo dicho anteriormente la empresa no mantiene un grupo personas especializadas para realizar capacitaciones sobre el mal uso de la información, virus, confidencialidad y cambios que se realizan en el sistema, para evitar daños en los activos de información.

De tal forma que la crisis en la seguridad de la información es bastante alta y en cualquier momento la empresa puede quedar en jaque y si es posible sin servicio ya que sus niveles de seguridad no son los apropiados para dar un buen uso de la información.

5. CONCLUSIONES

Una vez desarrollado todo este proyecto podemos evidenciar que se realizo un diagnóstico de la seguridad del Sistema de Información **myProcess** que da soporte a los servicios que presta el E.S.E Hospital Emiro Quintero Cañizares, también una evaluación de riesgos asociados a la seguridad del sistema de Información **myProcess** y por último se Elaboró el informe de Auditoria, llegando a mostrar el nivel de seguridad que tiene el sistema y las consecuencia de mal manejo para toda la entidad y el servicio a la comunidad.

De acuerdo al diagnóstico realizado a la E.S.E Hospital Emiro Quintero Cañizares, se pudo identificar que no cuenta con un Sistema de Gestión de Seguridad de la Información, situación que lo hace altamente vulnerable, dado que las probabilidades de ocurrencia y la posibilidad de que un evento adverso (externo o interno) obstaculice el logro de objetivos y metas institucionales sea grave; impacto desfavorable para la Empresa, teniendo en cuenta la relevancia de la Institución para la región y el servicio público que presta a la comunidad. Por tal motivo se hace necesario e indispensable realizar controles, que conlleven a mitigar los riesgos.

El servicio que presta la Entidad es para todas aquellas personas de la área urbana, rural y Municipios aledaños, dándole un alto grado de responsabilidad con la población, que entre otras, son personas con una situación socioeconómica baja, lo que puede acarrear descontento, si el servicio prestado no es oportuno y se identifican fallas de tipo humano y tecnológico. Las consecuencias para la Institución y los usuarios serían graves, dado que se vería seriamente afectada la imagen de la Empresa, los usuarios perderían tiempo y dinero, generando problemas legales, económicos y financieros a la Institución.

6. RECOMENDACIONES

Gestionar los recursos económicos para crear el Departamento de Sistemas o Informática, dada la capacidad de la Empresa y la relevancia del servicio que presta, como garante de la del Derecho a la Salud en la Región.

Implementar el diseño de Políticas de seguridad empleadas para garantizar el Buen Uso del sistema de información myProcess, de esta manera también realizar formatos de Seguimiento a las Copias de Seguridad, Inscripción a las Capacitaciones, además implementar un Plan de Contingencia con el propósito de mejorar el sistema de seguridad de la información en la entidad.

Socializar al interior por partes de los ingenieros de sistemas y entes importantes de la institución, el diagnóstico de los Riesgos identificados en la Empresa E.S.E. Hospital Emiro Quintero Cañizares, en lo que compete a la implementación del Sistema de Gestión de Seguridad de la Información, con el objeto de que interioricen, la necesidad de implementar un proceso sistemático seguro, documentado y conocido por toda la organización, que permita preservar la confidencialidad, integridad y disponibilidad de la información.

Estudiar la posibilidad de gestionar la asignación de recursos para la compra de una planta eléctrica de mayor capacidad para el suministro de energía en caso de que se presente deficiencia en el fluido eléctrico y evite suspensión de actividades, perdida de la información, la prestación de servicio y daño en equipos tecnológicos.

Gestionar recursos económicos para brindar capacitaciones constantes a todos los usuarios de la entidad en el buen uso de la seguridad de la información y los controles que se deben tener para seguir mejorando.

Presupuestar la adquisición de un servidor remoto que tenga como función el almacenamiento del Backups (Copia de seguridad), que permita guardar periódicamente la información y recuperarlas en diferentes eventos tales como catástrofe informática, natural o ataque, que puedan haberse eliminado accidentalmente, infectado por un virus u otras causas.

BIBLIOGRAFIA

MONTE DE PAZ**,** Marta.calidad y seguridad de la información y auditoría Informática. España: Universidad Carlos III de Madrid escuela politécnica superior. Faculta de Ingenierías. 2010.259 p.

ROMERO, Oscar Arnulfo. Auditoria a los sistemas informáticos del hospital de ciudad barrios, Universidad Estatal a Distancia. Facultad de Ingenierías. 2009.60 p.

DEL PESO NAVARRO, Emilio; DEL PESO, Mar; PIATTINI VELTHUIS, Mario G. Auditoria de Tecnologías y Sistemas de información. México, Universidad Alfa omega Ra-Ma. 2008.135 p.

VILLAR BARRIO, José Francisco. La auditoría de los sistemas de gestión de calidad, FC Editorial, Agosto 1999.220 p.

MEZA CERVANTES, Rosalba. Administración de centros de cómputo: Unidad IV-Seguridad Lógica. 210 p.

DE MONTES, Pedro. Estudio sobre la seguridad física y lógica. Universidad Estatal a Distancia. Auditoria Interna. 320 p.

ZORAIDA, Eliza. Seguridad en el comercio electrónico, Capitulo II, Facultad de Ingenierías. 85 P.

SCHÜTZ, Seguridad física y lógica. Santiago de Chile. Universidad de los lagos. Facultad de Ingenierías. 2010. 148 p.

ISO/IEC 27002:2013, Information Technology – Security techniques Code of practice for security management.

REFERENCIAS DOCUMENTALES ELECTRONICAS

Auditoría ISO 27002.
https://www.s2grupo.es/auditoria_iso27002.php

Auditoría Integral y seguridad de sistemas de información LTDA.
http://www.audisis.com/

Sistema de gestión de seguridad de la información ISO/IEC 27001
http://www.tuvsud.es/uploads/images/13506354580193723904 09/pdf2-0039-iso-iec-27001-es-260412.pdf

Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009.
<http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm

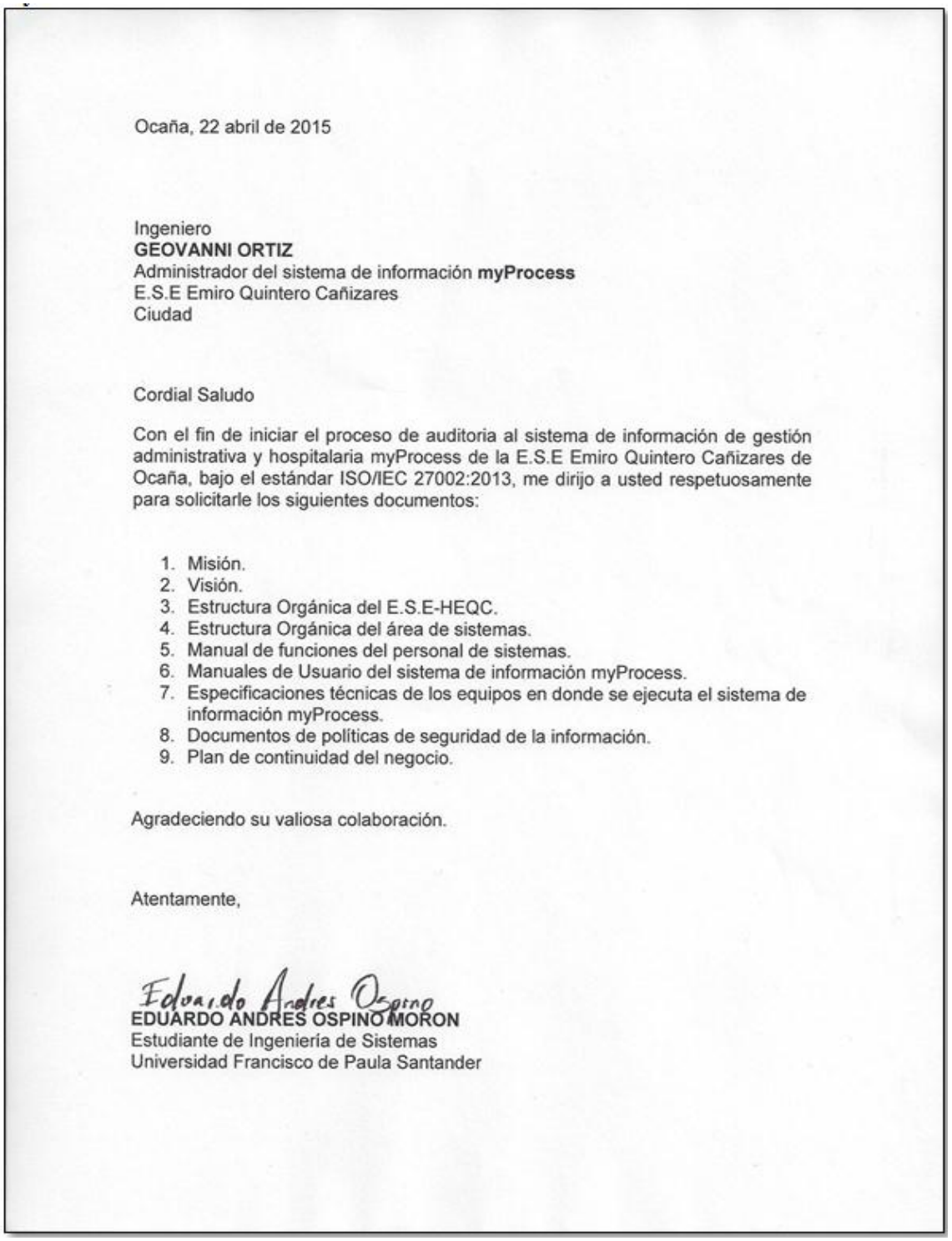
Auditoria a la Seguridad Lógica.
https://prezi.com/-n16dhzu17aa/auditoria-de-la-seguridad-logica/

Auditoria informática: c o n t r o l e s de la auditoria informática. (2009).
https://www.u-cursos.cl/ieb/2009/1/0718/255001/material.../18815

Seguridad Lógica y Confidencial
http://muziek-film-kunst.blogspot.com/2011/01/seguridad-logica-y-confidencial.html

ANEXOS

Anexo A. Solicitud de información inicial al administrador del S.I. myProcess .



Ocaña, 22 abril de 2015

Ingeniero
GEOVANNI ORTIZ
Administrador del sistema de información **myProcess**
E.S.E Emiro Quintero Cañizares
Ciudad

Cordial Saludo

Con el fin de iniciar el proceso de auditoria al sistema de información de gestión administrativa y hospitalaria myProcess de la E.S.E Emiro Quintero Cañizares de Ocaña, bajo el estándar ISO/IEC 27002:2013, me dirijo a usted respetuosamente para solicitarle los siguientes documentos:

1. Misión.
2. Visión.
3. Estructura Orgánica del E.S.E-HEQC.
4. Estructura Orgánica del área de sistemas.
5. Manual de funciones del personal de sistemas.
6. Manuales de Usuario del sistema de información myProcess.
7. Especificaciones técnicas de los equipos en donde se ejecuta el sistema de información myProcess.
8. Documentos de políticas de seguridad de la información.
9. Plan de continuidad del negocio.

Agradeciendo su valiosa colaboración.

Atentamente,

Eduardo Andres Ospino

EDUARDO ANDRES OSPINO MORON
Estudiante de Ingeniería de Sistemas
Universidad Francisco de Paula Santander

Anexo B. Entrega de documentación por parte de la E.S.E-H.E.Q.

GOBERNACIÓN DE NORTE DE SANTANDER

INSTITUTO DEPARTAMENTAL DE SALUD

E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES

NIT. 890501438-1

Gobernación de Norte de Santander

Ocaña, 23 abril de 2015

Pasante
EDUARDO ANDRES OSPINO MORON
Estudiante de Ingeniería de Sistemas
UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
Ciudad

Cordial Saludo.

Dando respuesta a su solicitud le informo que puedo colaborarle con los siguientes documentos:

1. Misión.
2. Visión.
3. Estructura Orgánica del E.S.E-HEQC.
4. Plan de continuidad del negocio.
5. Especificaciones técnicas de los equipos en donde se ejecuta el sistema de información myProcess.

Cabe resaltar que algunos documentos no los tenemos hechos (6, 7,9) y otros como (8) apenas se están haciendo.

6. Estructura Orgánica del área de sistemas.
7. Manual de funciones del personal de sistemas.
8. Manuales de Usuario del sistema de información myProcess.
9. Documentos de políticas de seguridad de la información.

Atentamente,

Geovanny Ortiz Sánchez

GEOVANNY ORTIZ
Ing. Administrador de Software myProcess.

Calle 7 No. 29-144 Barrio La Primavera PBX (097) 5636330 – fax: 5611435
Urgencias 5611940 E-mail: info@hospitaleqc.gov.co Web: www.hospitaleqc.gov.co
Ocaña, Norte de Santander

Anexo C. Entrevista al administrador del sistema de información myProcess - Política de control de acceso

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS OCAÑA

R/PT ENT01

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares — Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Ing. Geovanny Ortiz

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la existencia de una política de control de acceso a la información y al sistema de información myProcess que soporta las actividades de gestión administrativa y hospitalaria.

PREGUNTAS

1. ¿Existe una política de control de acceso claramente definida que contenga los requerimientos de seguridad de los activos de información del E.S.E. Emiro quintero cañizares?

   No

2. ¿Existen procedimientos para gestionar las altas y bajas en el registro de usuario?

   Si

3. ¿Cómo se administran?

   Como Administrador del Sistema asigno permisos a los usuarios, de esa manera gestiono las altas, las bajas por lo general no se dan, ya que un usuario no se elimina, si no que se le restringen los permisos.

4. ¿Cómo se admistran los privilegios de acceso al S.I myProcess?

Se administran por medio de asignación de permisos, dependiendo el rol del usuario que quiere acceder al Sistema.

5. ¿Existe un procedimiento formal que se les proporcione a los usuarios del sistema que enuncie sus derechos de acceso?

NO.

6. ¿Cada cuánto se revisan y cambian los derechos de acceso a los usuarios?

Cada vez que el usuario lo solicite.

7. ¿Qué procedimiento existe para administrar los derechos de acceso de los usuarios que han cambiado de puesto de trabajo o han terminado su contrato laboral?

El usuario se desabilita del sistema, de esta manera se administran sus derechos de acceso.

8. ¿Existen acuerdos de confidencialidad para los usuarios del sistema de información?

NO.

9. ¿Existen usuarios con privilegios especiales?

Solamente el administrador y algunos usuarios que tienen un determinado perfil profesional.

10. ¿Cada cuánto son revisados estos privilegios especiales?

Cada 3 meses

11. ¿Se ha capacitado a los usuarios en el uso de buenas prácticas de seguridad de la información que tiene a su cargo?

Sí, pero pocas veces.

Eduardo Ospino
EDUARDO ANDRES OSPINO MORON
Estudiante encargado Auditoria
Entrevistador

Geovanny Ortiz Sánchez
GEOVANNY ORTIZ
Ing. Administrador del Software myProcess
Entrevistado

Anexo D. Entrevista al Personal de Trabajo de la E.S.E-H.E.Q.C.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS OCAÑA

R/PT ENT01

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

Asignación de citas, Correos institucionales, Verificación de pacientes en el Fosiga y Sisben.

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

No.

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

Si

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

No.

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?
Si
6. ¿Cuánto tiempo lleva manejando el sistema?
1 AÑO
7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?
2 Veces al año, ella misma realiza el Cambio.
8. ¿Recibe usted notificación formal de los cambios de contraseñas?
No.
9. ¿Las funciones del sistema que no debe utilizar están restringidas?
Si
10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?
Si, Cuando se instalan Software nuevo o equipos
Eduardo Ospino **EDUARDO ANDRES OSPINO MORON** Auditor Entrevistador Duke Mario Vila G. Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS. OCAÑA

R/PT ENT02

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC
Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

Ubicación, registro de la información que se consigna de los pacientes que existen a control de crecimiento y desarrollo.

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

NO, en su totalidad.

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

Si, se poseen dos (2) contraseñas por usuario para poder registrar la información. sugerencia: Registrar al usuario con la misma contraseña.

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

NO.....

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

NO.....

6. ¿Cuánto tiempo lleva manejando el sistema?

tres (3) meses

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

NO aplica.

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

NO aplica.

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

NO aplica.

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

SI, eventualmente.

Eduardo A. Ospino Morón.

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Oscar Ospino

Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS OCAÑA

R/PT ENT02

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

llenar historias de interconsultas, registrar los pacientes

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

No, mas o menos

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

Si.

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

NO.

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

Si, por encima

6. ¿Cuánto tiempo lleva manejando el sistema?

5 meses

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

Nunca, no aplica

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

NO.

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

Si.

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

NO.

Eduardo Andres Ospino.

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS. OCAÑA

R/PT ENT01

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

   Cierro ingresos y capacito a los medicos

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

   Si

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

   NO

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

   NO.

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

Si

6. ¿Cuánto tiempo lleva manejando el sistema?

2 meses

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

Nunca

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

No.

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

Si

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

Si

Eduardo Andres Ospino

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS OCAÑA

R/PT ENT02

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC
Fecha: 01/05/2015

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

capasitaciones, buscar errores al programa

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

Sí

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

NO

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

NO.

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

SÍ

6. ¿Cuánto tiempo lleva manejando el sistema?

un Mes y 10 días

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

Cada Mes

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

SÍ

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

SÍ

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

SÍ

Eduardo Andres Ospino

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Jesús Fabian Zumbrano Q.

Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS. OCAÑA

R/PT ENT01

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC
Fecha: 01/05/2015

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

Notas de Jefatura, Registrar procedimientos, Sigun citas.

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

NO, en su totalidad.

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

Si.

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

NO

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

Si.

6. ¿Cuánto tiempo lleva manejando el sistema?

8 Meses.

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

Nunca.

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

NO.

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

Si

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

Si

Eduardo Ospino

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT ENT02

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

   Manejo de historias clinicas de control prenatal.

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

   Si.

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

   Si.

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

   Si.

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?
Si.
6. ¿Cuánto tiempo lleva manejando el sistema?
7 meses
7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?
Nunca.
8. ¿Recibe usted notificación formal de los cambios de contraseñas?
No.
9. ¿Las funciones del sistema que no debe utilizar están restringidas?
Si.
10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?
Si.
Eduardo Andres Ospino. **EDUARDO ANDRES OSPINO MORON** Auditor Entrevistador Alvaro Carriazo k Entrevistado Jefe.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

EN EL FUTURO DE TODOS OCAÑA

R/PT ENT01

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

dipsto Notas de enfermera, registro medicamentos revisa ordenes medicas.

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

Conosko la mayorr de funciones.

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

Si

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

No

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?
No.
6. ¿Cuánto tiempo lleva manejando el sistema?
desde que inicio más o menos 8 meses.
7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?
Nunca
8. ¿Recibe usted notificación formal de los cambios de contraseñas?
No.
9. ¿Las funciones del sistema que no debe utilizar están restringidas?
Si
10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?
Si
Eduardo Andres Ospino. **EDUARDO ANDRES OSPINO MORON** Auditor Entrevistador Gloria Amparo Acevedo. Jefe. Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT ENT02

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

Capacitacion, errores al programa (buscar)

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

Si

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

No

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

Si

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

Si

6. ¿Cuánto tiempo lleva manejando el sistema?

Un mes

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

Cada mes

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

No

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

Si

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

Si

Eduardo Andres Ospino M

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Jhon Alexander Alvarez

Entrevistado

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS. OCAÑA

Entrevista. R/PT ENT02

Empresa: E.S.E. Emiro Quintero Cañizares

Área o Proceso: Sistemas Fecha: 01/05/2015

Aplicada a: Personal de Trabajo de la E.S.E-HEQC

Auditor: Eduardo Andrés Ospino Morón

Objetivo

Verificar la implementación de la política de control de acceso y el conocimiento que los usuarios tienen sobre la misma.

PREGUNTAS

1. ¿Qué funciones realiza en el sistema **myProcess**?

   - Revisión de ordenes.
   - Revisión de Notas de ENF y Supervisión.
   - Revisión de Hojas y Hos a seguir

2. ¿Conoce usted en su totalidad las funciones del módulo o sistema que maneja?

   NO. Solo lo esencial

3. ¿Posee usted un usuario y contraseña para acceder al sistema?

   Si.

4. ¿Recibe formalmente por escrito la información relacionada con el acceso al sistema y las tareas que puede o no realizar en el mismo?

   NO.

5. ¿En el momento de su contratación le dan a conocer las actividades y responsabilidades en el manejo de la información que tendrá a su cargo y de las sanciones que acarrea el incumplimiento de las mismas?

NO. Parcialmente recibi intormación de su uso.

6. ¿Cuánto tiempo lleva manejando el sistema?

1 año.

7. ¿Cada cuánto es cambiada la contraseña de acceso al sistema y quien realiza este cambio?

hasta el momento no lahe cambiado.

8. ¿Recibe usted notificación formal de los cambios de contraseñas?

NO se han cambiado.

9. ¿Las funciones del sistema que no debe utilizar están restringidas?

algunas.

10. ¿Ha recibido capacitación en el uso seguro de la información y de los equipos que tiene a su cargo?

NO.

Eduardo Andres Ospina
EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Entrevistado

Anexo E. Entrevista al administrador de myProcess para evaluar la existencia de controles de acceso.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS OCAÑA

R/PT ENT03

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 01/05/2015
Área o Proceso: Sistemas
Aplicada a: Ing. Geovanny Ortiz
Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la existencia de controles de acceso que dan soporte al buen uso del sistema de información myProcess.

PREGUNTAS

1. ¿Son controlados los accesos a otras aplicaciones diferentes de myProcess?

NO.

2. ¿Existen procedimientos formales para manejar el control de acceso a myProcess y aplicaciones necesarias para su funcionamiento?

NO, estos procedimientos formales no existen para el control de acceso a myProcess.

3. ¿Existen controles para el acceso no autorizado a myProcess?

Si, se restringe por medio de un Usuario y contraseña.

4. ¿Cómo se manejan?

Se manejan por medio de un usuario y contraseña, tambien se restringen los privilegios de acceso al software.

5. ¿Al hacer actualizaciones al sistema de información myProcess tiende a comprometer la integridad de otros sistemas de información?
Algunas Veces. Se dan errores pequeños, pero son Solucionados inmediatamente.
6. ¿Existe restricciones de acceso a los usuarios para acceder al código fuente del sistema del sistema de información myProcess?
Si
7. ¿Cómo se maneja esta seguridad?
En el software se manejan restricciones de todo tipo, dentro de esas restricciones esta el no acceso al codigo fuente del software.

Eduardo Ospino Morón
EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Geovanny Ortiz Sánchez
GEOVANNY ORTIZ
Ing. Administrador del Software myProcess
Entrevistado

Anexo F. Entrevista para verificar la existencia de políticas preventivas y correctivas de código malicioso

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

OCAÑA

R/PT ENT04

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 14/05/2015
Área o Proceso: Sistemas
Aplicada a: Ing. Yolimer Arévalo Claro

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la existencia de controles preventivos y correctivos contra el código malicioso que pueda afectar al sistema de información.

PREGUNTAS

1. ¿Existen políticas formales preventivas y correctivas que prohíban el uso de software no autorizado al sistema?

   No, muy poco

2. ¿Los usuarios que utilizan el sistema de información la conocen y la aplican?

   No las conocen, pero si existen

3. ¿Se realizan capacitaciones de prevención a los usuarios para evitar los ataques por virus, robo de información, malware y demás códigos maliciosos?

   muy pocas veces

4. ¿Existen políticas disciplinarias para los usuarios que no hacen caso omiso al uso de medios informáticos que pueden poner en riesgo la información por códigos maliciosos?

No hay en el momento.

5. ¿Cuándo se manifiesta amenazas como virus u otro tipo de ataque mal intencionado, como se maneja?

Se realiza el procedimiento de desinfección de Archivos y luego una Copia de Seguridad.

6. ¿Existen revisiones constantes a la data que sostienes los procesos que se realizan a diario para evitar código malicioso?

Si se hacen revisiones Constantes

7. ¿Cada cuánto se realizan?

Cada mes.

8. ¿Qué tipo de seguridad a nivel de software y hardware se utiliza para contrarrestar software mal intencionado?

Software Antivirus
Dispositivo Fisico Firewall

9. ¿Existen restricciones o bloqueos para los usuarios que entran a internet a páginas inseguras, juegos y demás elementos que ponen en riesgo la seguridad de la información?

Si, por medio del Firewall.

10. ¿Se realizan chequeos de cualquier archivo en medios electrónico u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo?

Si se realizan, pero en pocas Ocasiones.

Eduardo Ospino

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

YOLIMER AREVALO CLARO
Ing. de Infraestructura Técnica
Entrevistado

Anexo G: Lista de chequeo, eficiencia de los controles implementados para contrarrestar código malicioso.

LISTA DE CHEQUEO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT CHL01

Empresa: **E.S.E. Emiro Quintero Cañizares**
Área o Proceso: **Sistemas**
Fecha: 14/05/2015

Objetivo
Realizar comprobación de la eficiencia de los controles implementados para contrarrestar la presencia de código malicioso.

No.	ELEMENTOS	CRITERIO DE EVALUACIÓN			R/PT	AUDITOR
1	Software Antivirus	EXISTE SI X NO ___	ACTUALIZADO SI X NO ___	FUNCIONAMIENTO B X R ___ M ___ N ___	AFO01	E.A.O.M
2	Software Antispyware	EXISTE SI ___ NO X	ACTUALIZADO SI ___ NO X	FUNCIONAMIENTO B ___ R ___ M ___ N X		
3	Dispositivo Físico Firewall	EXISTE SI X NO ___	ACTUALIZADO SI X NO ___	FUNCIONAMIENTO B ___ R X M ___ N ___	AFO02	
4	Windows Update	ACTIVADO SI X NO ___	ACTUALIZADO SI X NO ___	FUNCIONAMIENTO B X R ___ M ___ N ___	AFO03	
5	Servidor Proxy	EXISTE SI ___ NO X	ACTUALIZADO SI ___ NO X	FUNCIONAMIENTO B ___ R ___ M ___ N X		
6	VPN(Red Privada Virtual)	EXISTE SI ___ NO X	ACTUALIZADO SI ___ NO X	FUNCIONAMIENTO B ___ R ___ M ___ N X		

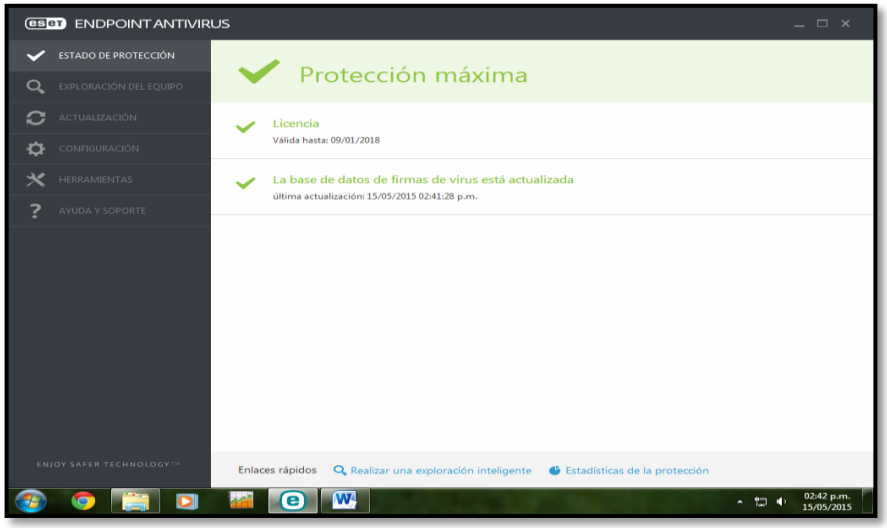
MARCAS O TILDES UTILIZADAS

CHL01: Lista de Chequeo No. 1
E.A.O.M: Eduardo Andrés Ospino Moron – Auditor
AFO01: Archivo Fotográfico No.1
AFO02: Archivo Fotográfico No.2
AFO03: Archivo Fotográfico No.3

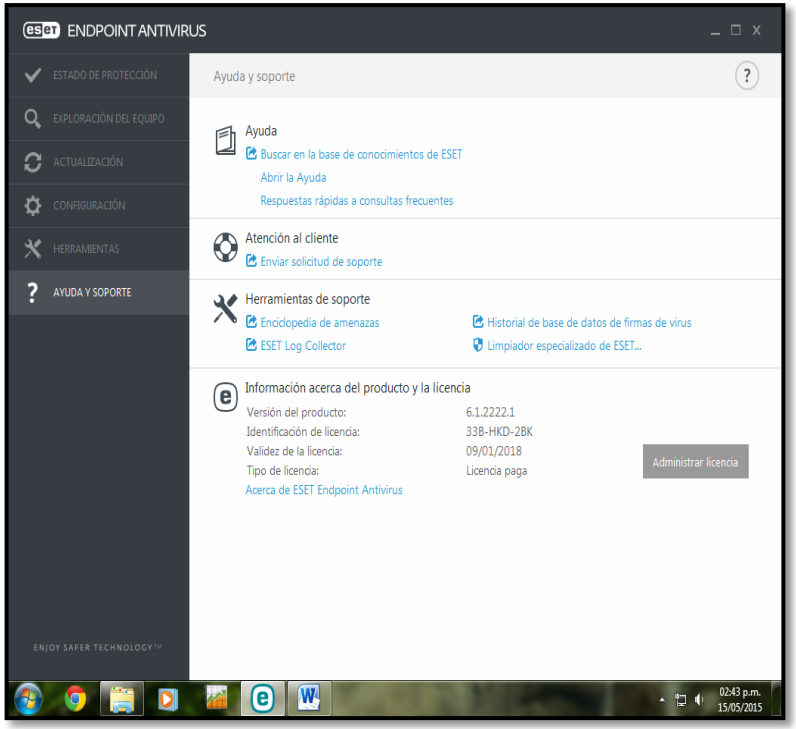
EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

YOLIMER AREVALO CLARO
Ing. de Infraestructura Técnica
Entrevistado

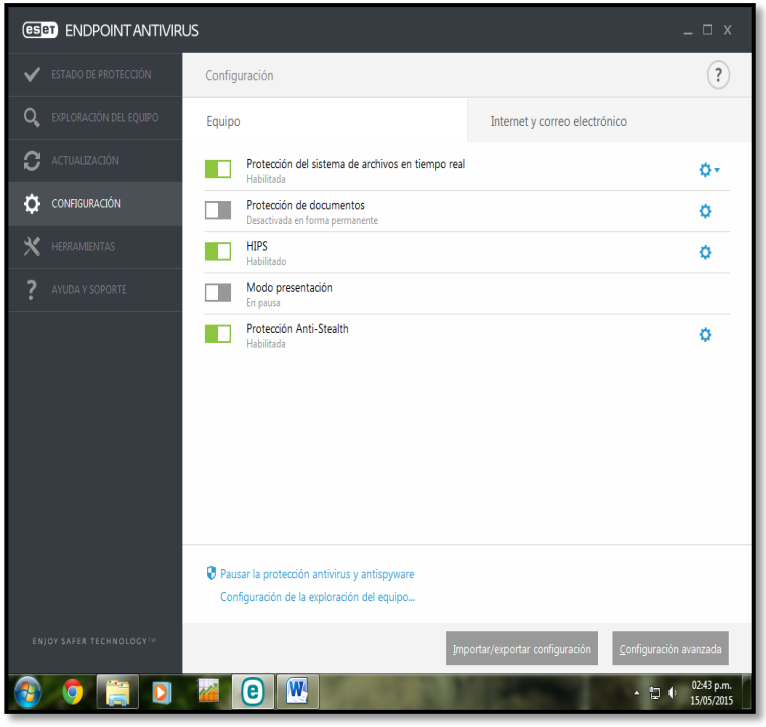
PT. No. **AFO01**



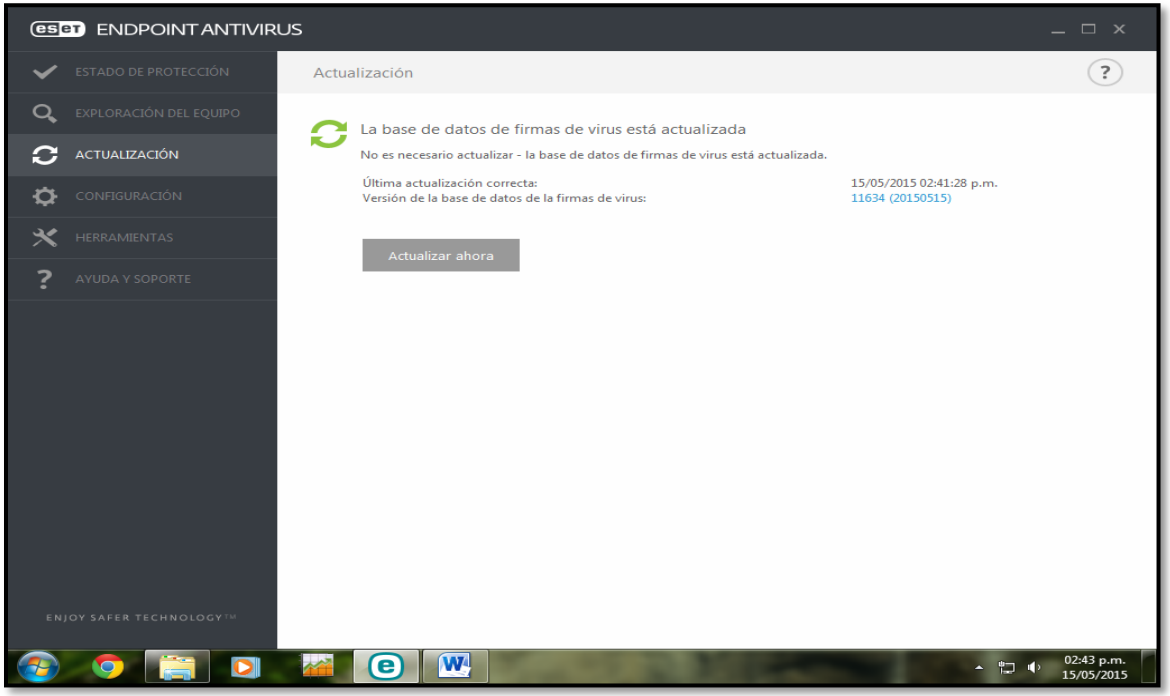
Img01. Pantalla inicial Software Antivirus.



Img02. Ayuda y Soporte de Antivirus

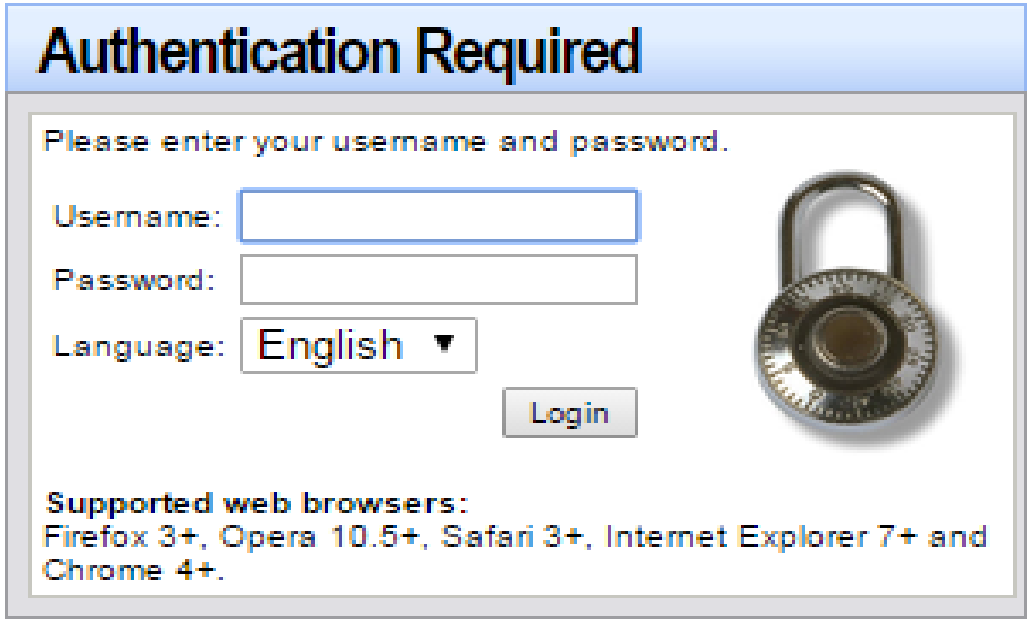


Img03. Configuración de Antivirus.

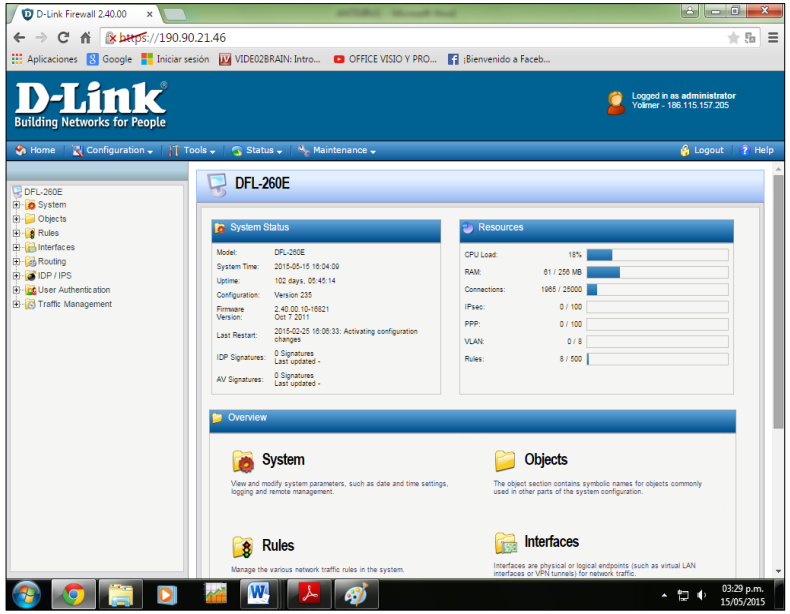


Img04. Software de Antivirus Actualizado.

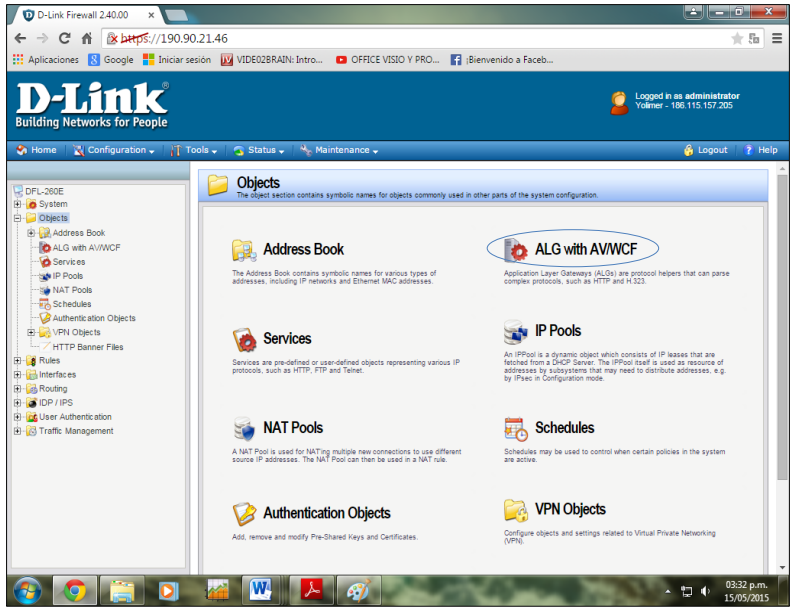
PT. No. **AFO02**



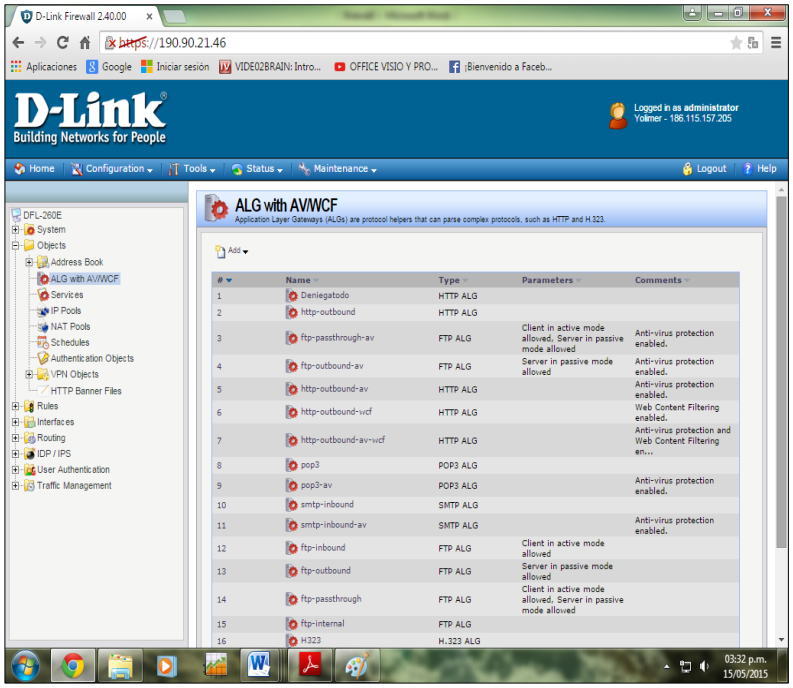
Img05. Pantalla de inicio de sesión del Firewall



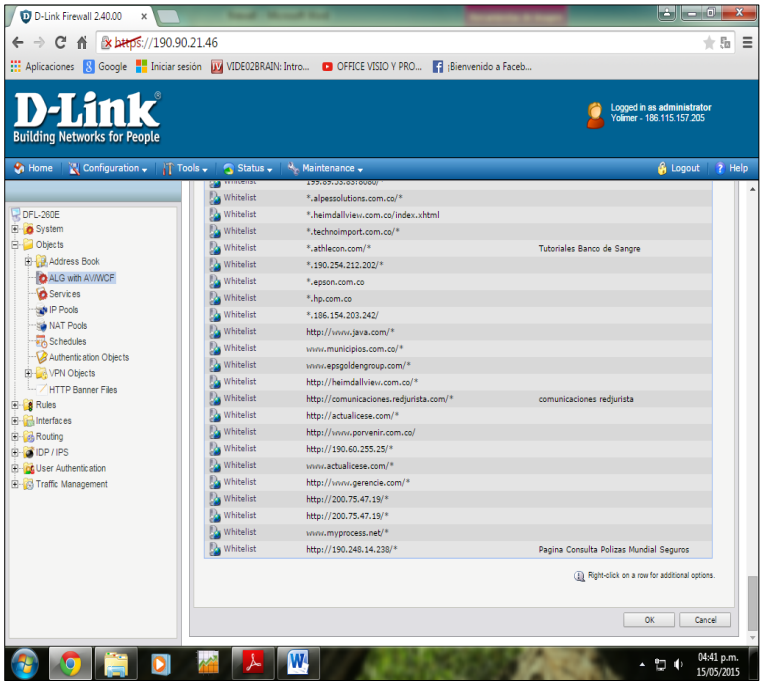
Img06. Menú de herramientas del Firewall.



Img07. Administrador de páginas web (ALG with AV/WCF)

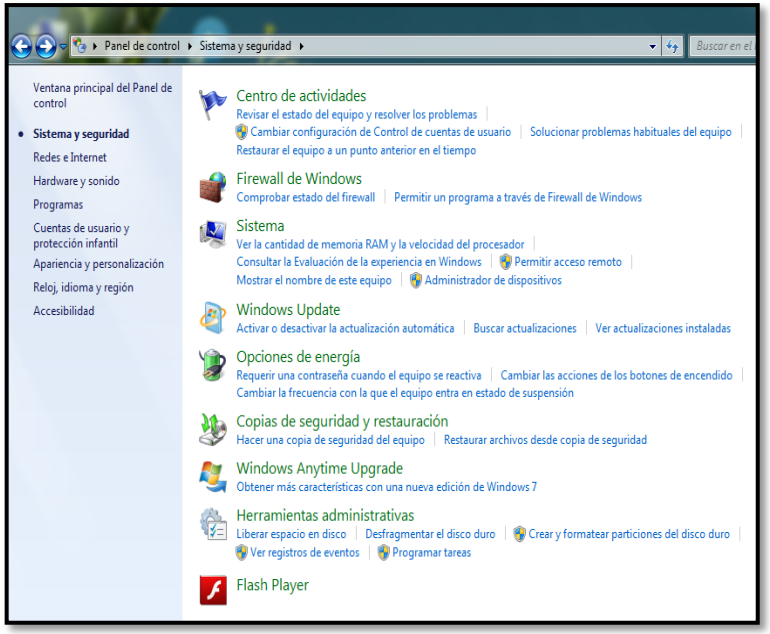


Img08. Opciones de administrador de páginas web

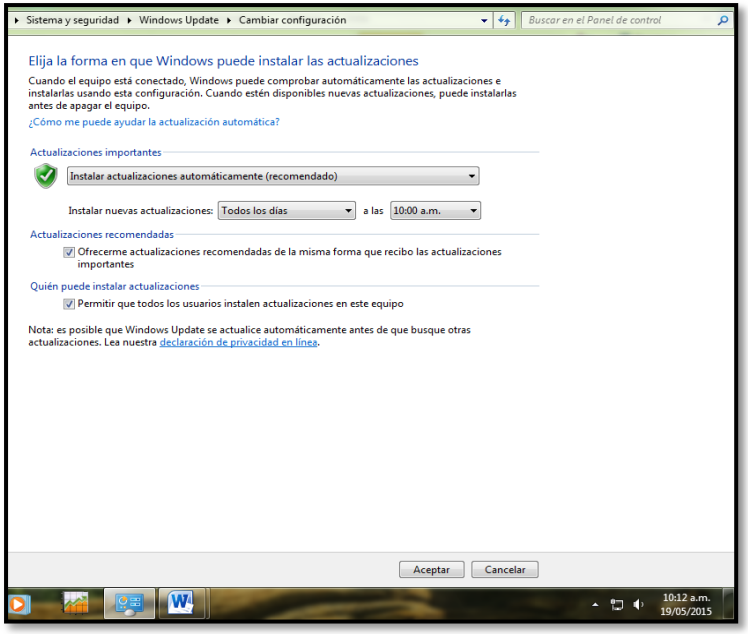


Img09. Páginas web permitidas

PT. No.**AFO03**



Img10. Opciones de Sistema y Seguridad.



Img11. Configuración de actualizaciones automáticas.

Anexo H: Entrevista para verificar la existencia de políticas para realización de copias de respaldo.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT ENT05

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 20/05/2015
Área o Proceso: Sistemas
Aplicada a: Ing. Geovanny Ortiz Sánchez
Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la existencia de una política de realización de copias de respaldo de la data en el sistema de información myProcess.

PREGUNTAS

1. ¿Existen procedimientos formales para la realización y restauración de Back-Up en el sistema de información myProcess?

No, Se lleva un control de las copias de seguridad en el disco duro interno, pero en el momento no realizamos procedimientos formales.

2. ¿Cada cuánto se realizan copias de respaldo en el sistema de información?

Diariamente, aparte de que el servidor realiza una copia cada 30 segundos

3. ¿Dónde son almacenadas estas copias de seguridad?

Son almacenadas en el disco duro interno del computador, en el servidor espejo y en un disco duro externo.

4. ¿Existen un lugar externo a las instalaciones del hospital donde se almacenen las copias de seguridad para los casos en que se presente un siniestro?

No, pero se esta en proceso para almacenarlas en la nube.

5. ¿Quién realiza las copias de respaldo?

El Administrador del Software

6. ¿Existe controles preventivos sobre los medios en los cuales se realizan las copias de seguridad?

Si existen.

7. ¿Qué tipos de controles preventivos manejan?

1. Mantenimiento fisico al computador y al Servidor.
2. Chequeo Constante de su funcionamiento.

8. ¿Cuándo se realizan Back-Up, este es probado para evitar inconvenientes o errores en su restauración?

Si.

9. ¿El acceso a la información contenida en las copias de respaldo, se encuentra restringido?

Si, estan protegidos con una clave de acceso.

10. ¿A que módulos del sistema de información se le realizan copias de respaldo?

Facturación, Historia clinica, pediatria, consulta externa, urgencias pediatricas.

Eduardo Andres Ospino M

EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Geovanny Ortiz Sánchez

GEOVANNY ORTIZ
Ing. Administrador del Software myProcess
Entrevistado

Anexo I: Lista de chequeo para Comprobar la eficiencia de los procedimientos para realización de backups y su restauración.

LISTA DE CHEQUEO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT CHL02

Empresa: **E.S.E. Emiro Quintero Cañizares**
Área o Proceso**: Sistemas**
Fecha: 20/06/2015

Objetivo
Comprobar la eficiencia de los procedimientos de rutina para realización de backups y su restauración.

No	ELEMENTOS	CRITERIO DE EVALUACIÓN				AUDITOR
1	Frecuencia de Realización de Backup	DIARIO X	SEMANAL ___	MENSUAL ___		E.A.O.M
3	Dispositivo de almacenamiento de Backup	CD/DVD ___	DISCO DURO INTERNO X	SERVIDOR X	DISCO DURO EXTERNO X	
4	Tipo de información que se respalda	DATA ___	CONFIGUACION ___	APLICACIONES ___	ALG. MODULOS X	
5	Seguridad de acceso a copias de seguridad	EXISTE SI X NO ___				

MARCAS O TILDES UTILIZADAS
CHL02: Lista de Chequeo No. 2
E.A.O.M: Eduardo Andrés Ospino Morón – Auditor

Eduardo Andres Ospino Morón
EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Geovanny Ortiz Sánchez
GEOVANNY ORTIZ
Ing. Administrador del Software myProcess
Entrevistado

Anexo J: Entrevista para Verificar la existencia e implementación de procedimientos formales, especificación, prueba y control que dan soporte a la seguridad y desarrollo del sistema de información.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

UFPS EN EL FUTURO DE TODOS OCAÑA

R/PT ENT06

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares Fecha: 20/05/2015
Área o Proceso: Sistemas
Aplicada a: Ing. Geovanny Ortiz Sánchez
Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la existencia e implementación de procedimientos formales, especificación, prueba y control que dan soporte a la seguridad y desarrollo del sistema de información myProcess.

PREGUNTAS

1. ¿Existen procedimientos formales para la realización de cambios en los módulos o aplicaciones del sistema de información myProcess?

   NO.

2. ¿los cambios realizados son autorizados o se realizan espontáneamente?

   Algunos Cambios Son autorizados, ya que Se manejan Cambios aveces muy Sencillos.

3. ¿Cuándo se realizan cambios en el sistema es afectada la integridad de software?

   NO.

4. ¿los cambios en el sistema de información son informados al personal de trabajo del HEQC?

   Algunas Veces.

5. ¿Se manejan controles documentados sobre las actualizaciones y versiones del sistema de información myProcess?

Si.

6. ¿Existe horarios especiales para el control de cambios e implementación de estos en el sistema de información myProcess?

Si. Por lo general en horas de la tarde.

7. ¿Existe algún personal capacitado para revisar constantemente los cambios que se realizan en el sistema?

NO.

8. ¿Cada cuánto se realizan cambios y monitoreo en el sistema?

2 Veces a la Semana monitoreo General, los Cambios se dan Constantemente.

Eduardo Andres Ospino.
EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Geovanny Ortiz Sánchez
GEOVANNY ORTIZ
Ing. Administrador del Software myProcess
Entrevistado

Anexo K: Entrevista para Verificar la existencia de controles de acceso a la base de datos que dan soporte al sistema de información myProcess.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS
AUDITORIA AL SISTEMA DE INFORMACION DE GESTION ADMINISTRATIVA Y HOSPITALARIA MYPROCESS DE LA E.S.E EMIRO QUINTERO CAÑIZARES DE OCAÑA, BAJO EL ESTANDAR ISO/IEC 27002:2013

R/PT ENT07

Entrevista.
Empresa: E.S.E. Emiro Quintero Cañizares
Fecha: 20/06/2015
Área o Proceso: Sistemas
Aplicada a: Ing. Geovanny Ortiz Sánchez

Auditor: Eduardo Andrés Ospino Morón

Objetivo
Verificar la existencia de controles de acceso a la base de datos que dan soporte al sistema de información myProcess.

PREGUNTAS

1. ¿Cuál es el motor de base de datos que da soporte al sistema de información myProcess?

SQL Server 2012

2. ¿Aproximadamente cuantas tablas tiene la base de datos del sistema de información?

85 Tablas

3. ¿Qué características tiene el servidor que da soporte al sistema de información myProcess?

Las caracteristicas Tecnicas del Servidor son:
- 32 GB memoria Ram
- 4 Discos duros de un Terabay
- Sistema operativo Windows Server.
- Monitor de 19.5"

4. ¿Cuántos usuarios se conectan de manera simultánea a la base de datos?

Practicamente todos, 611 usuarios.

5. ¿Qué inconvenientes se han presentado en el acceso a la base datos?

Con respecto a la base de datos, hasta el momento no se han presentado inconvenientes.

6. ¿Con que frecuencia se presentan estos casos?

No se han presentado

7. ¿Cómo se da solución a estos inconvenientes?

Hasta el momento no se le ha dado Solución a inconvenientes en el sistema, ya que no se han presentado.

8. ¿Cuál es el tiempo máximo en el que el sistema ha quedado fuera de operación?

8 horas, por motivo de la red, un punto se había caído.

9. ¿De qué manera se ha resuelto?

Se realizo por parte del ingeniero una revisión paso a paso de toda la red, hasta encontrar el daño y se Soluciono de manera inmediata, aunque la perdida de tiempo y trabajo fue bastante.

10. ¿Se han presentado ataques externos o internos al sistema de información myProcess?

No, hasta el momento ningun atague.

11. ¿De qué tipo?

ninguno.

Eduardo Ospino Morón
EDUARDO ANDRES OSPINO MORON
Auditor
Entrevistador

Geovanny Ortiz Sánchez
GEOVANNY ORTIZ
Ing. Administrador del Software myProcess
Entrevistado