ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPPA PARA LA REDUCCIÓN DE RIESGOS EN LA SEGURIDAD EN HOSPITALES NIVEL I DEL IESS

CHRISTIAN FERNANDO BARRAGÁN QUIZHPE

Proyecto de Investigación, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de Magíster en Seguridad Telemática

RIOBAMBA - ECUADOR

Octubre, 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
CERTIFICACIÓN

El Tribunal del PROYECTO DE INVESTIGACIÓN CERTIFICA QUE:
El trabajo de titulación titulado "ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPPA PARA LA REDUCCIÓN DE RIESGOS EN LA SEGURIDAD EN HOSPITALES NIVEL I DEL IESS", de responsabilidad del Ing. Christian Fernando Barragán Quizhpe, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal de Tesis

Ing. Freddy Proaño. PhD.	
PRESIDENTE DEL TRIBUNAL	**FIRMA**
Ing. Vinicio Ramos Valencia Msc.	
DIRECTOR	**FIRMA**
Ing. Oswaldo Martínez. Msc.	
MIEMBRO DEL TRIBUNAL	**FIRMA**
Ing. Fernando Mejía. Msc.	
MIEMBRO DEL TRIBUNAL	**FIRMA**

Riobamba, Octubre 2017

DERECHOS INTELECTUALES

Yo, Christian Fernando Barragán Quizhpe, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el presente Proyecto de Investigación, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

020156720-3

DEDICATORIA

Dedico este trabajo principalmente a Dios y a mis hijos Edwin Fernando y Christian Alexander quienes han sido el motor emocional durante el tiempo que cursaba los estudios de esta maestría y escribía la tesis, a toda mi familia en especial a mi esposa y a mi madre, además de a mis amigos quienes me han brindado su apoyo incondicional para continuar y no desmayar en este nuevo reto que me he planteado y que ahora lo estoy culminando.

Christian Barragán

AGRADECIMIENTO

Agradezco a todos y a cada uno de los maestros que brindaron sus conocimientos y experiencias en las aulas de clases, y de manera muy especial a los miembros del tribunal de tesis que han aportado significativamente en la elaboración de este trabajo. A mis amigos Renny y Fabian con quienes formamos un buen equipo de trabajo durante la maestría y compartimos muchos momentos agradables.

Christian Barragán

ÍNDICE GENERAL

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE GRAFICOS

RESUMEN

Se generó una adaptación de las Normas ISO 27001 e HIPAA (HIPPA) para reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la historia clínica digital que utiliza esta institución. Esta adaptación se realizó tomando en consideración la legislación actual vigente, además de una comparación entre las Normas ISO 27001 e HIPAA; esta adaptación ha sido implementada en el Hospital de Nivel 1 del IESS de Guaranda, con una evaluación efectuada en dos circunstancias; la primera antes de implementar la adaptación de la norma, donde se estableció y ponderó los riesgos a presentarse enfocados a la confidencialidad, integridad, y privacidad de la información, estableciéndose los riesgos más críticos; bajo el mismo criterio y metodología se evaluó luego de la implementación de la norma adaptada. Del estudio realizado se pudo establecer coincidencias de las Normas ISO 27001 e HIPAA en base a la información recolectada de sus características para proteger los activos de información de la organización estableciendo sus ventajas individuales, además de sus desventajas como generalización en el caso de la norma ISO y orientación a seguros de salud de EEUU en las HIPAA, se ha reducido sustancialmente el promedio de ponderación de probabilidad que los riesgos ocurran en un 61,86% frente a la situación inicial, por lo que se recomienda su implementación en Hospitales de Nivel 1 del IESS, previo una evaluación de riesgos para cada Hospital, con el objeto de identificar adecuadamente los riesgos más críticos, generando políticas de seguridad individuales en función a los procesos de cada Unidad Hospitalaria.

Palabras claves: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <TECNOLOGÍA DE LAS COMUNICACIONES>, <SEGURIDAD INFORMÁTICA>, <NORMAS ISO 27001>, <NORMA HIPAA> <HISTORIAS CLÍNICAS>.

ABSTRACT

An adaptation of ISO 27001 and HIPAA (HIPPA) Standards was generated for the reduction of information security risks in the IESS level I hospitals, with the aim of ensuring the confidentiality, integrity and availability of digital clinical history that uses this institution. This adaptation was developed taking into account of current legislation in force, in addition to a comparison between the standards ISO 27001 and HIPAA; this adaptation has been implemented in the Hospital of level 1 of the IESS in Guaranda, with an assessment in two circumstances; The first assessment was before implementing the adaptation of the norm, where it established itself and pondered the risks to be focused on the confidentiality, integrity, and privacy of information, proving the most critical risks; under the same criteria and methodology, it was evaluated after the implementation of the standard adapted. The study could evidence coincidences between the standards ISO 27001 and HIPAA (HIPPA) based on the information collected from its features to protect information assets of the organization by setting their individual advantages. In addition to their disadvantages as a generalization in the case of the ISO standard and guidance to the health insurance in the USA related to the HIPAA, it has substantially reduced the average probability weighting that the risks occur in a 61.86% compared to the initial situation. For that reason, its implementation in hospitals of level 1 of the ISSE it is recommended previous a risk assessment for each Hospital in order to properly identify the most critical risks, generating individual security policies according to the processes of each hospital unit.

KEYWORDS: <TECHNOLOGY AND THE ENGINEERING SCIENCES>, <COMMUNICATIONS TECHNOLOGY>, <COMPUTER SECURITY>, <ISO 27001 STANDARDS>, <HIPAA STANDARD>, <MEDICAL RECORDS>.

CAPÍTULO I

1. INTRODUCCIÓN

Dentro del país no existen estudios sobre la seguridad de la información de los registros médicos en las instituciones de salud, algo se quiere hacer con la implementación del EGSI publicado en el Acuerdo Ministerial 166, pero lamentablemente esta norma es demasiado general y poco aplicable con el sector de la salud.

Por otro lado tenemos las normas estadounidenses HIPAA o también conocida como HIPPA que han sido difundidas a nivel mundial con un buen éxito y que se especializan en asegurar los registros médicos de los pacientes, y que han sido ampliamente analizadas por diferentes artículos científicos donde se las pone a prueba para asegurar la información de los registros médicos.

En el país la falta de una norma o de una política que permita asegurar este tipo de datos, y que no han sido estudiadas estas normas a nivel local, permite que la adaptación de estas normas puede llegar a ser una solución para la reducción de riesgos en el tratamiento de los datos contenidos en las historias clínicas del Ecuador.

1.1. Planteamiento del problema.

Con la implementación de la historia clínica digital en el Instituto Ecuatoriano de Seguridad Social y la posibilidad de ser la única institución pública ecuatoriana que puede acceder a los registros médicos de una persona a nivel nacional, surge la necesidad de reforzar la seguridad de los datos personales de salud para garantizar su privacidad. A pesar de la gran cantidad de medidas de seguridad técnicas y de recomendaciones existentes para el ámbito sanitario plasmadas en ciertas normativas locales, hay un aumento en las violaciones de la privacidad de los datos personales de los pacientes en los centros sanitarios del IESS, en muchos casos como consecuencia de errores o descuidos del profesional de la casa de salud. Es por eso que es necesaria una “Adaptación de las Normas ISO 27001 e HIPPA para la reducción de riesgos de seguridad en Hospitales Nivel I del IESS” con el fin de proporcionar los 3 pilares básicos: confidencialidad, integridad y disponibilidad de la misma

1.2. Situación problemática.

Mediante Acuerdo Ministerial 166 publicado en el Registro Oficial Suplemento 88 de 25-sep-2013 por Cristian Castillo Peñaherrera – Secretario de la Administración Pública, expide el ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI, donde según el Art. 1 se dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información; según Art. 2 indica que la implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información; y que según el Art. 7.- Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013).

La familia de normas ISO 27000 ayuda a las organizaciones a mantener los activos de información seguros, el uso de esta familia de normas ayuda a las organizaciones a administrar la seguridad de los activos como la información financiera, la propiedad intelectual, detalles de los empleados o la información confiada por terceros. La ISO / IEC 27001 es el estándar más conocido de la familia ISO 27000 que proporciona requisitos para un sistema de gestión de seguridad de la información (SGSI), Un SGSI es un enfoque sistemático para la gestión de la información confidencial de la empresa para que siga siendo seguro. Incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgos ("ISO 27001 - Information security management", s/f).

Los riesgos en la seguridad de los sistemas de información en el sector de la salud del Ecuador son altos por la falta de identificación, medición, evaluación y tratamientos de los riesgos o fallas en los sistemas de información provocando como consecuencia la fuga de información vital o publicación datos de los registros médicos de los ecuatorianos por el incumplimiento del EGSI.

Existen normativas específicas para el tratamiento de la información personal de los pacientes como la LOPD (Health Insurance Portability and Accountability Act - Ley Orgánica de Protección de Datos Personales) en España, o la HIPPA (Ley de Portabilidad y Responsabilidad del Seguro Médico) en US, en el Ecuador no existe una normativa o Ley que regule adecuadamente la seguridad de estos datos.

HIPAA[1] protege la privacidad de los registros médicos de los pacientes mediante la prevención de la divulgación no autorizada y el uso inadecuado de la información de salud protegida (PHI[2]) de los pacientes. Con un énfasis significativo y la inversión monetaria en la década de 1990 en la informatización de las operaciones de servicios de salud, la posibilidad de manipulación de datos y el uso secundario sin consentimiento de los registros de identificación personal se ha incrementado enormemente. HIPAA declara PHI "privilegiada", protegiendo a las personas de las pérdidas resultantes de la construcción de sus datos personales. Las empresas sometidas a la ley HIPAA están dirigidas a proteger la integridad, confidencialidad y disponibilidad de la PHI electrónico que recogen para mantener, utilizar y transmitir (Sanchez, Olmo, Alvarez, Medina, & Piattini, 2012).

Según Benitez y Malin, se pueden definir varias métricas de riesgo; para cada estado de Estados Unidos, se estima el riesgo que representa para los conjuntos de datos hipotéticos, protegida por las políticas de HIPAA Safe Harbor y Limited Dataset por un atacante con pleno conocimiento de identificadores de pacientes y con un conocimiento limitado en la forma de registros de electores (Benitez & Malin, 2010). Esta es una base sobre la cual se puede actuar para establecer los riesgos que no han sido identificados en Hospitales Nivel I del IESS.

La falta de una política definida en el sector de la Salud en el Ecuador impide que se pueda cumplir con una correcta aplicación del EGSI que es de cumplimiento obligatorio en las instituciones públicas, y más aún en el sector de la Salud que maneja datos sensibles de los pacientes a los cuales han atendido, la fuga de información o exposición de la información contenida en las historias clínicas de los pacientes puede ser utilizada por personas en favor propio o de terceros, como por ejemplo al hacer uso de datos estadísticos de morbilidad para beneficiar a ciertas farmacéuticas o proveedores de insumos.

1.3. Formulación del Problema

¿Cómo contribuirá la Adaptación de las Normas ISO 27001 e HIPAA, en la reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS?

[1] HIPAA: Health Insurance Portability and Accountability Act

[2] PHI: Protected Health Information

1.4. Preguntas directrices.

- ¿Cuáles son las normativas Ecuatorianas aplicadas en el sector de la salud para seguridad de los sistemas de información?
- ¿Cuáles son las ventajas y desventajas de las Normas ISO 27001 e HIPAA?
- ¿Cómo se pueden adaptar las Normas ISO 27001 e HIPAA, para la asegurar los sistemas de información en Hospitales Nivel I del IESS?
- ¿Cuáles son los riesgos más importantes en la seguridad de los sistemas de información en Hospitales Nivel I del IESS?

1.5. Justificación de la investigación

Teórico

En la cláusula cuarta del convenio marco de la Red Integral Pública de Salud se establece que se debe implementar un sistema informático que permita mantener y acceder a un registro sobre todos los beneficiarios/usuarios de los servicios; el Instituto Ecuatoriano de Seguridad Social a través de sus Unidades Médicas tiene un sistema informático conectado en red donde se puede manejar una historia clínica única tal como lo estable la Ley Orgánica del SNS[3].

Es necesario cumplir con el ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION (EGSI), donde se dispone el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información, estas al ser aplicables a cualquier tipo de ambiente se convierten en muy generales es por eso que se necesita obtener una adaptación de las Normas ISO 27000 con alguna norma que se especialice en el sector de la Salud; las normas HIPAA es específica para la protección de datos de los registros médicos, lo que nos da el sustento de trabajo y un marco legal para su aplicación.

En la actualidad no se cuenta con normas específicas que permitan asegurar la información sensible de las casas de salud en el Ecuador, lo que provoca fallas de seguridad que pueden ocasionar por ejemplo fuga de información o exposición de datos sensibles sin el conocimiento ni consentimiento de sus propietarios.

[3] SNS: Sistema Nacional de Salud.

Metodológico

La metodología a utilizarse en esta investigación, consiste en tomar el Esquema Gubernamental de seguridad de la información en conjunto con las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información a las cuales hace mención y confrontarlas con las normas HIPAA que es específica para la protección de registros médicos, para establecer coincidencias, ventajas y desventajas de tal forma que se puedan adaptar en un framework permitiendo obtener mejores prácticas de manejo de los registros médicos de las personas, lo que permitirá reducir los riesgos en la seguridad de los sistemas de información.

Práctico

Las Unidades Médicas del Instituto Ecuatoriano de Seguridad Social poseen un sistema informático a nivel nacional donde se almacenan todos los registros médicos de los afiliados, al ser estos registros médicos digitales es conveniente implementar políticas de seguridad que permitan disminuir los riesgos de seguridad en los sistemas de información que contengan información que debe ser manejada con un carácter de confidencial con el fin de cumplir con ciertas normativas legales vigentes; en tal virtud se va a tomar como referencia al Hospital de Nivel I del IESS "Dr. Humberto del Pozo" ubicado en la ciudad de Guaranda, estableciendo políticas de seguridad que permitan reducir los valores de impacto producidos por los riesgos presentes en esa casa de salud mediante la aplicación del framework establecido en la investigación.

El EGSI planteado por la SANP[4] al igual que las HIPAA al ser estándares basados en normas internacionales pueden ser aplicadas en con ciertas adaptaciones en el país y más aún en el IESS donde ya se cuenta con un sistema informático para el manejo de los datos de las historias clínicas, lo que permitirá asegurar la integridad, confidencialidad y disponibilidad de estos.

1.6. Objetivos

1.6.1. Objetivo General

Generar una adaptación de las Normas ISO 27001 e HIPAA para reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS.

[4] SNAP: Secretaria Nacional de Administración Pública

1.6.2. Objetivos Específicos

- Analizar las normativas Ecuatorianas aplicadas en el sector de la salud para la seguridad de los sistemas de información
- Establecer ventajas y desventajas entre las Normas ISO 27001 e HIPAA para proponer una adaptación entre ellas, para asegurar los sistemas de información en Hospitales Nivel 1 del IESS.
- Implementar la adaptación de las normas ISO 27001 e HIPAA en el Hospital del IESS de Guaranda.
- Evaluar la implementación de la adaptación de las normas ISO 27001 e HIPAA en el Hospital del IESS de Guaranda.

1.7. Hipótesis

La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS.

CAPITULO II

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos.

Legislación vigente.

En el caso de Europa, la protección de los datos personales ha tenido una enorme importancia a lo largo de toda la constitución del espacio Europeo, dictándose en el año 1995 la directiva 95/46/CEE, relativa a la "protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" y que pasó a convertirse en un derecho fundamental de los europeos al reconocerse así en el artículo 8.1 de la Carta de Derechos Fundamentales de la Unión Europea, proclamada en Niza el 7 de diciembre de 2000, según la cual "Toda persona tiene Derecho a la protección de los datos de carácter personal que le conciernan". En el caso de UK la privacidad de los datos personales se mantiene sobre la "Data Proteccion Act –1998" (Sanchez et al., 2012, pp. 2–4).

Dentro del marco de la Unión Europea, España y Portugal marcan una excepción en materia de privacidad al tener influencia de dos zonas, por un lado la UE y por otro Latinoamérica:

- En el caso Español, la privacidad viene regulada por el Artículo 18.4 de Constitución Española (de 27 de diciembre de 1978) según el cual "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Además existe una fuerte legislación para proteger la privacidad de los ciudadanos, basada en la Ley Orgánica de Protección de Datos Personales (LOPD), que es una de las más restrictivas y exigentes del mundo y que se sustenta sobre la Ley Orgánica 15/1999 de 13 de Diciembre, el Real Decreto 1720/2007 de 21 de Diciembre y la Ley 2/2011 del 4 de Marzo. En materia de datos de salud: la ley 41/2002 de 14 de noviembre regula la autonomía del paciente y sus derechos y obligaciones en materia de información y documentación clínica. (Sanchez et al., 2012, pp. 2–4)
- Portugal: Existe una previsión constitucional específica sobre el derecho a la protección de datos desde 1976, en el artículo 35 de la Constitución de la República Portuguesa, que fue modificado en 1997 para adaptarlo a la Directiva 95/46/CE. La privacidad también se sustenta sobre la Ley de Protección de Datos Personales 67/98 de 26 de octubre que también se encuentra adaptada a la directiva Europea. (Sanchez et al., 2012, pp. 2–4)

En el caso de Latinoamérica, la privacidad de la información también ha sido una preocupación constante.

- En el caso de Argentina, la privacidad viene protegida mediante el Artículo 43 de la Constitución Nacional y la Ley nº 25.326, sancionada en el año 2000 y reglamentada en el año 2001. (Sanchez et al., 2012, pp. 2–4)
- En el caso de Brasil, la Constitución Federal prevé el acceso a datos (art. 5º, LXXII), la protección de la intimidad y la vida privada (art. 5º, X); la inviolabilidad de las comunicaciones donde se sitúan los datos (art. 5º XII) y por la Ley nº 9.507/97 que reglamenta el habeas data. (Sanchez et al., 2012, pp. 2–4)
- Perú: Es posiblemente el país de Latinoamérica que más esfuerzos ha realizado para regular y proteger los datos personales de sus ciudadanos. Estos están protegidos por el articulo 2 y 200 de la Constitución política de 1993, además de por un amplio conjunto de leyes específicas y de la existencia de un anteproyecto de ley para la "Protección de Datos Personales". Entre sus leyes podemos destacar Ley General de Salud, Ley 26842 del 20 de julio de 1997 que establece que “toda persona está obligada a proporcionar a la Autoridad de Salud la información que le sea exigible de acuerdo a Ley con las excepciones que establece la Ley; y toda persona usuaria de los servicios de salud, tiene derecho a exigir la reserva de la información relacionada con el acto médico y su historia clínica, con las excepciones de Ley. Art. XIV del Título Preliminar, Art. 5°, 15°”. (Sanchez et al., 2012, pp. 2–4)

En el caso de América del Norte, también ha sido una preocupación la privacidad, destacando especialmente la legislación de Estados Unidos en este campo.

- Estados Unidos Mexicanos: El artículo 16 de la Constitución de los Estados Unidos Mexicanos señala que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. La privacidad también se sustenta sobre la Ley Federal de Transparencia y Acceso a la Información Pública publicada el 11 de junio de 2002. Y en el caso sanitario, existe una ley específica, denominada "Ley de Salud Pública", que regula cómo y quiénes tienen acceso a los expedientes médicos de los ciudadanos. (Sanchez et al., 2012, pp. 2–4)
- Estados Unidos: Desde la década de los 90, y con los avances tecnológicos, el Congreso de Estados Unidos entendió la importancia de tener leyes que mantuvieran la privacidad en el tratamiento de la información personal de sus ciudadanos, por lo que comenzó a emitir leyes al respecto, principalmente con un carácter sectorial como la HIPAA, GLBA, SB 1386, COPPA y varias “State Breach laws”, lo que lo convirtió en uno de los países donde es más complejo cumplir los principios de privacidad. Dentro de este conjunto de normas, podemos destacar la HIPAA creada en 1996 para mantener la privacidad en el sector sanitario. La HIPAA es de obligado cumplimiento no solo para los hospitales, sino también para todos sus

proveedores. Hay dos cláusulas HIPAA que se relacionan específicamente con la privacidad y seguridad de su información médica (PHI - Protected Health Information):

- ✓ Regla de privacidad: Que permite que el personal médico use y revele la información médica protegida para su tratamiento, pago y operaciones de atención médica sin autorización escrita.
- ✓ Regla de seguridad: Especifica un conjunto de procesos empresariales y requisitos técnicos que los proveedores, planes médicos y oficinas de compensación deben seguir para garantizar la seguridad de la información médica privada. Está orientada en tres áreas: Salvaguardas administrativas, físicas y técnicas.

- Canadá: La legislación Canadiense en materia de privacidad es más parecida a la adoptada por la Unión Europea que por Estados Unidos, regulándose actualmente por la "Canada's Personal Information Protection and Electronic Documents Act" del año 2000. Existen trabajos muy destacados del marco de la privacidad en Canadá, destacando los escritos por Ann Cavoukian y, en especial, algunos para el sector sanitario donde se menciona la existencia de la PHIPA (Personal Health Information Protection Act) de 2004 Pero la privacidad de los datos en el sector Sanitario no sólo es una preocupación del ámbito Europeo y Americano." (Sanchez et al., 2012, pp. 2–4)

En el Ecuador: La privacidad se garantiza mediante El Art. 66 de la Constitución de la República, donde se dispone "…Se reconoce y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley", lo cual guarda concordancia con: Art. 92 CR; Arts. 49, 50, 51 LOGJCC; 202.2 CP ("LA PROTECCIÓN DE DATOS PERSONALES - Derecho Ecuador", s/f).

También tiene el Código Integral Penal promulgado en el Suplemento del Registro Oficial Nº 180 del 10 de febrero de 2014, en el cual mediante los artículos 186, 190, 191, 192, 195, 211, 229, 230, 231, 232, 233, 234 y el 476 ya se tipifican y establecen ciertas sanciones para los delitos que son considerados como informáticos (ASAMBLEA NACIONAL REPUBLICA DEL ECUADOR, 2014).

En cambio para proteger la confidencialidad de los datos de los pacientes se cuenta con la Ley de Derechos del Paciente, según su artículo 4 que menciona: "Derecho a la confidencialidad.- Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial." (CONGRESO NACIONAL, 1995)

Esquema Gubernamental de Seguridad de la Información.

Mediante Acuerdo Ministerial No. 166 se establece:

Art. 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013).

Art. 2.- Las entidades de la Administración Pública implementarán en un plazo de dieciocho (18) meses el Esquema Gubernamental de Seguridad de la Información (EGSI), que se adjunta a este acuerdo como Anexo 1, a excepción de las disposiciones o normas marcadas como prioritarias en dicho esquema, las cuales se implementarán en (6) meses desde la emisión del presente Acuerdo. La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013).

Art. 7.- Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013).

Herramienta de Seguridad para las reglas HIPAA.

El NIST[5] desarrollo una herramienta guía para la aplicación de las reglas de seguridad HIPAA, en el cual se establece que el "El Seguro de Salud de Portabilidad y Responsabilidad (HIPAA) para reglas de seguridad (45 CFR 160, 162, y 164) establece normas nacionales para proteger información personal electrónica de salud de los individuos que es creada, recibida utilizada o mantenida por una entidad cubierta. La regla de seguridad requiere medidas de seguridad administrativas, físicas y técnicas apropiadas para asegurar la confidencialidad, integridad y seguridad de la información de salud electrónica protegida." (National Institute of Standards and Technology (último), 2011).

El kit de herramientas de HSR[6] es una aplicación de escritorio que está destinado a ser un recurso útil entre un conjunto de herramientas y procesos que una organización puede utilizar para ayudar

[5] NIST: National Institute of Standards and Technology

[6] HSR: HIPAA Security Rule

en la revisión de la aplicación de la HSR. El contenido de seguridad que conforma el conjunto de preguntas proporcionará el apoyo que otras organizaciones pueden reutilizar una y otra vez.

El kit de herramientas de HSR aborda las especificaciones de implementación 45, identificados en la Regla de Seguridad HIPAA y cubre las prácticas básicas de seguridad, fallas de seguridad, gestión de riesgos, y las cuestiones de personal. Preguntas básicas de la práctica de seguridad incluyen la definición y gestión de accesos, copias de seguridad, recuperación y seguridad física.

Preguntas que abordan los fallos de seguridad se ocupan de artículos legales que atender después de un incidente, como notificaciones de violación. Preguntas de gestión de riesgos frente a revisiones periódicas y evaluaciones y pueden incluir funciones regulares, como la vigilancia continua. Por último, las preguntas de cuestión personal abordan el acceso a la información, así como la incorporación y la liberación del personal. (National Institute of Standards and Technology (último), 2011)

2.2. Marco Conceptual

Según la Resolución de la Comisión Interventora del Instituto Ecuatoriano de Seguridad Social en el año 2000 mediante Resolución CI. 056 se define como:

Hospital de Nivel 1. – Es la Unidad Médica de referencia cantonal, responsable de la prevención y atención de enfermedades mediante cirugía, clínica, cuidado materno infantil, urgencias, y auxiliares de diagnóstico. (Comisión interventora del Instituto Ecuatoriano de Seguridad Social, 2000, p. 2).

Posee un Órgano de Gestión dependiente de la Gerencia del Hospital, la Subgerencia Médica que comprende: el área de Especialidades Clínicas, el área de Especialidades de Cirugías, el área de Especialidades de Cuidado Materno – Infantil, el área de Especialidades de Medicina Crítica, el área de Especialidades de Auxiliares de Diagnóstico, el área de Odontología, el Centro de Rehabilitación, y el centro Quirúrgico y Obstétrico. (Comisión interventora del Instituto Ecuatoriano de Seguridad Social, 2000, p. 64)

El Hospital de Nivel I IESS Guaranda “Dr. Humberto del Pozo” se creó como dispensario tipo C de salud en 1939, posteriormente y mediante resolución CI 056 somos clasificados como centro de atención ambulatoria. Con fecha 07 de noviembre de 2005 el consejo directivo re categoriza el centro a “Hospital Nivel I” y partir de junio del 2007 entra en funcionamiento como hospital con los servicios de consulta externa con las especialidades de medicina interna, medicina familiar, ginecología y obstetricia, pediatría, cirugía general, gastroenterología, fisiatría,

psicología, nutrición, urología, traumatología, endocrinología, medicina interna, cardiología, medicina general y odontología; emergencia 24 horas, hospitalización, centro quirúrgico, centro obstétrico, y servicios complementarios de diagnóstico y tratamiento como cuidados de enfermería, radiología e imagen, laboratorio de análisis clínico, farmacia institucional y rehabilitación integral.

Según Acuerdo Ministerial 5212 del 30 de enero del 2015, el Ministerio de Salud Pública expide la "Tipologia sustitutiva para homologar los establecimientos de salud por niveles de atención y servicios de apoyo del sistema nacional de salud" donde se define como Hospital Básico a los establecimiento de salud que cuenta con los servicios de consulta externa, emergencia e internación y con las especialidades clínicas y/o quirúrgicas básicas de medicina interna, medicina familiar, ginecología y obstetricia, pediatría, cirugía general y odontología. Dispone de cuidados de enfermería y obstetricia, además de los siguientes servicios de apoyo diagnóstico y terapéutico: centro quirúrgico, centro obstétrico, radiología e imagen, laboratorio de análisis clínico, medicina transfusional, nutrición y dietética, farmacia institucional para el establecimiento público y farmacia interna para el establecimiento privado, con un stock de medicamentos autorizados por la Autoridad Sanitaria Nacional; puede contar con rehabilitación integral.

Desarrolla acciones de promoción, prevención, rehabilitación, cuidados paliativos y recuperación de la salud. Puede contar con el servicio de docencia e investigación. Constituye el escalón de referencia inmediata del Primer Nivel de Atención y direcciona la contrareferencia.(Ministerio de Salud Pública, 2015a, p. 5)

Según la Tipología del Ministerio de Salud Publica el Hospital de Nivel I del IESS Guaranda es Homologado como un Hospital Básico.

ISO - Seguridad de la Información.- Las normas ISO de Gestión de la Seguridad de la Información se denominan familia de normas ISO 27000 que se refieren a Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de la Seguridad de la Información (SGSI). Generalidades y vocabulario y son las siguientes:

- **ISO 27001:** Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

- **ISO 27002:** Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- **ISO 27003:** Sistema de Gestión de la Seguridad de la Información (SGSI). Guía de implantación.
- **ISO 27004:** Tecnología de la información. Técnicas de Seguridad. Gestión de la Seguridad de la Información. Métricas.
- **ISO 27005:** Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- **ISO 27006:** Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- **ISO 27007:** Tecnología de la información. Técnicas de Seguridad. Guía de auditoría de un SGSI.

Información. Es uno de los activos más importantes de la empresa contenido en papeles y en sistemas de información. La información que posee la organización debe mantenerse protegida rigurosamente por tal motivo se deben tomar las precauciones necesarias para mantenerla bajo cuidado y preservarla dentro de la entidad y se deben tener en cuenta tres conceptos importantes: Confidencialidad, integridad y disponibilidad. (Muñoz, 2003)

Activo.- Todo bien que tiene valor para la institución; documentos que contienen información de salud se entienden: historias clínicas, resultados de exámenes de laboratorio, imagenología y otros procedimientos, tarjetas de registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales. (Ministerio de Salud Pública, 2015b, p. 3)

Confidencialidad. Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información. (Ministerio de Salud Pública, 2015, p. 2)

Integridad de la información.- Es la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por tanto mantiene sus características y valores asignados o recogidos en la fuente. Esta cualidad debe mantenerse en cualquier formato de soporte en el que

se registre la información, independientemente de los procesos de migración entre ellos. (Ministerio de Salud Pública, 2015b, p. 2)

Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional. (Ministerio de Salud Pública, 2015b, p. 2)

Seguridad en el manejo de la información.- Es el conjunto sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su condición de confidencial, así como su integridad y disponibilidad. Inicia desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona. El deber de confidencialidad respecto a la información de los documentos que contienen información de salud perdurará, incluso, después de finalizada la actividad del establecimiento de salud, la vinculación profesional o el fallecimiento del titular de la información. (Ministerio de Salud Pública, 2015b, p. 2)

Secreto Médico.- Es la categoría que se asigna a toda información que es revelada por un/a usuario/a al profesional de la salud que le brinda la atención de salud. Se configura como un compromiso que adquiere el médico ante el/la usuario/a y la sociedad, de guardar silencio sobre toda información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional. Los profesionales de salud de los establecimientos de salud cumplirán con el deber del secreto médico, para generar condiciones de confianza en la relación con los/as usuarios/as y así garantizar el derecho a la intimidad. El secreto médico es extensible a toda la cadena sanitaria asistencial. (Ministerio de Salud Pública, 2015b, p. 3)

Amenaza.- Evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. (EAR/PILAR, 2011, p. 4).

Impacto.- Consecuencia que sobre un activo tiene la materialización de una amenaza. (EAR/PILAR, 2011, p. 8).

Información Digital. “Se trata de información que es almacenada electrónicamente desglosada en dígitos o unidades binarias de unos y ceros que se guardan y se recuperan mediante un conjunto de instrucciones llamados programas o código”. (NFSTC, 2012, p.3).

Seguridad. Según algunos autores la seguridad en un sistema de información es un estado que nos indica que ese sistema está libre de peligro, daño o riesgo, entendiendo como peligro todo aquello que puede afectar su funcionamiento directo o los resultados que se obtienen del mismo (Contreras, 2004, p. 1).

Seguridad informática, es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable. (López, 2010, p. 9)

2.3. ISO 27001.

ISO (la Organización Internacional para la Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización universal cuyos comités técnicos colaboran en campos de interés mutuo. Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). ("ISO 27001", 2013, p. 27001)

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de Insumos en outputs, se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el Insumo del siguiente proceso. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'. (ISO IEC, 2005)

Un enfoque del proceso para la gestión de la seguridad de la información fomenta que sus usuarios enfaticen la importancia de:

a) entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) monitorear y revisar el desempeño y la efectividad del SGSI; y
d) mejoramiento continuo en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La Ilustración 1 muestra cómo un SGSI toma como Insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. Este Estándar Internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad (ISO IEC, 2005).

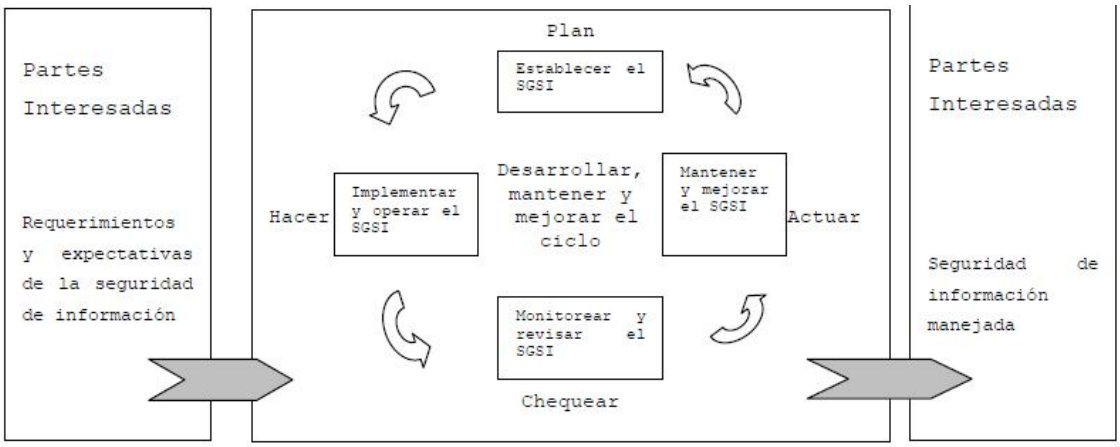

***Figura 1-2** Modelo PDCA aplicado a los procesos SGSI*

Fuente: ("ISO 27001", 2013)

- Planear (establecer el SGSI).- Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización. (ISO IEC, 2005)
- Hacer (implementar y operar el SGSI).- Implementar y operar la política, controles, procesos y procedimientos SGSI. (ISO IEC, 2005)
- Chequear (monitorear y revisar el SGSI).- Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión. (ISO IEC, 2005, p. 7)
- Actuar (mantener y mejorar el SGSI).- Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI. (ISO IEC, 2005, p. 7)

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

Figura 2-1 *Modelo de un SGSI*

Fuente: ("ISO 27001", 2013)

2.3.1. Gestión de la Seguridad.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

Figura 3-2. *Modelo de gestión de seguridad*

Fuente: ("ISO 27001", 2013)

Los beneficios de implantación de un SGSI está reflejado en la obtención y mantenimiento de una estructura e inversiones adecuadas al costo correcto, con la clasificación y control adecuado de los activos de la información, se define la Política de Seguridad que rige a la organización, se identifican y evalúan los riesgos internos y a terceros, se definen y ejecutan los Planes de Contingencia con el afán de mitigar los riesgos, con el objetivo de dar cumplimiento con la legislación vigente.

La metodología de un SGSI según ISO 27001 gráficamente puede estar resumido de la siguiente manera:

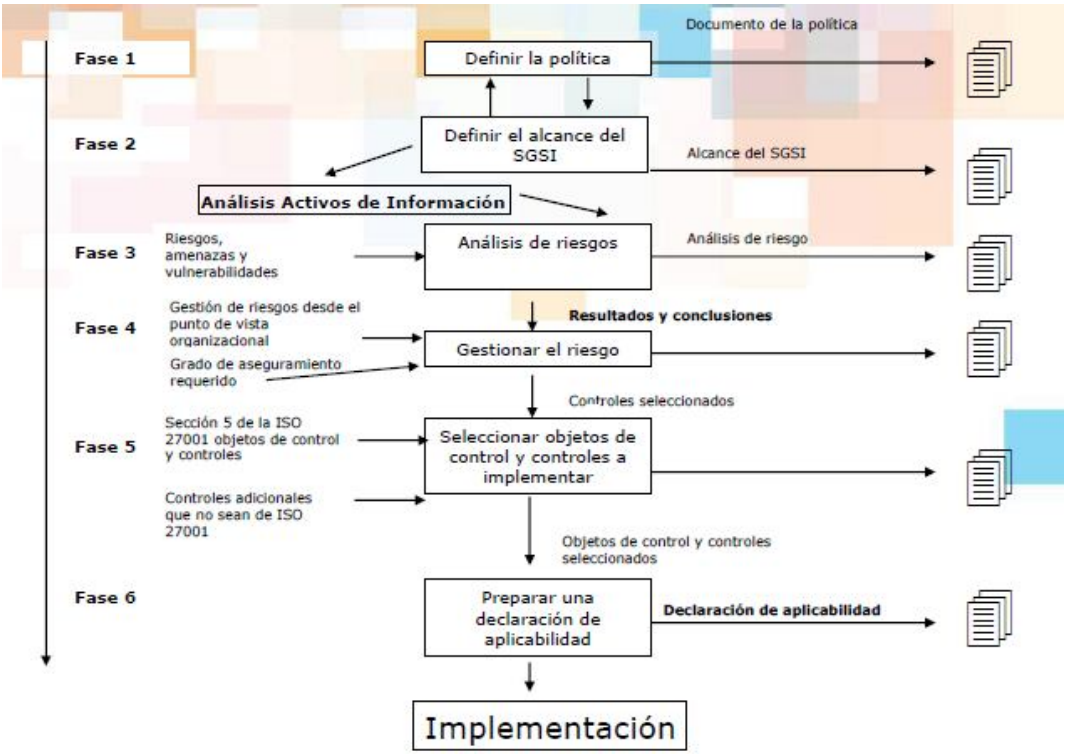

***Figura 4-2** Metodología de un SGSI según ISO 27001*

2.3.2. Cláusulas del Estándar Internacional ISO/IEC 27001.

1. Alcance

En esta cláusula se habla sobre el alcance General y la aplicación del Estándar, que abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) (ISO IEC, 2005, p. 8). Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado. El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

Las aplicaciones de los requerimientos establecidos son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar. (ISO IEC, 2005)

2. Referencias normativas

Habla sobre los documentos mencionados como indispensables para la aplicación de del Estándar.

3. Términos y definiciones

1. **Activo** cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004)
2. **Disponibilidad** la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 13335-1:2004)
3. **Confidencialidad** la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados (ISO/IEC 13335-1:2004)
4. **Seguridad de información** preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad (ISO/IEC 17799:2005)
5. **Evento de seguridad de la información** una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/IEC TR 18044:2004)
6. **Incidente de seguridad de la información** un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información (ISO/IEC TR 18044:2004)
7. **Sistema de gestión de seguridad de la información SGSI** esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información
8. **Integridad la propiedad** de salvaguardar la exactitud e integridad de los activos (ISO/IEC 13335-1:2004)
9. **Riesgo residual** el riesgo remanente después del tratamiento del riesgo (ISO/IEC Guía 73:2002)
10. **Aceptación de riesgo** decisión de aceptar el riesgo (ISO/IEC Guía 73:2002)
11. **Análisis de riesgo** uso sistemático de la información para identificar fuent0es y para estimar el riesgo (ISO/IEC Guía 73:2002)

12. **Valuación del riesgo** proceso general de análisis del riesgo y evaluación del riesgo (ISO/IEC Guía 73:2002)
13. **Evaluación del riesgo** proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo (ISO/IEC Guía 73:2002)
14. **Gestión del riesgo** actividades coordinadas para dirigir y controlar una organización con relación al riesgo (ISO/IEC Guía 73:2002)
15. **Tratamiento del riesgo** proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo (ISO/IEC Guía 73:2002)
16. **Enunciado de aplicabilidad** enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

4. Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan. Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA. (ISO IEC, 2005)

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI:

Definir el alcance, los límites y una política del SGSI en términos de las características del negocio, con un enfoque de valuación del riesgo de la organización, identificando, analizando y evaluando los riesgos; así como identificar y evaluar las opciones para el tratamiento de los riesgos, seleccionando objetivos de control y controles para su tratamiento, además de obtener la aprobación de la gerencia para los riesgos residuales propuestos y su autorización para implementar y operar el SGSI, preparando un Enunciado de Aplicabilidad. (ISO IEC, 2005)

4.2.2 Implementar y operar el SGSI

Formular e implementar un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información, para poder lograr los objetivos de control, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades. Se debe también definir cómo medir

la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control; se debe también implementar los programas de capacitación y conocimiento. (ISO IEC, 2005)

4.2.3 Monitorear y revisar el SGSI

Se debe ejecutar procedimientos de monitoreo y revisión, para detectar errores en los resultados de procesamiento, e identificar incidentes y violaciones de seguridad fallidos y exitosos, para así permitir a la gerencia determinar si las actividades de seguridad se están realizando o son efectivas las acciones tomadas para resolver una violación de seguridad. (ISO IEC, 2005)

Realizar revisiones regulares de la efectividad del SGSI tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas, midiendo la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad. Revisar las evaluaciones del riesgo, el nivel de riesgo residual y riesgo aceptable identificado; realizar auditorías SGSI internas a intervalos planeados así como realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI. (ISO IEC, 2005)

Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión, registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI. (ISO IEC, 2005)

4.2.4 Mantener y mejorar el SGSI

Se debe implementar las mejoras identificadas en el SGSI, para tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3, comunicando los resultados y acciones a todas las partes interesadas para asegurar que las mejoras logren sus objetivos. (ISO IEC, 2005)

4.3. Requerimientos de documentación

4.3.1 General

La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas

gerenciales, y los resultados registrados deben ser reproducibles. La documentación SGSI debe incluir los enunciados documentados de la política y los objetivos, el alcance, procedimientos y controles de soporte del SGSI, una descripción de la metodología de evaluación del riesgo, reporte de evaluación del riesgo, plan de tratamiento del riesgo, los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles, registros requeridos y el enunciado de Aplicabilidad. (ISO IEC, 2005)

4.3.2 Control de documentos

Los documentos deben ser protegidos y controlados, estableciendo un procedimiento documentado para definir las acciones gerenciales necesarias para aprobar, revisar y actualizar los documentos, asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos, asegurar que las versiones más recientes de los documentos relevantes estén disponibles, asegurar que los documentos se mantengan legibles y fácilmente identificables, asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación, asegurar que se identifiquen los documentos de origen externo, que se controle la distribución de documentos, evitando el uso indebido de documentos obsoletos; y aplicarles una identificación adecuada si se van a retener por algún propósito. (ISO IEC, 2005)

4.3.3 Control de registros

Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros. (ISO IEC, 2005)

5. Responsabilidad de la gerencia

5.1. Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del

SGSI al establecer una política SGSI, asegurando que se establezcan objetivos, planes, roles y responsabilidades para la seguridad de información; asegurar que se realicen las auditorías internas y realizar revisiones gerenciales del SGSI. (ISO IEC, 2005)

5.2. Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI; asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales y de donde se requiera, mejorar la efectividad del SGSI. (ISO IEC, 2005)

5.2.2 Capacitación, conocimiento y capacidad

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas. La organización también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI. (ISO IEC, 2005)

6. Auditorías internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI cumplen con los requerimientos del Estándar y la legislación y regulaciones relevantes. Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo. (ISO IEC, 2005)

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros se deben definir en un procedimiento documentado. La gerencia responsable para el área siendo auditada debe

asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. (ISO IEC, 2005)

7. Revisión Gerencial del SGSI

7.1. General

La gerencia debe revisar el SGSI de la organización a intervalos planeados para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. (ISO IEC, 2005)

7.2. Insumo de la revisión

El insumo para la revisión gerencial debe incluir los resultados de auditorías y revisiones del SGSI, retroalimentación de las partes interesadas, técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI, status de acciones preventivas y correctivas, vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa, resultados de mediciones de efectividad, acciones de seguimiento de las revisiones gerenciales previas, cualquier cambio que pudiera afectar el SGSI; y recomendaciones para el mejoramiento. (ISO IEC, 2005)

7.3. Resultado de la revisión

El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con el mejoramiento de la efectividad del SGSI, actualización de la evaluación del riesgo y el plan de tratamiento del riesgo, modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI. (ISO IEC, 2005)

8. Mejoramiento del SGSI

8.1. Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial. (ISO IEC, 2005)

8.2. Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para identificar, determinar las causas y evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir; determinar e implementar la acción correctiva necesaria, registrar los resultados de la acción tomada y revisar la acción correctiva tomada. (ISO IEC, 2005)

8.3. Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para identificar las no-conformidades potenciales y sus causas; evaluar, determinar e implementar la acción preventiva necesaria; registrar y revisar la acción preventiva tomada. (ISO IEC, 2005)

2.4. HIPAA.

HIPAA es una ley federal que fue aprobada el 16 de agosto de 1996 por el Congreso de los Estados Unidos; la Regla de Seguridad de HIPAA se enfoca específicamente en la salvaguardia de la información electrónica protegida sobre la salud (EPHI). Todas las entidades cubiertas por HIPAA deben cumplir con la Regla de Seguridad, que se enfoca específicamente en proteger la confidencialidad, integridad y disponibilidad de EPHI, como se define en la Regla de Seguridad. El EPHI que una entidad cubierta crea, recibe, mantiene o transmite debe estar protegido contra amenazas, riesgos y usos y / o revelaciones no permitidos razonablemente previstos. En general, los requisitos, normas y especificaciones de implementación de la Regla de Seguridad se aplican a las siguientes entidades cubiertas:

- **Proveedores de atención médica cubiertos**: Cualquier proveedor de servicios médicos o de otro tipo, o suministros, que transmita cualquier información de salud en forma electrónica en relación con una transacción para la cual el Departamento de Salud y Servicios Humanos (DHHS) ha adoptado una norma.
- **Planes de salud**: cualquier plan individual o grupal que provea o paga el costo de atención médica, incluyendo ciertos programas gubernamentales específicamente

listados (por ejemplo, un emisor de seguro de salud y los programas de Medicare y Medicaid).

- **Centros de Atención de Salud**: Una entidad pública o privada que procesa las transacciones de atención médica de otra entidad desde un formato estándar a un formato no estándar, o viceversa.
- **Patrocinadores de la Tarjeta de Medicamentos Recetados de Medicare**: Una entidad no gubernamental que ofreció un programa de medicamentos con descuento aprobado bajo la Ley de Modernización de Medicare. Esta cuarta categoría de "entidad cubierta" permaneció en vigor hasta que el programa de tarjetas de medicamentos terminó en 2006.

Las normas y pautas de seguridad del NIST (Federal Information Processing Standards), que pueden utilizarse para respaldar los requisitos de HIPAA, pueden ser utilizadas por las organizaciones para ayudar a proporcionar un marco estructurado pero flexible Para seleccionar, especificar, emplear y evaluar los controles de seguridad en los sistemas de información. (National Institute of Standards and Technology, 2008, p. 7)

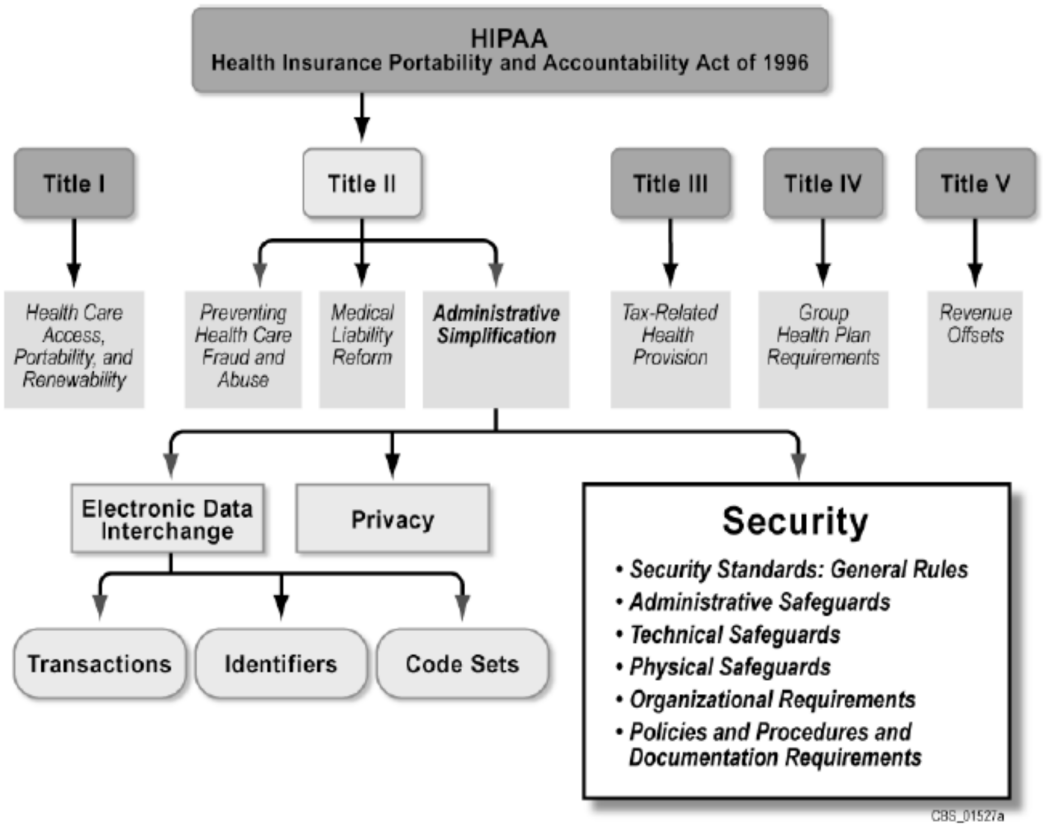

Ilustración 1-2 *Componentes HIPAA*

Fuente: (National Institute of Standards and Technology, 2008, fig. 1)

HIPAA se divide en cinco títulos o secciones. Cada título trata un aspecto único de la reforma del seguro de salud.

Titulo 1: Portabilidad (movilidad):

La movilidad permite a las personas llevar su seguro médico de un trabajo a otro para que no tengan un lapso en la cobertura. También restringe a los planes médicos de requerir condiciones preexistentes a personas que cambian un plan médico a otro.

Título II. Simplificación Administrativa.

Tiene un impacto mayor para los proveedores. Se diseñó para:

- Combatir el fraude y abuso en el cuidado de la salud
- Garantizar la seguridad y la privacidad de la información médica.
- Establecer estándares para la información y transacciones médicas
- Reducir el costo del cuidado médico mediante la estandarización de la manera en que la industria comunica la información.

Título III. Ahorros Médicos y Deducciones Contributivas:

Trabaja con las disposiciones de Salud relacionadas a los impuestos. Estas son disposiciones fiscales relacionadas con la salud; establece ciertas deducciones para el seguro médico, y realiza otros cambios a la ley de seguro de salud.

Título IV. Provisiones de Grupos de Salud:

Aplicación y cumplimiento de los requisitos de planes grupales de salud que permiten a individuos llevar su cobertura médica anterior a su empleo actual. Especifica las condiciones para los planes de salud de grupo relacionadas con la cobertura de las personas con condiciones pre-existentes y modifica los requisitos de continuación de cobertura.

Título V. Compensación de los ingresos:

Incluye regulaciones sobre cómo los empleadores pueden deducir las primas de los seguros de vida de la compañía para fines de tributación sobre los ingresos.

- Retención de ingresos.
- Depende de la PHI (información protegida de salud).

PROPÓSITO PRINCIPAL DE LA LEY HIPAA

Como se requiere en la sección "Normas de seguridad: Reglas generales" de la Regla de Seguridad de HIPAA, cada entidad cubierta debe:

- Garantizar la confidencialidad, integridad y disponibilidad de EPHI que crea, recibe, mantiene o transmite;
- Proteger contra cualquier amenaza y peligro razonablemente anticipado a la seguridad o integridad de EPHI; y
- Protegerse contra usos o divulgaciones razonablemente anticipados de tal información que no están permitidos por la Regla de Privacidad.

Al cumplir con esta sección de la Regla de Seguridad, las entidades cubiertas deben estar al tanto de las definiciones proporcionadas para la confidencialidad, integridad y disponibilidad según lo dispuesto en § 164.304 (National Institute of Standards and Technology, 2008):

- La confidencialidad es "la propiedad de que los datos o la información no se ponen a disposición ni se revelan a personas o procesos no autorizados".
- La integridad es "la propiedad de que los datos o la información no han sido alterados o destruidos de manera no autorizada".
- La disponibilidad es "la propiedad de que los datos o la información sean accesibles y utilizables a petición de una persona autorizada".

2.4.1. Organización de Reglas de Seguridad

La Regla de Seguridad se divide en seis secciones principales que incluyen varias normas y especificaciones de implementación que una entidad cubierta debe tratar. Las seis secciones se enumeran a continuación (National Institute of Standards and Technology, 2008):

- **Normas de seguridad: Reglas Generales** - incluye los requisitos generales que todas las entidades cubiertas deben cumplir; Establece flexibilidad de enfoque; Identifica las normas y especificaciones de implementación (tanto obligatorias como direccionables); Describe las decisiones que una entidad cubierta debe hacer con respecto a las especificaciones de implementación direccionables; Y requiere el mantenimiento de las medidas de seguridad para continuar la protección razonable y adecuada de la información electrónica de salud protegida.
- **Salvaguardias Administrativas** - se definen en la Regla de Seguridad como las "acciones y políticas administrativas y procedimientos para gestionar la selección, desarrollo, implementación y mantenimiento de medidas de seguridad para proteger la información electrónica protegida sobre la salud y para manejar la conducta de la Relación con la protección de esa información".

- **Salvaguardias físicas** - se definen como "medidas físicas, políticas y procedimientos para proteger los sistemas de información electrónicos de una entidad cubierta y los edificios y equipos relacionados, de los peligros naturales y ambientales y la intrusión no autorizada".
- **Salvaguardias técnicas:** se definen como "la tecnología y la política y procedimientos para su uso que protegen la información de salud protegida electrónica y controlan el acceso a ella".
- **Requisitos de organización**: incluye estándares para contratos de asociado de negocios y otros arreglos, incluyendo memorandos de entendimiento entre una entidad cubierta y un asociado de negocios cuando ambas entidades son organizaciones gubernamentales; Y los requisitos para los planes de salud grupales.
- **Requisitos de Políticas y Procedimientos y Documentación:** requiere la implementación de políticas y procedimientos razonables y apropiados para cumplir con las normas, especificaciones de implementación y otros requisitos de la Regla de Seguridad; Mantenimiento de documentación escrita (que puede ser electrónica) y / o registros que incluye políticas, procedimientos, acciones, actividades o evaluaciones requeridas por la Regla de Seguridad; Y los requisitos de retención, disponibilidad y actualización relacionados con la documentación.

2.4.2. Marco para la Gestión del Riesgo

La Regla de Seguridad de HIPAA tiene que ver con la implementación de una gestión de riesgos efectiva para proteger de manera adecuada y efectiva la EPHI. La evaluación, el análisis y la gestión del riesgo constituyen la base de los esfuerzos de cumplimiento de la Regla de Seguridad de una entidad cubierta, sirviendo como herramientas para desarrollar y mantener la estrategia de una entidad cubierta para proteger la confidencialidad, integridad y disponibilidad de EPHI.

Las entidades cubiertas están obligadas a implementar medidas de seguridad, razonables y apropiadas para protegerse contra amenazas o vulnerabilidades razonablemente anticipadas a la seguridad de EPHI. Bajo la Regla de Seguridad, las entidades cubiertas deben evaluar los riesgos y vulnerabilidades en sus entornos e implementar controles de seguridad para enfrentar esos riesgos y vulnerabilidades.

La selección y especificación de los controles de seguridad pueden lograrse como parte de un programa de seguridad de la información que involucra la gestión del riesgo organizacional, es

decir, el riesgo para la información, los individuos y la organización en su conjunto. La gestión del riesgo es un elemento clave en el programa de seguridad de la información de la organización y proporciona un marco eficaz para seleccionar los controles de seguridad adecuados para un sistema de información: los controles de seguridad necesarios para proteger a las personas y las operaciones y activos de la organización. (National Institute of Standards and Technology, 2008)

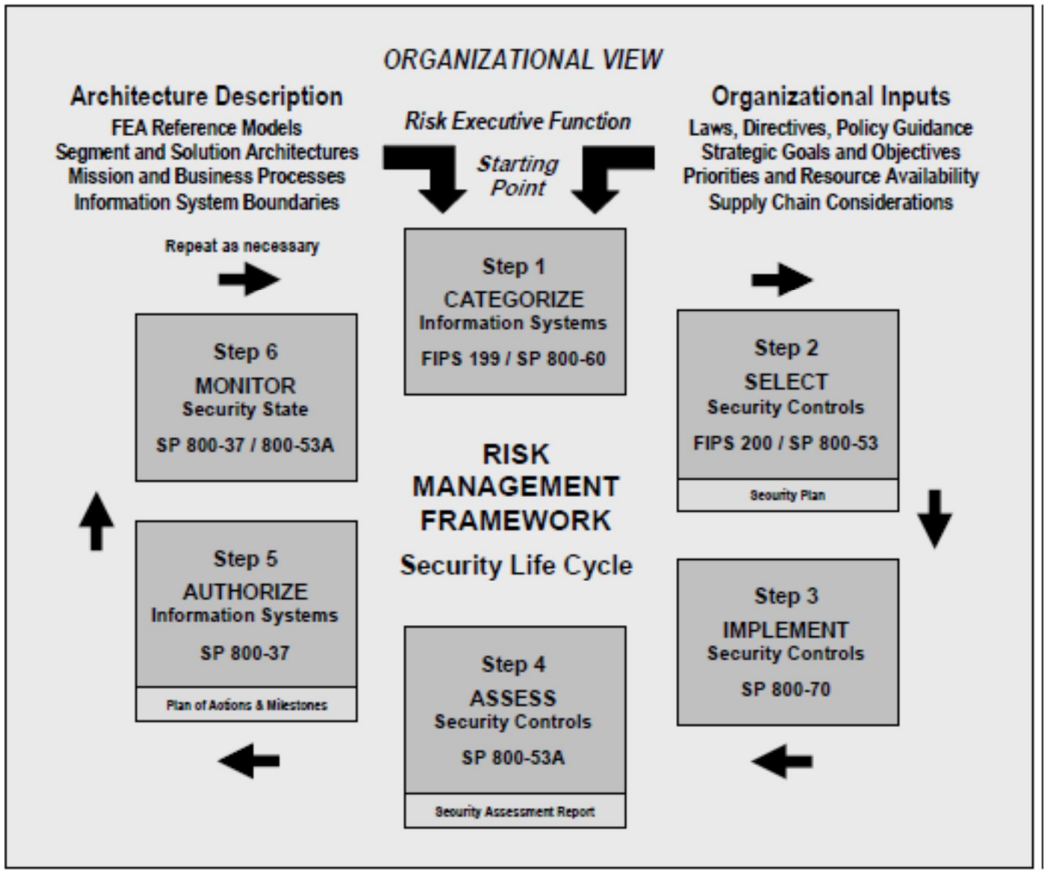

Ilustración 2-1 *Marco de gestión del riesgo del NIST*

Fuente: (National Institute of Standards and Technology, 2008, fig. 2)

2.4.3. Consideraciones de la ley HIPAA

Las consideraciones de la Ley es mantener la seguridad y privacidad en el manejo: garantiza los derechos a la privacidad del paciente al entregar explicaciones claras por escrito de cómo el proveedor podría utilizar y revelar su información de salud. Asegurar que los pacientes puedan ver y obtener copias de sus expedientes y poder solicitar correcciones.

Obtengan el consentimiento del paciente antes de compartir su información para tratamiento, pago y actividades del cuidado médico. Obtengan la autorización del paciente para las

revelaciones no rutinarias y la mayoría de los propósitos no relacionados al cuidado médico. Permitan a los pacientes solicitar restricciones en los usos y revelaciones de su información.

Además, adopten procedimientos de privacidad por escrito que incluyan: quién tiene el acceso a la información protegida, cómo se utiliza dentro de la agencia, cuándo la información se revelará. Aseguren que los empleados del centro de servicios médicos protejan la privacidad de la información de salud. Enseñen a los empleados los procedimientos de privacidad del proveedor. Designen un oficial de privacidad que es responsable de asegurarse que los procedimientos de seguridad se cumplen.

2.4.4. Catálogo de Normas HIPAA y especificaciones de Implementación

Catálogo normas HIPAA y especificaciones de implementación

Tabla 1-2 *Catálogo de normas HIPAA y especificaciones de implementación*

Sección de Regla de Seguridad HIPAA	Normas Regla de Seguridad HIPAA	Implementación Especificaciones
	Salvaguardias administrativas	
164.308(a)(1)(i)	Proceso de gestión de seguridad: Implementar políticas y procedimientos para prevenir, detectar, contener y corregir infracciones de seguridad.	
164.308(a)(1)(ii)(A)		Análisis de Riesgo (R): Realizar una evaluación precisa y completa de los riesgos y vulnerabilidades potenciales a la confidencialidad, integridad y disponibilidad de información de salud protegida electrónica en poder de la entidad cubierta.
164.308(a)(1)(ii)(B)		Gestión de riesgos (R): Implementar medidas de seguridad suficientes para reducir riesgos y vulnerabilidades a un nivel razonable y apropiado para cumplir con la Sección 164.306 (a).
164.308(a)(1)(ii)(C)		Política de Sanciones (R): Aplicar sanciones apropiadas contra los miembros de la fuerza de trabajo que no cumplan con las políticas y procedimientos de seguridad de la entidad cubierta.
164.308(a)(1)(ii)(D)		Revisión de la Actividad del Sistema de Información (R): Implementar procedimientos para revisar periódicamente los registros de la actividad del sistema de información, tales como registros de auditoría, informes de acceso e informes de seguimiento de incidentes de seguridad.
164.308(a)(2)	Responsabilidad de seguridad asignada: Identificar al funcionario de seguridad que es responsable del desarrollo e implementación de las políticas y procedimientos requeridos por esta subparte para la entidad.	
164.308(a)(3)(i)	Seguridad de la fuerza de trabajo: Implementar políticas y procedimientos para asegurar que todos los miembros de su fuerza de trabajo tengan acceso	

	adecuado a información de salud protegida electrónica, como se dispone en el párrafo (a) (4) de esta sección, y para evitar que los miembros de la fuerza de trabajo que no tienen acceso bajo Párrafo (a) (4) de esta sección de obtener acceso a información electrónica protegida de salud.	
164.308(a)(3)(ii)(A)		Autorización y / o Supervisión (A): Implementar procedimientos para la autorización y / o supervisión de los miembros de la fuerza de trabajo que trabajan con información de salud protegida electrónica o en lugares a los que se pueda acceder.
164.308(a)(3)(ii)(B)		Procedimiento de autorización de personal (A): Implementar procedimientos para determinar que el acceso de un miembro de la fuerza de trabajo a la información de salud protegida electrónica es apropiado.
164.308(a)(3)(ii)(C)		Procedimiento de Terminación (A): Implementar procedimientos para terminar el acceso a la información de salud protegida electrónica cuando termine el empleo de un miembro de la fuerza de trabajo o como lo requieran las determinaciones hechas como se especifica en el párrafo (a) (3) (ii) (B) de esta sección.
164.308(a)(4)(i)	Gestión del acceso a la información: Implementar políticas y procedimientos para autorizar el acceso a información de salud protegida electrónica que sea consistente con los requisitos aplicables de la subparte E de esta parte.	
164.308(a)(4)(ii)(A)		Aislar las funciones de la cámara de compensación de la salud (R): Si una cámara de compensación médica es parte de una organización más grande, la cámara de compensación debe implementar políticas y procedimientos que protejan la información de salud protegida electrónica de la cámara de compensación del acceso no autorizado por la organización más grande.
164.308(a)(4)(ii)(B)		Autorización de acceso (A): Implementar políticas y procedimientos para otorgar acceso a información de salud protegida electrónica, por ejemplo, a través del acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.
64.308(a)(4)(ii)(C)		Establecimiento y Modificación de Acceso (A): Implementar políticas y procedimientos que, basados en las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso de un usuario a una estación de trabajo, transacción, programa o proceso.
164.308(a)(5)(i)	Concienciación y capacitación en materia de seguridad: Implementar un programa de sensibilización y capacitación para todos los miembros de su fuerza de trabajo (incluida la administración).	
164.308(a)(5)(ii)(A)		Recordatorios de seguridad (A): actualizaciones periódicas de seguridad.
164.308(a)(5)(ii)(B)		Protección contra software malintencionado (A): Procedimientos para proteger, detectar y reportar software malicioso.

164.308(a)(5)(ii)(C)		Monitorización de inicio de sesión (A): Procedimientos para supervisar los intentos de inicio de sesión y notificar discrepancias.
164.308(a)(5)(ii)(D)		Administración de contraseñas (A): Procedimientos para crear, cambiar y proteger contraseñas.
164.308(a)(6)(i)	Procedimientos de incidentes de seguridad: Implementar políticas y procedimientos para abordar incidentes de seguridad.	
164.308(a)(6)(ii)		Respuesta e Informes (R): Identificar y responder a incidentes de seguridad sospechosos o conocidos; Mitigar, en la medida de lo posible, los efectos nocivos de los incidentes de seguridad conocidos por la entidad cubierta; Y documentar los incidentes de seguridad y sus resultados.
164.308(a)(7)(i)	Plan de Contingencia: Establecer (e implementar según sea necesario) las políticas y procedimientos para responder a una emergencia u otra ocurrencia (por ejemplo, incendio, vandalismo, falla del sistema y desastre natural) que daña sistemas que contienen información de salud protegida electrónicamente.	
164.308(a)(7)(ii)(A)		Plan de respaldo de datos (R): Establecer e implementar procedimientos para crear y mantener copias exactas recuperables de información de salud protegida electrónica.
164.308(a)(7)(ii)(B)		Plan de Recuperación de Desastres (R): Establezca (e implemente según sea necesario) los procedimientos para restaurar cualquier pérdida de datos.
164.308(a)(7)(ii)(C)		Plan de Operación en Modo de Emergencia (R): Establezca (e implemente según sea necesario) procedimientos para permitir la continuación de procesos críticos de negocio para la protección de la seguridad de información de salud protegida electrónica mientras opera en modo de emergencia.
164.308(a)(7)(ii)(D)		Procedimiento de prueba y revisión (A): Implementar procedimientos para pruebas periódicas y revisión de planes de contingencia.
164.308(a)(7)(ii)(E)		Aplicaciones y análisis de criticidad de datos (A): Evaluar la criticidad relativa de aplicaciones y datos específicos en apoyo de otros componentes del plan de contingencia.
164.308(a)(8)	Evaluación: Realizar una evaluación técnica y no técnica periódica, basada inicialmente en los estándares implementados bajo esta regla y posteriormente en respuesta a cambios ambientales o operacionales que afectan la seguridad de la información electrónica protegida de salud que establece en qué medida las políticas y procedimientos de seguridad de una entidad Los requisitos de esta subparte.	
164.308(b)(1)	Contratos de Negocios y Otros Arreglos: Una entidad cubierta, de acuerdo con § 164.306, puede permitir que un asociado de negocios cree, reciba, mantenga o transmita información de salud protegida electrónica en nombre de la entidad cubierta si la entidad cubierta	

	obtiene garantías satisfactorias, Conformidad con Sec. 164.314 (a), que el asociado de negocios protegerá adecuadamente la información.	
164.308(b)(4)		(R): Documentar las garantías satisfactorias requeridas en el párrafo (b) (1) de esta sección a través de un contrato escrito u otro acuerdo con el socio comercial que cumpla con los requisitos aplicables de la sección 164.314 (a).
	Salvaguardas físicas	
164.310(a)(1)	Controles de acceso a instalaciones: Implementar políticas y procedimientos para limitar el acceso físico a sus sistemas electrónicos de información y las instalaciones o instalaciones en las que están alojados, asegurando al mismo tiempo el acceso debidamente autorizado.	
164.310(a)(2)(i)		Operaciones de contingencia (A): Establecer (e implementar según sea necesario) procedimientos que permitan el acceso a las instalaciones en apoyo de la restauración de datos perdidos bajo el plan de recuperación ante desastres y el plan de operaciones en caso de emergencia en caso de emergencia.
164.310(a)(2)(ii)		Plan de Seguridad de la Instalación (A): Implementar políticas y procedimientos para salvaguardar la instalación y el equipo en la misma desde el acceso físico no autorizado, manipulación y robo.
164.310(a)(2)(iii)		Procedimientos de control de acceso y validación (A): Implementar procedimientos para controlar y validar el acceso de una persona a las instalaciones basadas en su rol o función, incluyendo el control de visitantes y el control del acceso a los programas de software para pruebas y revisión.
164.310(a)(2)(iv)		Registros de mantenimiento (A): Implementar políticas y procedimientos para documentar las reparaciones y modificaciones de los componentes físicos de una instalación, relacionadas con la seguridad (por ejemplo, hardware, paredes, puertas y cerraduras).
164.310(b)	Uso de la estación de trabajo: Implementar políticas y procedimientos que especifiquen las funciones apropiadas a realizar, la forma en que se van a realizar esas funciones y los atributos físicos del entorno de una estación de trabajo o clase de estación de trabajo específica que pueda acceder a información de salud protegida electrónica.	
164.310(c)	Seguridad de la estación de trabajo: Implementar salvaguardas físicas para todas las estaciones de trabajo que tengan acceso a información de salud protegida electrónica para restringir el acceso a usuarios autorizados.	
164.310(d)(1)	Controles de Dispositivos y Medios: Implementar políticas y procedimientos que rigen la recepción y remoción de hardware y medios electrónicos que contienen información de salud protegida electrónica dentro y fuera de una instalación y el movimiento de estos artículos dentro de la instalación.	

164.310(d)(2)(i)		Eliminación (R): Implementar políticas y procedimientos para abordar la disposición final de información de salud protegida electrónica y / o el hardware o medio electrónico en el que se almacena.
164.310(d)(2)(ii)		Reutilización de los medios de comunicación (R): Implementar procedimientos para eliminar la información de salud protegida electrónicamente de los medios electrónicos antes de que los medios estén disponibles para su reutilización.
164.310(d)(2)(iii)		Responsabilidad (A): Mantener un registro de los movimientos de hardware y medios electrónicos y cualquier persona responsable por lo tanto.
164.310(d)(2)(iv)		Copia de seguridad y almacenamiento de datos (A): Cree una copia exacta recuperable de información de salud protegida electrónica, cuando sea necesario, antes del movimiento del equipo.
Salvaguardias técnicas		
164.312(a)(1)	Control de acceso: Implementar políticas y procedimientos técnicos para sistemas electrónicos de información que mantienen información de salud protegida electrónica para permitir el acceso sólo a aquellas personas o programas de software a los que se les han otorgado derechos de acceso como se especifica en § 164.308 (a) (4).	
164.312(a)(2)(i)		Identificación Única del Usuario (R): Asigne un nombre y / o número único para identificar y rastrear la identidad del usuario.
164.312(a)(2)(ii)		Procedimiento de Acceso de Emergencia (R): Establecer (e implementar según sea necesario) los procedimientos para obtener la información médica protegida electrónica necesaria durante una emergencia.
164.312(a)(2)(iii)		Desconexión automática (A): Implementar procedimientos electrónicos que terminen una sesión electrónica después de un tiempo predeterminado de inactividad
164.312(a)(2)(iv)		Cifrado y descifrado (A): Implementar un mecanismo para cifrar y descifrar información de salud protegida electrónica.
164.312(b)	Controles de auditoría: Implementar hardware, software y / o mecanismos de procedimiento que registran y examinan la actividad en sistemas de información que contienen o usan información de salud protegida electrónica.	
164.312(c)(1)	Integridad: Implementar políticas y procedimientos para proteger la información de salud protegida electrónica contra alteraciones o destrucción inadecuadas.	
164.312(c)(2)		Mecanismo para Autenticar la Información de Salud Protegida Electrónica (A): Implementar mecanismos electrónicos para corroborar que la información de salud protegida electrónica no ha sido alterada o destruida de manera no autorizada.
164.312(d)	Autenticación de persona o entidad: Implementar procedimientos para verificar que una persona o entidad que	

	busque acceso a información de salud protegida electrónica sea la reclamada.	
164.312(e)(1)	Seguridad de Transmisión: Implementar medidas de seguridad técnicas para prevenir el acceso no autorizado a información de salud protegida electrónica que se está transmitiendo a través de una red de comunicaciones electrónicas.	
164.312(e)(2)(i)		Controles de Integridad (A): Implementar medidas de seguridad para asegurar que la información electrónica protegida electrónicamente de salud protegida no se modifique indebidamente sin detección hasta que se elimine.
164.312(e)(2)(ii)		Cifrado (A): Implementar un mecanismo para cifrar la información de salud protegida electrónica cuando se considere apropiado.
	Organizativo	
164.314(a)(1)	Contratos de Negocios Asociados u Otros Acuerdos: (i) El contrato u otro acuerdo entre la entidad cubierta y su socio comercial requerido por la Sección 164.308 (b) debe cumplir con los requisitos del párrafo (a) (2) (i) o (a) 2) (ii) de esta sección, según corresponda. (Ii) Una entidad cubierta no cumple con las normas establecidas en la sección 164.502 (e) y el párrafo (a) de esta sección si la entidad cubierta conocía un patrón de una actividad o práctica de la empresa asociada que constituyó una violación material o Violación de la obligación del asociado de negocios bajo el contrato u otro acuerdo, a menos que la entidad cubierta tomó medidas razonables para curar el incumplimiento o poner fin a la violación, según corresponda, y, si tales medidas no tuvieron éxito- (A) Terminado el contrato o acuerdo, factible; O (B) Si la terminación no es factible, reportó el problema al Secretario	
164.314(a)(2)(i)		Contratos de Asociados de Negocios (R): El contrato entre una entidad cubierta y un asociado de negocios debe proveer que el asociado de negocios: (A) Implementará salvaguardias administrativas, físicas y técnicas que protejan razonablemente y apropiadamente la confidencialidad, integridad y disponibilidad de La información de salud protegida electrónica que crea, recibe, mantiene o transmite en nombre de la entidad cubierta como se requiere en esta subparte; (B) Asegurarse de que cualquier agente, incluido un subcontratista, a quien suministre dicha información, acuerde poner en práctica salvaguardias razonables y apropiadas para protegerla; (C) Informar a la entidad cubierta cualquier incidente de seguridad de que tenga conocimiento; (D) Autorizar la terminación del contrato por parte de la entidad cubierta si la entidad cubierta determina que la empresa asociada ha violado una parte importante del contrato.
164.314(a)(2)(ii)		Otros Acuerdos: Cuando una entidad cubierta y su socio comercial son ambas entidades

		gubernamentales, la entidad cubierta cumple con lo dispuesto en el párrafo (a) (1) de esta sección, si: (1) Celebra un memorando de entendimiento con la empresa Asociado que contenga términos que cumplan los objetivos del párrafo (a) (2) (i) de esta sección; O (2) La otra ley (incluyendo los reglamentos adoptados por la entidad cubierta o su asociada comercial) contiene requisitos aplicables a la asociada que cumplan los objetivos del párrafo (a) (2) (i) de esta sección.
164.314(b)(1)	Requisitos para los Planes de Salud de Grupo: Excepto cuando la única información de salud protegida electrónica revelada a un patrocinador del plan sea divulgada de acuerdo con § 164.504 (f) (1) (ii) o (iii), o como autorizado bajo la Sección 164.508, Debe asegurarse de que los documentos del plan establezcan que el patrocinador del plan protegerá de manera razonable y apropiada la información de salud protegida electrónica creada, recibida, mantenida o transmitida al o por el patrocinador del plan en nombre del plan de salud grupal.	
164.314(b)(2)(i)		Especificación de Implementación del Plan de Salud del Grupo (R): Los documentos del plan del plan de salud grupal deben ser enmendados para incorporar disposiciones que requieran que el patrocinador del plan: (i) implemente salvaguardias administrativas, físicas y técnicas que protejan razonablemente y apropiadamente la confidencialidad, Integridad y disponibilidad de la información de salud protegida electrónica que crea, recibe, mantiene o transmite en nombre del plan de salud del grupo.
164.314(b)(2)(ii)		Especificación de Implementación del Plan de Salud del Grupo (R): Los documentos del plan del plan de salud grupal deben ser enmendados para incorporar disposiciones que requieran que el patrocinador del plan: (ii) Asegure que la separación adecuada requerida por § 164.504 (f) (2) Iii) está respaldado por medidas de seguridad razonables y apropiadas.
164.314(b)(2)(iii)		Especificación de Implementación del Plan de Salud del Grupo (R): Los documentos del plan del plan de salud grupal deben ser enmendados para incorporar disposiciones que exijan al patrocinador del plan: (iii) Asegurar que cualquier agente, incluyendo un subcontratista, a quien provea esta información, Acuerda implementar medidas de seguridad razonables y apropiadas para proteger la información.
164.314(b)(2)(iv)		Especificación de Implementación del Plan de Salud del Grupo (R): Los documentos del plan del plan de salud grupal deben ser enmendados para incorporar disposiciones que exijan al patrocinador del plan: (iv) Informar al plan de salud grupal cualquier incidente de seguridad del cual se da cuenta.
Requisitos de políticas y procedimientos y documentación		
164.316(a)	Políticas y Procedimientos: Implementar políticas y procedimientos razonables y	

	apropiados para cumplir con las normas, especificaciones de implementación u otros requisitos de esta subparte, teniendo en cuenta los factores especificados en § 164.306 (b) (2) (i), (ii), (Iii), y (iv). Esta norma no debe interpretarse para permitir o excusar una acción que viole cualquier otra norma, especificación de implementación u otros requisitos de esta subparte. Una entidad cubierta puede cambiar sus políticas y procedimientos en cualquier momento, siempre que los cambios estén documentados y se implementen de acuerdo con esta subparte.	
164.316(b)(1)	Documentación: (i) Mantener las políticas y procedimientos implementados para cumplir con esta subparte en forma escrita (que puede ser electrónica); Y (ii) Si una acción, actividad o evaluación es requerida por esta subparte para documentarse, mantenga un registro escrito (que puede ser electrónico) de la acción, actividad o evaluación.	
164.316(b)(2)(i)		Límite de Tiempo (R): Conserve la documentación requerida por el párrafo (b) (1) de esta sección durante seis años a partir de la fecha de su creación o la fecha en que estuvo vigente, lo que ocurra más tarde.
164.316(b)(2)(ii)		Disponibilidad (R): Poner la documentación a disposición de las personas responsables de implementar los procedimientos a los que se refiere la documentación.
164.316(b)(2)(iii)		Actualizaciones (R): Revise la documentación periódicamente y actualícela según sea necesario en respuesta a cambios ambientales o operacionales que afecten la seguridad de la información electrónica protegida sobre la salud.

Fuente: (National Institute of Standards and Technology, 2008, pp. 74–78)

2.5. Esquema Gubernamental de Seguridad de la Información (EGSI).

El EGSI publicado por la Secretaría Nacional de la Administración Pública expresa lo siguiente:

Política de Seguridad de la Información

Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013b).

Organización de la Seguridad de la Información

La organización de la seguridad debe cumplir con los acápites que se enumeran a continuación además de formar un comité de coordinación de la seguridad de la información que deberá convocarse de forma periódica o cuando las circunstancias lo ameriten. Se deberá llevar registros y actas de las reuniones.

- Compromiso de la máxima autoridad de la institución con la seguridad de la información.
- Coordinación de la Gestión de la Seguridad de la Información
- Asignación de responsabilidades para la seguridad de la información
- Proceso de autorización para nuevos servicios de procesamiento de la información.
- Acuerdos sobre Confidencialidad
- Contacto con las autoridades
- Contactos con grupos de interés especiales
- Revisión independiente de la seguridad de la información
- Identificación de los riesgos relacionados con las partes externas
- Consideraciones de la seguridad cuando se trata con ciudadanos o clientes
- Consideraciones de la seguridad en los acuerdos con terceras partes

Gestión de los Activos

Inventariar los activos primarios, en formatos físicos y/o electrónicos así como también los activos de soporte Hardware, Software y de Redes; además de inventariar los activos referentes a la estructura organizacional; todo esto con la asignación de responsables de los activos y sus inventarios, uso aceptable de los activos basado en reglamentos; etiquetado y uso de la información. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Seguridad de los Recursos Humanos

Trata sobre las Funciones y responsabilidades, Selección, Términos y condiciones laborales, Responsabilidades de la dirección a cargo del funcionario, Educación, formación y sensibilización en seguridad de la información, Proceso disciplinario, Responsabilidades de terminación del contrato, Devolución de activos y el Retiro de los privilegios de acceso. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Seguridad Física y del Entorno

Toma en consideración el manejo del Perímetro de la seguridad física, Controles de acceso físico, Seguridad de oficinas, recintos e instalaciones, Protección contra amenazas externas y ambientales, Trabajo en áreas seguras, Áreas de carga, despacho y acceso público, Ubicación y protección de los equipos, Servicios de suministro, Seguridad del cableado, Mantenimiento de los

equipos, Seguridad de los equipos fuera de las instalaciones, Seguridad en la reutilización o eliminación de los equipos el Retiro de activos de la propiedad. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Gestión de Comunicaciones y Operaciones

Contempla la gestión de la Documentación de los procedimientos de Operación, Gestión del Cambio, Distribución de funciones, Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción, Presentación del Servicio, Monitoreo y revisión de los servicios, por terceros, Gestión de los cambios en los servicios ofrecidos por terceros, Gestión de la capacidad, Aceptación del Sistema, Controles contra código malicioso, Controles contra códigos móviles, Respaldo de la información, Controles de las redes, Seguridad de los servicios de la red, Gestión de los medios removibles, Eliminación de los medios, Procedimientos para el manejo de la información, Seguridad de la documentación del sistema, Políticas y procedimientos para el intercambio de información, Acuerdos para el intercambio, Medios físicos en tránsito, Mensajería electrónica, Sistemas de información del negocio, Transacciones en línea, Información disponible al público, Registros de auditorías, Monitoreo de uso del sistema, Protección del registro de la información, Registros del administrador y del operador, Registro de fallas, Sincronización de relojes. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Control de Acceso

Trata de establecer una Política de control de acceso, Registro de usuarios, Gestión de privilegios, Gestión de contraseñas para usuarios, Revisión de los derechos de acceso de los usuarios, Uso de contraseñas, Equipo de usuario desatendido, Política de puesto de trabajo despejado y pantalla limpia, Política de uso de los servicios de red, Autenticación de usuarios para conexiones externas, Identificación de los equipos en las redes, Protección de los puertos de configuración y diagnóstico remoto, Separación en las redes, Control de conexión a las redes, Control del enrutamiento en la red, Procedimiento de registro de inicio seguro, Identificación y autenticación de usuarios, Sistema de gestión de contraseñas, Uso de las utilidades del sistema, Tiempo de inactividad de la sesión, Limitación del tiempo de conexión, Control de acceso a las aplicaciones y a la información, Restricción de acceso a la información Aislamiento de sistemas sensibles, Computación y comunicaciones móviles, Trabajo remoto. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Asegura un correcto Análisis y especificaciones de los requerimientos de seguridad, Validación de datos de entrada, Control de procesamiento interno, Integridad del mensaje, Validación de datos de salidas, Política sobre el uso de controles criptográficos, Gestión de claves, Control del software operativo, Protección de los datos de prueba del sistema, Control de acceso al código fuente de los programas, Procedimiento de control de cambios, Revisión técnica de las aplicaciones después de los cambios en el sistema operativo, Restricción del cambio de paquetes de software, Fuga de información, Desarrollo de software contratado externamente, Control de las vulnerabilidades técnicas. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Gestión de los incidentes de la Seguridad de la Información

Intenta establecer procedimientos formales para la elaboración de Reporte sobre los eventos de seguridad de la información, Reporte sobre las debilidades en la seguridad, Responsabilidades y procedimientos, Aprendizaje debido a los incidentes de seguridad de la información, Recolección de evidencias. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Gestión de la continuidad del negocio

Trata sobre la inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio, evaluación de riesgos, el desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información y la ejecución de pruebas, mantenimiento y revisión de los planes de continuidad del negocio. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

Cumplimiento

Habla sobre la Identificación de la legislación aplicable, Derechos de Propiedad Intelectual, Protección de registros en cada entidad, Protección de los datos y privacidad de la información personal, Prevención del uso inadecuado de servicios de procesamiento de información, Reglamentación de controles criptográficos, Cumplimiento con las políticas y las normas de la seguridad, Verificación del cumplimiento técnico, Controles de auditoría de los sistemas de información, Protección de las herramientas de auditoría de los sistemas de información. (Cristian Castillo Peñaherrera & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA, 2013)

2.6. Coincidencias entre las normas ISO 27001 e HIPAA

Una vez analizadas la ISO 27001 y la norma HIPAA se puede establecer coincidencias entre ellas de la siguiente manera:

Tabla 2-1 *Coincidencias entre normas HIPAA e ISO (EGSI)*

HIPAA (45 CFR)	Especificaciones de HIPAA	ISO 27002:2005 Referencia
Regla de Seguridad - medidas de seguridad administrativas		
§164.308(a)(1)(ii)(A)	El análisis de riesgos (Obligatorio). Llevar a cabo una evaluación precisa y exhaustiva de los posibles riesgos y vulnerabilidades a la confidencialidad, integridad y disponibilidad de la información protegida de la salud electrónica en poder de la entidad cubierta.	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
§164.308(a)(1)(ii)(B)	La gestión de riesgos (Obligatorio). Implementar medidas de seguridad suficientes para reducir los riesgos y las vulnerabilidades a un nivel razonable y apropiada para cumplir con § 164.306	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
§164.308(a)(1)(ii)(C)	Política de sanciones (Obligatorio). Aplicar las sanciones adecuadas contra los miembros de la fuerza de trabajo que no cumplan con las políticas y procedimientos de seguridad de la entidad cubierta.	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
§164.308(a)(1)(ii)(D)	Plan de copia de seguridad de datos (obligatorio). Establecer e implementar procedimientos para crear y mantener copias exactas recuperables de información protegida de salud electrónica.	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
§164.308(a)(2)	Estándar: Asignado responsabilidad de la seguridad. Identificar el funcionario de seguridad, que es responsable de la elaboración y aplicación de las políticas y los procedimientos requeridos por esta sub-parte para la entidad	Asignación de responsabilidades de seguridad de la información
§164.308(a)(3)(ii)(A)	Autorización y / o supervisión (Direccionable). Implementar procedimientos para la autorización y / o supervisión de los miembros del personal que trabajan con información protegida de salud electrónica o en lugares en los que se pueda acceder.	SEGURIDAD DE LOS RECURSOS HUMANOS
§164.308(a)(3)(ii)(B)	Procedimiento de liquidación de mano de obra (direccionable). Implementar procedimientos para determinar que el acceso de un miembro de la fuerza de trabajo a la información protegida de la salud electrónica es apropiado.	SEGURIDAD DE LOS RECURSOS HUMANOS
§164.308(a)(3)(ii)(C)	Procedimientos de terminación (direccionables). Implementar procedimientos para la terminación de acceso a la información protegida de la salud electrónica cuando el empleo de un miembro de la fuerza de trabajo termina o se exija mediante determinaciones hechas como se especifica en el párrafo (a) (3) (ii) (B) de esta sección.	SEGURIDAD DE LOS RECURSOS HUMANOS

§164.308(a)(4)(ii)(A)	Aislamiento de las funciones de atención de la salud de intercambio de información (obligatorio). Si un centro de atención de la salud es parte de una organización mayor, la cámara de compensación debe implementar políticas y procedimientos que protegen la información protegida de salud electrónica de la cámara de compensación del acceso no autorizado por la organización más grande.	REQUISITOS PARA EL CONTROL DE ACCESO GESTIÓN DEL ACCESO DEL USUARIO
§164.308(a)(4)(ii)(B)	Autorización de acceso (direccionable). Implementar políticas y procedimientos para otorgar acceso a información de salud protegida electrónica, por ejemplo, a través del acceso a una estación de trabajo, transacción, programa, proceso u otro mecanismo.	Especificación CONFIDENCIAL
§164.308(a)(4)(ii)(C)	Establecimiento de acceso y modificación (direccionable). Implementar políticas y procedimientos que, basados en las políticas de autorización de acceso de la entidad, establezcan, documenten, revisen y modifiquen el derecho de acceso de un usuario a una estación de trabajo, transacción, programa o proceso.	(Divulgado bajo NDA solamente)
§164.308(a)(5)(ii)(A)	Avisos de seguridad (direccionable). Actualizaciones periódicas de seguridad.	Sensibilización, educación y capacitación en materia de seguridad de la información
		Uso de la contraseña
§164.308(a)(5)(ii)(B)	Protección contra software malintencionado (direccionable). Procedimientos para proteger, detectar y reportar software malicioso.	Sensibilización, educación y capacitación en materia de seguridad de la información
		Uso de la contraseña
§164.308(a)(5)(ii)(C)	Monitorización de registro (direccionable). Procedimientos para monitorear los intentos de registro y reportar discrepancias.	Sensibilización, educación y capacitación en materia de seguridad de la información
		Uso de la contraseña

Fuente: (Hash, 2005)

2.7. Recomendaciones de seguridad informática del entorno sanitario.

En la siguiente tabla se identifican y numeran algunas de las recomendaciones de organismos oficiales nacionales e inter-nacionales, normas y estándares de seguridad aplicables a los entornos de AP y que han sido seleccionados para la elaboración de la guía de buenas prácticas de seguridad informática que aborda este trabajo. Además de estas recomendaciones, en el año 2014 está prevista la entrada en vigor de la nueva directiva europea de protección de datos de carácter personal, que podría suponer cambios en la guía presentada en este trabajo.

Tabla 3-2 *Estándares, normas y recomendaciones de seguridad para el ámbito de los centros de atención primaria*

	ESTÁNDARES
1	Estándar ISO 27002 Security techniques Code of practice for information security management
2	Estándar ISO 27799 Information security management in health using ISO/IEC 27002
	RECOMENDACIONES DE ORGANISMOS OFICIALES
	Health Information Technology. Organización para la formación en seguridad y privacidad de los datos personales de salud. Depende del Department of Health & Human Services de EE. UU.
3	Guide to Privacy and Security of Health Information. The Office of the National Coordinator for Health Information Technology. Department of Health and Human Services, EE. UU.
	Instituto Nacional de Tecnologías de la Comunicación (INTECO)
4	Recomendaciones para la creación de una contraseña segura, 20 de noviembre de 2012
	Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT)
5	Guía de Seguridad (CCN-STIC-803) Esquema Nacional de Seguridad. Valoración de los Sistemas 2011
6	Guía de seguridad (CCN-STIC-821) Esquema Nacional de Seguridad. Normas de seguridad. 2012
7	CCN-STIC-821.Apéndice I. Normativa General de Utilización de los Recursos y Sistemas de Información. NG00
8	CCN-STIC-821. Apéndice II. Normas de acceso a Internet. NP10
9	CCN-STIC-821. Apéndice III. Normas de uso del correo electrónico (e-mail). NP20
10	CCN-STIC-821. Apéndice IV. Normas de Seguridad en el ENS. Normas para trabajar fuera de las instalaciones. NP30
11	CCN-STIC-821. Apéndice V. Normas de creación y uso de contraseñas.NP40
12	CCN-STIC-821. Apéndice VI. Acuerdo de confidencialidad para terceros. NP50
13	CCN-STIC-821. Apéndice VII. Modelo de contenido de buenas prácticas para terceros. NP60 NIST (National Institute of Standards and Technology)
14	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule 2009
15	Guide to Enterprise Password Management Recommendations of the National Institute of Standards and Technology
	NORMAS
	HIPAA (Health Insurance Portability and Accountability Act). Ley Federal de EE.UU.
16	HIPAA Handbook for Behavioral Health Staff: Understanding the Privacy and Security Regulations. En: Congress US, editor. 2009

17	Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)
18	Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica
19	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
20	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
21	Acuerdo Ministerial 166, ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI
22	LEY DE DERECHOS Y AMPARO AL PACIENTE

Fuente: (Sánchez-Henarejos et al., 2014)

2.8. Seguridad Física

Por más que una empresa o institución sea la más segura de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma sería un fracaso si no se tiene un plan de acción para combatir un incendio o cualquier otro tipo de desastre natural y no tener presente buenas políticas de recuperación.

La seguridad física es uno de los aspectos más olvidados, si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno que intenta acceder físicamente al data center. Esto puede ocasionar que para un atacante sea más fácil lograr tomar y copiar una cinta de back up o un respaldo fisco de una historia clínica, que intentar acceder vía lógica a la misma.

Por lo tanto, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. (GERARDO CESAR MOSQUERA QUINTERO, JORGE ARMANDO SARAVIA ALVERNIA, & JOSE JULIAN PACHECO PEREZ, 2015)

Teniendo las siguientes ventajas:

- Disminuir siniestros.
- Trabajar mejor manteniendo la sensación de seguridad.
- Descartar falsas hipótesis si se produjeran incidentes.
- Tener los medios para luchar contra accidentes.

Amenazas previstas en Seguridad Física:

- Desastres naturales.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

Desastre. Es un suceso que causa interrupción grave en el funcionamiento de una comunidad causando grandes pérdidas a nivel humano, material o ambiental, suficientes para que la comunidad afectada no pueda salir adelante por sus propios medios, necesitando apoyo externo. Los desastres se clasifican de acuerdo a su origen (natural o tecnológico). (GERARDO CESAR MOSQUERA QUINTERO et al., 2015)

Vulnerabilidad Física. Está relacionada con la calidad o tipo de material utilizado y el tipo de construcción de las viviendas, establecimientos comerciales e industriales y de servicios salud, educación, etc., e infraestructura socioeconómica (central hidroeléctrica, carretera, puente y canales de riego), para asimilar los efectos del peligro. La vulnerabilidad, es el grado de debilidad o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro natural o antrópico de una magnitud dada, se expresa en términos de probabilidad, en porcentaje de 0 a 100.

La vulnerabilidad, es entonces una condición previa que se manifiesta durante el desastre, cuando no se ha invertido lo suficiente en obras o acciones de prevención y mitigación y se ha aceptado un nivel de riesgo demasiado alto. Para su análisis, la vulnerabilidad debe promover la identificación y caracterización de los elementos que se encuentran expuestos, en una determinada área geográfica, a los efectos desfavorables de un peligro adverso.

Mitigar. Es la reducción de los efectos de un desastre con anticipación, principalmente disminuyendo la vulnerabilidad.

2.8.1. Seguridad Física y del Entorno o Ambiente

Áreas Seguras.- Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización o institución (GERARDO CESAR MOSQUERA QUINTERO et al., 2015, p. 26).

- Perímetro de Seguridad Física.- Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información y medios de procesamiento de información.

- Controles de Ingreso Físico.- Para asegurar que sólo se le permita el acceso al personal autorizado.
- Protección contra Amenazas Externas e Internas.- Se asigna y aplica protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.
- Trabajo en Áreas Aseguradas.- Se diseña y aplica la protección física y los lineamientos para trabajar en áreas aseguradas.
- Áreas de Acceso Público, Entrega y Carga.- Control 6: Se controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y, se aísla de los medios de procesamiento de información para evitar el acceso no autorizado.

Equipo de Seguridad.- Evita la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización (GERARDO CESAR MOSQUERA QUINTERO et al., 2015, p. 27).

- Ubicación y Protección del equipo.- Se ubica o protege el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no autorizado.
- Servicios Públicos de Soporte.- Se protege el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
- Seguridad del Cableado.- El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño.
- Mantenimiento de Equipo.- Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e integridad
- Seguridad de la Eliminación o Re uso del Equipo.- Se debieran chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación. Los dispositivos que contienen data confidencial pueden requerir una evaluación del riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.
- Retiro de Propiedad.- El equipo, información o software no debiera retirarse sin autorización previa. También se pueden realizar chequeos inesperados para detectar el retiro de propiedad, dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso al local. Estos chequeos inesperados debieran ser llevados a cabo en concordancia con la legislación y regulaciones relevantes. Las personas debieran saber que se llevan a cabo chequeos inesperados, y los chequeos se debieran realizar con la debida autorización de los requerimientos legales y reguladores.

2.9. Evaluación de Riesgo.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

Figura 5-2. *Modelo de Gestión de Riesgos.*

Fuente: ("ISO 27001", 2013)

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Los dos puntos importantes a considerar son:

- La probabilidad de una amenaza

- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad.

2.9.1. Determinación de la probabilidad.

Con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- Fuente de la amenaza y su capacidad.
- Naturaleza de la vulnerabilidad.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media-baja y baja.

Tabla 4-2 *Probabilidad de una vulnerabilidad potencial*

Nivel	Definición
Alta	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo.
Media-Alta	La amenaza está fundamentada y es posible.
Media	La amenaza es posible.
Media-Baja	La amenaza no posee la suficiente capacidad.
Baja	La amenaza no posee la suficiente motivación y capacidad.

Fuente: (Chacón Mejía, 2012)

La probabilidad es una medida sobre la escala 0 a 1 de tal forma que (Muñoz, 2012):

- Al suceso imposible le corresponde el valor 0
- Al suceso seguro le corresponde el valor 1
- El resto de sucesos tendrán una probabilidad comprendida entre 0 y 1

Figura 6-2 *Escala de valor de probabilidad*

Fuente: (Hern, Hern, & ez, s/f)

Número de ocurrencias del evento en un periodo de un año.

Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de potencia, falla en las comunicaciones, utilizamos información obtenida de ciertas publicaciones tecnológicas como Information Week e Infosecurity.

De esta manera se define una escala en la cual, a una probabilidad alta, le asignamos el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al número de veces que el evento puede ocurrir en un periodo de un año. Para el caso P=5 se considera que ocurre al menos dos veces al año.

2.9.2. Identificación de vulnerabilidades.

Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinan vulnerabilidades a nivel del sistema operativo y firewall:

- Seguridad Física. (Monitoreo ambiental, Control de acceso, Desastres naturales, Control de incendios, Inundaciones)
- Seguridad en las conexiones a Internet. (Políticas en el Firewall, VPN, Detección de intrusos)
- Seguridad en la infraestructura de comunicaciones. (Routers, Switches, Firewall, Hubs, RAS)
- Seguridad en Sistema Operacionales (Unix, Windows)
- Correo Electrónico
- Seguridad en las aplicaciones Críticas.- Se define las aplicaciones que son críticas para la organización y por cada una de ellas se obtendrá una matriz de riesgo. Es importante considerar que las aplicaciones están soportadas por: Sistemas operativos, hardware servidor, redes LAN y WAN, y el Centro de cómputo.

También con el fin de realizar una correspondencia con los datos obtenidos por medio de las listas de verificación, contamos con el uso de una herramienta especializada fabricada por GFI Languard, la cual identifica vulnerabilidades en los sistemas operativos, ayudándonos de esta forma en el proceso de identificación de vulnerabilidades. A continuación se muestra algunas de las características de esta herramienta:

- Búsqueda de vulnerabilidades en su red (Windows y Linux)
- Directorios compartidos, puertos abiertos, cuentas no usadas.
- Revisión de actualizaciones aplicadas en los sistemas operativos.
- Detección de dispositivos USB

2.9.3. Análisis del impacto y el factor de riesgo

El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos:

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- La importancia crítica de los datos y el sistema (importancia a la organización).
- Sensibilidad de los datos y el sistema.

Identificación de controles.

En esta fase se evaluarán las conclusiones de la valoración respecto a ISO 17799 y la matriz de riesgo con el fin de identificar los controles que mitiguen los riesgos encontrados.

Plan de Implementación Tecnológica.

El plan de Implementación tecnológica, se presenta como una herramienta para el control por parte de las actividades que se deben llevar a cabo para mitigar los riesgos identificados, en la evaluación de riesgo del proyecto en curso y de acuerdo al alcance definido.

De esta forma la seguridad hoy en día se ha convertido en la carta de navegación para el tema de la inversión en tecnología, debemos en toda inversión tecnológica considerar aspectos relacionados con la gestión de la seguridad, con el fin de que esta inversión este alineada plenamente con la estrategia del negocio y garantice de manera efectiva y eficiente su continuidad.

2.10. Consecuencias derivadas de amenazas a la seguridad

Las amenazas son acontecimientos que pueden desencadenar un incidente en el centro de salud, produciendo impactos materiales o inmateriales en los recursos del sistema de información o relacionados con este, necesarios para que el centro funcione correctamente. Las consecuencias de estos impactos, producidos o no por una negligencia de sus trabajadores, pueden ser muy variadas y han de ser asumidas por la casa de salud:

- Daños de imagen. Generan impacto negativo en la imagen del centro y además generan pérdida de confianza de los pacientes en el mismo.
- Consecuencias legales. Se enmarcan en el ámbito legal, y podrían conllevar sanciones económicas o administrativas. Se debe tener en cuenta que la Ley Orgánica de Protección de Datos (LOPD) establece como falta muy grave recabar y tratar datos especialmente protegidos sin consentimiento del afectado y vulnerar el deber de secreto sobre estos datos.
- Otras consecuencias. Son aquellas que tienen impacto negativo en ámbitos muy diversos, como por ejemplo el ámbito político, institucional o gubernamental, entre otros. En general se trata de consecuencias que no están englobadas en los otros 2 tipos.

2.11. Clasificación de las amenazas a datos personales de salud

Los datos personales de salud incluyen cualquier información relacionada con un determinado paciente, ya sean en formato electrónico, escrito u oral. Suelen contener un identificador, como el nombre, la fecha de nacimiento, el número de teléfono, la dirección de correo electrónico, etc., que los relaciona con la identidad del paciente de manera inequívoca.

Tabla 5-2 *Clasificación de las amenazas que pueden producir un problema de seguridad en la organización*

Nivel	Clasificación de amenazas
1	*Divulgación accidental (accidental disclosure).* El trabajador sanitario, sin querer, revela información del paciente a otros. Por ejemplo, mensaje de correo electrónico enviado a la dirección incorrecta
2	*Empleado curioso.* Un trabajador con privilegios de acceso a los datos de un paciente accede a ellos por curiosidad o para sus propios fines. Por ejemplo, un profesional sanitario que accede a la información de salud de un compañero de trabajo
3	*Violación de la privacidad de los datos por un trabajador.* Miembro del personal que tiene acceso a la información de un paciente y la transmite al exterior con ánimo de lucro o por algún tipo de animadversión hacia un paciente
4	*Violación de la privacidad de los datos por un externo con intrusión física.* Un externo que entra en la instalación física y de manera forzada accede al sistema
5	*Intrusión no autorizada en la red del sistema.* Un externo, ex empleado, paciente o hacker que se introduce en la red del sistema de la organización desde el exterior y accede a la información del paciente o hace que el sistema deje de funcionar (ataque a la disponibilidad)

Fuente: (Sánchez-Henarejos et al., 2014)

Las amenazas a la privacidad y a la seguridad de los datos personales del paciente en un centro de salud, son aquellas que surgen del acceso inadecuado a estos datos, ya sea por personal interno abusando de sus privilegios o por errores no intencionados, o por agentes externos que explotan la vulnerabilidad de los sistemas de información con ataques intencionados. La tabla muestra una clasificación de las amenazas de seguridad de 5 niveles, según aumenta la sofisticación de la amenaza (Sánchez-Henarejos et al., 2014)

2.12. Tendencias actuales de las amenazas a los datos personales de salud

Existen gran cantidad de incidentes derivados de deficiencias en la seguridad de las instalaciones sanitarias, o a causa de errores o descuidos del personal en la manipulación de los datos de pacientes.

1. Acceso a los datos de la hija menor de una doctora que trabajaba en un centro hospitalario, por parte de trabajadores del mismo sin consentimiento de la madre (2007). Tanto personal médico como administrativo accedieron a los datos médicos de la menor para consultar, modificar e imprimir información, sin previa autorización de su madre, trabajadora del centro (nivel2).
2. Cuatro mil historias clínicas de abortos se filtran en la red a través de eMule (2008). Un empleado de una clínica, que intentaba descargarse archivos desde el ordenador del trabajo a través de eMule, pudo provocar que 11.300 historias clínicas, de ellas 4.000 de casos de aborto, terminasen expuestas a cualquier internauta (nivel 1).
3. Un virus se introduce en los ordenadores de Sanidad (2009). Un virus se introdujo en los ordenadores de los hospitales y centros de salud madrileños. La incidencia impidió el acceso a las historias clínicas y las analíticas de los pacientes (nivel 5).
4. Una unidad flash fue robada del Departamento de Personal de un Hospital Provincial (2010). La unidad contenía datos personales que fueron robados tras forzar la puerta de un despacho (nivel 4).
5. Filtradas a través de Google 2 radiografías de pulmón de un paciente (2011). Un grupo *hospitalario español tuvo que indemnizar a un paciente que, haciendo una búsqueda por G*oogle, encontró 2 radiografías de pulmón que se le habían practicado (nivel 3).

Además de estos casos mediáticos, existen numerosas denuncias a la AEPD por violaciones de datos derivadas de malas prácticas del personal de la organización. En 2011, la AEPD resolvió 18 procedimientos sancionadores en sanidad por un importe de 143.204 euros. En enero de 2013, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), publicó el informe Threat Landscape. Responding to the Evolving ThreatEnvironment15, que indica las tendencias en los ataques a sistemas y organizaciones del año 2012. El documento Threat Landscape de ENISA recoge 120 informes procedentes de la industria de la seguridad, redes de excelencia, organismos de normalización y otros, entre 2011 y 2012,y proporciona una visión de conjunto de las amenazas observadas, las que actualmente son más importantes y las tendencias emergentes en este ámbito. También identifica las 10 principales amenazas en áreas de tecnologías emergentes. Las conclusiones fueron:

1. El año 2011 se caracterizó por ser el año de las violaciones de privacidad de los datos. Aumentó el interés delos cibercriminales por atacar sistemas de información sanitarios.
2. En los últimos años el número de violaciones en la privacidad de los datos en las organizaciones sanitarias aumentó con la adopción de sistemas de historia clínica digital.
3. La mayor parte de violaciones de la privacidad de los datos se produjo a consecuencia de negligencias de trabajadores y por ataques externos.

4. Nueve de cada 10 violaciones se pudieron haber pre-venido si las organizaciones hubiesen seguido buenas prácticas en la seguridad de los datos.
5. Entre enero y junio de 2012 el número de episodios que comprometieron la confidencialidad del sistema de información en organizaciones sanitarias casi se duplicó. El 96% de todas las organizaciones sanitarias encuestadas en el informe experimentaron al menos una violación de datos en los últimos años. Por tanto, es crucial vigilar y actualizar los hábitos de seguridad del personal con acceso a los sistemas informáticos de la organización sanitaria.

CAPITULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1. Tipo y diseño del estudio.

3.1.1. Diseño de la Investigación

La investigación es del tipo Cuasi-Experimental ya que se escoge varios métodos, normas y buenas practicas que serán utilizadas como base para la creación del nuevo método para el manejo de información segura en los registros médicos de los pacientes atendidos en el Hospital del IESS de la ciudad de Guaranda, y los datos que se obtendrán de las pruebas serán generados en esta investigación por el autor de esta investigación.

3.1.2. Tipo de la investigación.

Es de tipo descriptiva y aplicada, puesto ya que se basa en conocimientos existentes, derivados de investigaciones previas, dirigida al desarrollo tecnológico en la seguridad de la información de los registros médicos de las personas para establecer un nuevo esquema o marco de trabajo para mejorar los existentes.

3.2. Método de investigación.

Se utiliza el método científico ya que se refiere a la serie de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten fiables, el cual consta de las siguientes etapas:

- Planteamiento del problema
- Formulación dela hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis

- Difusión de resultados

Método deductivo debido que al estudiar el riesgo generado por las no conformidades encontradas en la seguridad de la información, se trata de encontrar un marco de trabajo adecuado de seguridad que contenga las mejores características de las normas ISO 27001 y de las HIPPA.

3.3. Fuentes de información.

Se basa en revisión de fuentes de información bibliográficas primarias como Pruebas y Observación de resultados y secundarias como:

- Tesis realizadas internacionales y nacionales de cuarto nivel
- Trabajos de investigaciones internacionales y nacionales
- Artículos científicos en base de datos de bibliotecas virtuales
- Diccionarios especializados
- Conferencias académicas, congresos, seminarios
- Revistas indexadas y no indexadas publicadas de prestigio
- Revistas electrónicas
- Páginas de internet que brinden información confiable.
- Estándares internacionales:
    - ISO 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.
    - ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
    - Código Federal de Regulaciones. CFR 2007 título 45.

3.4. Técnicas de recolección de datos

La técnica utilizada en el estudio es la búsqueda de información obtiene la información necesaria acerca del objeto de estudio de la investigación para su desarrollo, utilizando las fuentes secundarias disponibles.

- Observación.
- Recopilación de información.

- Análisis.

Todas las fuentes de información permiten establecer un marco de trabajo adecuado de seguridad que contenga las mejores características de las normas ISO 27001 y de las HIPPA, que debe ser implementada para su respectiva verificación estableciéndose un índice de seguridad promedio inicial previo a su instalación que será confrontado con el índice obtenido luego de la implementación.

3.5. De terminación de las Variables.

Variable Independiente:

Propuesta de adaptación de las Normas ISO 27001 e HIPPA.

Variable Dependiente:

Reducción de riesgos en la seguridad de los sistemas de información

3.6. Operacionalización conceptual de variables

VARIABLE	TIPO	CONCEPTO
Propuesta de adaptación de las Normas ISO 27001 e HIPPA	Variable Independiente	Establecer un Modelo de políticas de implementación basados en la adaptación de normas ISO e HIPPA
Reducción de riesgos en la seguridad de los sistemas de información	Variable Dependiente	Atenuar la probabilidad de no conformidades en la seguridad de los datos considerados privados en las Historias Clínicas

3.7. Operacionalización metodológica de variables

HIPOTESIS	VARIABLES	INDICADORES	INDICES	TECNICA
La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS.	**V. Independiente.** Propuesta de adaptación de las Normas ISO 27001 e HIPPA.	Confidencialidad	Salvaguardias administrativas	Observación, Análisis
		Privacidad	Salvaguardias físicas y técnicas	Observación, Análisis
		Integridad	Políticas y procedimientos	Observación, Análisis
		Procedimientos adecuados	Requisito organizacional y requisitos de documentación	Observación, Análisis
	V. Dependiente. Reducción de riesgos en la seguridad de los sistemas de información.	Divulgación accidental	Estrategia relacionada con el cumplimiento de HIPAA	Recopilación de información
		Empleado curioso.	Seguridad de la información	Recopilación de información
		Violación de la privacidad de los datos por un trabajador.	Capacitación para el uso adecuado de la computadora en relación con la seguridad de la información	Recopilación de información

3.8. Población.

La población es el conjunto de todos los elementos que pueden ser evaluados, es así que las Unidades Médicas del IESS ofrecen una amplia variedad de servicios para pacientes hospitalizados y / o ambulatorios a los afiliados atendidos, categorizándose en los Hospitales de nivel 1 de manera general en áreas como:

- Consulta Externa (por la presente se referencia como CE)
- Servicios auxiliares de diagnóstico (por la presente se referencia como SA)
- Emergencia (por la presente se referencia como EM)
- Hospitalización (por la presente se referencia como HO)
- Administrativos y de docencia. (por la presente se referencia como ADM)

El presente estudio es realizado en el Hospital de Nivel 1 del IESS Guaranda, como representante de las unidades hospitalarias de primer nivel, el número total de personal que trabaja en estas áreas o categorías antes descritas es de ciento veinticinco (125) funcionarios dispersos en las áreas antes mencionas.

3.9. Selección de la muestra

Para seleccionar una porción representativa de la población, que permita generalizar los resultados de la investigación, y por motivos de factibilidad relacionados con la disponibilidad de recursos se establece una muestra del tipo probabilístico tomada de los 125 funcionarios.

3.10. Tamaño de la muestra

Se establece el tamaño de la muestra en función de la Fórmula (Willan GOO, De, Raúl Hatt).

$$n = \frac{N\sigma^2 Z^2}{e^2(N-1) + \sigma^2 Z^2}$$

Donde:

n = el tamaño de la muestra.

N = tamaño de la población (125).

σ = Desviación estándar de la población equivalente a un valor constante de 0,5.

Z = Valor obtenido mediante niveles de confianza. Nivel de confianza deseado (1,645) valor para el 90%

e = Límite aceptable de error muestral (0,1) para el 10 %.

$$n = \frac{125 \cdot 0{,}5^2 \cdot 1{,}645^2}{0{,}1^2(125 - 1) + 0{,}5^2 \cdot 1{,}645^2}$$

$$n = \frac{84{,}56}{1{,}92} = 44{,}04$$

Estableciéndose el tamaño de la muestra en 44 personas que deben ser consideradas para el estudio, para lo cual serán seleccionadas en función al número de personas que trabajen en las áreas categorizadas en la población.

3.11. Instrumentos de recolección de datos

La recolección de datos utilizada es una encuesta antes y luego de la implementación del modelo de adaptación de las normas ISO 27001 e HIPAA a la misma muestra de la población establecida, y la verificación de un análisis documental que se aplica en un momento en particular, con la finalidad de buscar información que será útil para evaluar los indicadores de las variables planteadas; encuesta adaptada de la publicada en el artículo "Security awareness for healthcare information systems: A HIPAA compliance perspective" publicado por Issues in Information Systems, (Mishra, Leone, Caputo, Calabrisi, & Morris, 2011), el modelo de cuestionario se puede verificar en el Anexo A.

Se debe indicar además que la infraestructura tecnológica del IESS a nivel nacional es restringida, controlada y monitoreada por el nivel central a través de la Dirección Nacional de Tecnologías de la Información, departamento con la que se trabajó mancomunadamente para la identificación y corrección de vulnerabilidades a nivel de equipos de telecomunicaciones.

3.12. Instrumentos para procesar datos recolectados.

Como instrumentos para procesar los datos recolectados se utiliza el software Microsoft Excel y SPSS para la tabulación y análisis estadístico de las encuestas aplicadas, y los reportes de auditoria del sistema MIS AS-400 como fuente de confrontación de uso adecuado del acceso a la información de la Historia Clínica.

3.13. Identificación y Priorización de Riesgos.

Denominamos **INCIDENCIA** al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

Riesgo: Es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.

3.13.1. Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. Se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permite categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

3.13.2. Probabilidad del Riesgo

Es la probabilidad de ocurrencia de un evento, resulta de gran importancia para determinar qué tan posible es que dicho evento se presente en la realidad. Según Andréi Kolmogórov La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio, asimismo, la probabilidad debe ser inferior a “1” o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

En función a la escala de valor de probabilidad publicada por Juan Hernández se puede establecer una tabla de Probabilidad de Ocurrencia:

Tabla 1-3 *Probabilidad de Ocurrencia*

PROBALIDAD DE OCURRENCIA	DESCRIPCION	VALOR
Frecuente	Incidentes repetidos	0.75 – 1.00
Probable	Incidentes aislados	0.5 - 0.74
Ocasional	Sucede alguna vez	0.25 – 0.45
Nulo	Improbable que suceda	0.0 – 0.24

Fuente: (Hern et al., s/f)

3.13.3. Impacto del Riesgo

Es importante contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia.

Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto. Para nuestro caso, se clasifica el impacto con una escala numérica del 1 al 4.

Tabla 2-3 *Impacto del riesgo*

IMPACTO	DESCRIPCION	VALOR
Bajo Impacto	Pérdida de Información y/o equipamiento no Sensitivo	1
Medio Impacto	Pérdida de información sensible	2
Alto Impacto	Pérdida de información sensible, retraso o interrupción	3
Gran Impacto	Información crítica, daño serio, patrimonial	4

Fuente: (Benitez & Malin, 2010)

Viendo la necesidad en el entorno empresarial de este tipo de herramientas y teniendo en cuenta que, una de las principales causas de los problemas dentro del entorno informático, es la inadecuada administración de riesgos informáticos, este trabajo sirve de apoyo para una adecuada gestión de la administración de riesgos, es así que un bajo impacto con un valor de 1 se considera a la perdida de información o equipamiento que maneje información no sensible o publica de los

afiliados; un impacto medio con un valor 2 hace referencia a información sensible del paciente, como número de cédula, número de historia clínica, datos personales de carácter privado; se considera como alto impacto a la perdida de información sensible en las cuales involucren también retrasos en la obtención o almacenamiento de dicha información por diferentes motivos, como la perdida de conexiones de red, o denegación de servicios; la pérdida o exposición de datos críticos de los afiliados, como datos de diagnósticos, exámenes, tratamientos, es considerado como de gran impacto por lo que se le da el valor de 4 considerado como el máximo establecido.

3.13.4. Ponderación del Riesgo

Según Benitez y Malin en "Evaluating re-identification risks with respect to the HIPAA privacy rule" la ponderación del riesgo o Riesgo Total, es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

Tomado en consideración que el valor máximo de ponderación puede ser el valor de 4 y el mínimo 0 para una máxima y mínima probabilidad de ocurrencia del riesgo, según podemos establecer que un valor pesimista esperado puede ser de 3.5 sobre 4 aplicando el criterio Hurwicz se establece que de la mediana es el valor de 2 por lo que los riesgos de ponderación superior a los 2.5 puntos se les puede considerar como críticos.

3.13.5. Identificación de Riesgos

Después de haber ponderado y validado objetivamente las probabilidades de ocurrencia de riesgos comunes en los Hospitales de Nivel 1 del IESS se observa que los siguientes riesgos, indicados en la siguiente tabla, son los que con mayor frecuencia ocurren.

Tabla 3-1 *Riesgos identificados*

Ítem	Amenazas
1	Divulgación accidental

2	Empleado curioso.
3	Violación de la privacidad de los datos por un trabajador.
4	Intrusión no autorizada en la red del sistema.
5	Infección de equipos por virus
6	Perdidas de los sistemas centrales
7	Sustracción o robo de información
8	Confidencialidad por exposición al internet
9	Privacidad por uso de redes compartidas
10	Integridad
11	Procedimientos adecuados

Fuente: Ing. Christian Barragán, 2016

Realizado por: Ing. Christian Barragán, 2016

Los riesgos identificados fueron establecidos luego de un análisis de vulnerabilidades existentes en el Hospital con el uso de herramientas como GFI, OpenVAS y NeXpose.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Análisis de la situación actual.

Dentro de la encuesta se establece la probabilidad de ocurrencia de un Riesgo establecido en función del promedio de las respuestas obtenidas a las preguntas establecidas para la evaluación de cada riesgo; es así que el cálculo de la probabilidad de ocurrencia del riesgo evaluado es igual a:

$$Probabilidad = \frac{Promedio\ de\ Respuestas\ negativas}{Total\ de\ la\ población\ encuestada}$$

Obteniéndose los siguientes resultados:

Tabla 1-4 *Datos de respuestas Probabilidad de ocurrencia de riesgos identificados*

Ítem	Amenazas	SI	NO	PROBABILIDAD
1	**Divulgación accidental**	**14,00**	**30,00**	**0,68**
	¿En el Hospital, hay un plan acordado para los esfuerzos de seguridad y cumplimiento de la privacidad de los datos clínicos?	2	42	
	Se le proporciona regularmente capacitación sobre medidas de seguridad	0	44	
	El acceso al sistema se basa en el papel que desempeño en el Hospital	40	4	
2	**Empleado curioso.**	**6,33**	**37,67**	**0,86**
	Crear conciencia de seguridad es un proceso continuo en el Hospital	10	34	
	En el Hospital, los controles de seguridad (control de acceso, política de contraseñas) se consideran un componente necesario para la seguridad	5	39	
	Existe una estructura clara para la acción de observación y manipulación de la información del afiliado	4	40	
3	**Violación de la privacidad de los datos por un trabajador.**	**9,00**	**35,00**	**0,80**
	En el Hospital, hay controles internos adecuados (políticas, procedimientos, capacitación, restricciones de acceso) para proporcionar seguridad y privacidad de los registros de salud	3	41	
	Estoy obligado a informar sobre cualquier uso indebido de la información (de la que estoy a cargo) o su acceso inapropiado	15	29	
4	**Intrusión no autorizada en la red del sistema.**	**18,50**	**25,50**	**0,58**
	El acceso al sistema se basa en el rol que desempeño dentro del Hospital	35	9	
	En el Hospital, tengo comunicación frecuente sobre temas de ingeniería social y soy consciente de cómo tales tácticas pueden crear vulnerabilidad para nuestro sistema	2	42	
5	**Infección de equipos por virus**	**36,00**	**8,00**	**0,18**
	En el Hospital, entiendo qué información tengo acceso y por qué?	40	4	
	En el Hospital, tengo que tomar permiso para usar sitios de redes sociales	38	6	
	Tengo conocimiento del procedimiento sobre qué hacer cuando mi sistema tiene malware en el Hospital	30	14	
6	**Perdidas de los sistemas centrales**	**38,00**	**6,00**	**0,14**

	La disponibilidad de comunicación con el sistema MIS-AS400 es permanente	40	4	
	Las políticas y procedimientos de seguridad alojadas en el repositorio del Hospital, son fácilmente accesibles y comprensibles en el Hospital	36	8	
7	**Sustracción o robo de información**	**22,33**	**21,67**	**0,49**
	Existe una estructura clara para la acción disciplinaria en caso de incumplimiento de las políticas y procedimientos en el Hospital	4	40	
	Tengo que acceder a la información de salud sólo a través de dispositivos y software aprobados en la organización	38	6	
	Tengo permiso para usar medios de almacenamiento extraíbles desde el exterior en mi máquina en la organización	25	19	
8	**Confidencialidad por exposición al internet**	**10,50**	**33,50**	**0,76**
	Se establece dentro del Hospital la importancia de administrar la información que no debemos divulgar salvo en casos de emergencia	20	24	
	Con frecuencia recibo información sobre la legislación vigente que trata sobre la confidencialidad de los datos del paciente	1	43	
9	**Privacidad por uso de redes compartidas**	**22,00**	**22,00**	**0,50**
	El Hospital, posee una estructura clara para el procedimiento de entrega de información de salud	30	14	
	Tengo conocimiento de la directiva de contraseñas que tengo que cumplir, en el Hospital	14	30	
10	**Integridad**	**1,00**	**43,00**	**0,98**
	La auditoría se considera una acción complementaria necesaria para mejorar la seguridad Iniciativas en el Hospital	0	44	
	En el Hospital, las políticas y procedimientos de seguridad son revisados periódicamente	2	42	
11	**Procedimientos adecuados**	**11,00**	**33,00**	**0,75**
	Hay un liderazgo visible sobre la seriedad de los esfuerzos de seguridad en el Hospital	15	29	
	La auditoría es vista como una acción complementaria necesaria para mejorar las iniciativas de seguridad en el Hospital	10	34	
	Tengo que leer las políticas de seguridad con frecuencia (trimestral, bi-anual, anual) en el Hospital	8	36	

Realizado por: Ing. Christian Barragán, 2016

De esta forma se puede obtener una ponderación de ocurrencia evaluando el impacto de que ocurra el riesgo evaluado, en función a la escala de impacto definida anteriormente, para lo cual se obtiene los siguientes datos:

Tabla 2-4 *Ponderación de ocurrencia de riesgos identificados*

Ítem	Amenazas	Probabilidad	Impacto	Ponderación
1	Divulgación accidental	0,68	4	2,73
2	Empleado curioso.	0,86	4	3,42
3	Violación de la privacidad de los datos por un trabajador.	0,80	4	3,18
4	Intrusión no autorizada en la red del sistema.	0,58	4	2,32
5	Infección de equipos por virus	0,18	1	0,18
6	Perdidas de los sistemas centrales	0,14	3	0,41
7	Sustracción o robo de información	0,49	4	1,97
8	Confidencialidad por exposición al internet	0,76	4	3,05
9	Privacidad por uso de redes compartidas	0,50	3	1,50

10	Integridad	0,98	3	2,93
11	Procedimientos adecuados	0,75	3	2,25

Realizado por: Ing. Christian Barragán, 2016

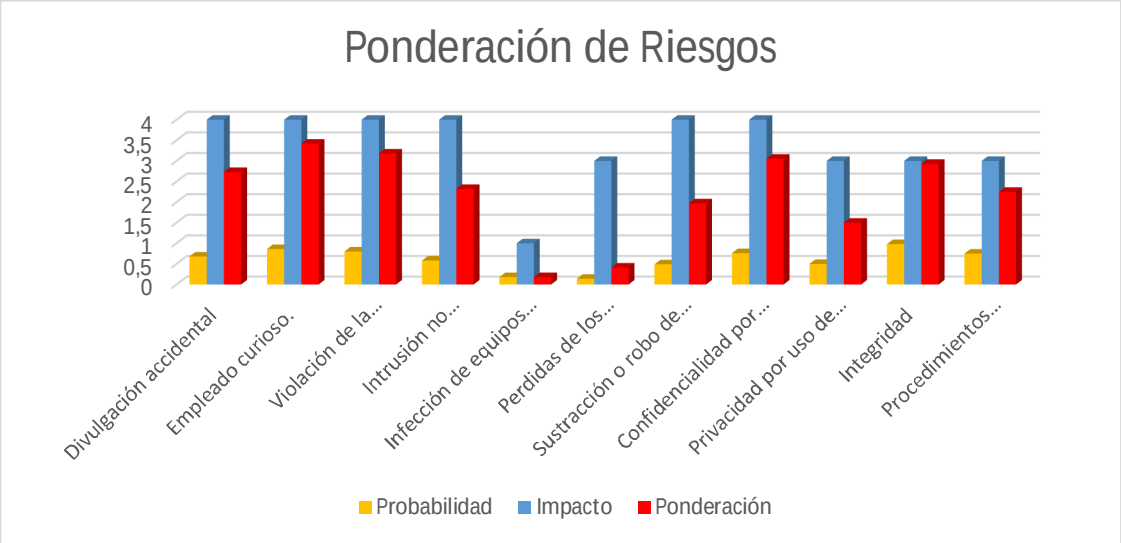

Gráfico 1-4 *Ponderación de riesgos.*

Realizado por: Ing. Christian Barragán, 2017.

En base a este análisis se puede establecer que los riesgos de ponderación superior a los 2.5 puntos son los riesgos más críticos y a los que más atención se debe prestar, por lo que se debe implementar con mayor urgencia una solución para los siguientes riesgos ordenados de mayor a menor prevalencia en función a su ponderación:

Tabla 3-4 *Riesgos de mayor prevalencia*

Ítem	Amenazas	Ponderación
1	Divulgación accidental	3,42
2	Empleado curioso.	3,18
3	Violación de la privacidad de los datos por un trabajador.	3,05
8	Confidencialidad por exposición al internet	2,73
10	Integridad	2,93

Realizado por: Ing. Christian Barragán, 2016

Lo que significa que el la divulgación accidental de información por desconocimiento de la normativa legal vigente, por desconocimiento o falta de una política explicita que permita asegurar el principal activo de la unidad médica (registros médicos) con el afán de cumplir con

las características principales de confidencialidad y privacidad en las que se basa la norma HIPPA, tomando en cuenta la integridad de la información que está presente en la norma ISO 27001.

Un empleado curioso está estrechamente ligada a la violación de la privacidad de los datos por un trabajador puesto que también está susceptible a divulgación de información confidencial de los registros de salud, puesto que ingresa a datos sensibles de la historia clínica sin autorización expresa del paciente, hecho que se corrobora con los datos obtenidos de auditoria del sistema MIS-AS400 en el cual existe un número de 52 consultas de datos versus apenas 23 autorizaciones expresadas.

Como nos podemos dar cuenta se está afectando directamente a la Confidencialidad, Privacidad, Integridad, de la información sensible de los datos clínicos de un paciente por la falta de procedimientos adecuados que permitan asegurar dicha información.

4.2. Análisis de la situación Post-Implementación.

Una vez implementadas las políticas de seguridad establecidas por la adaptación de las normas ISO 27001 e HIPAA se aplicó nuevamente la misma encuesta con la que se hizo el diagnóstico y análisis inicial para la evaluación de la probabilidad de ocurrencia de un Riesgo establecido siguiendo la misma metodología de análisis, por lo que se obtuvo los siguientes resultados:

Tabla 4-1 *Datos de respuestas Probabilidad de ocurrencia de riesgos identificados Post-Implementación*

Ítem	Amenazas	SI	NO	PROBABILIDAD
1	**Divulgación accidental**	**38,00**	**6,00**	**0,14**
	¿En el Hospital, hay un plan acordado para los esfuerzos de seguridad y cumplimiento de la privacidad de los datos clínicos?	35	9	
	Se le proporciona regularmente capacitación sobre medidas de seguridad	36	8	
	El acceso al sistema se basa en el papel que desempeño en el Hospital	43	1	
2	**Empleado curioso.**	**37,67**	**6,33**	**0,14**
	Crear conciencia de seguridad es un proceso continuo en el Hospital	38	6	
	En el Hospital, los controles de seguridad (control de acceso, política de contraseñas) se consideran un componente necesario para la seguridad	37	7	
	Existe una estructura clara para la acción de observación y manipulación de la información del afiliado	38	6	
3	**Violación de la privacidad de los datos por un trabajador.**	**36,50**	**7,50**	**0,17**

	En el Hospital, hay controles internos adecuados (políticas, procedimientos, capacitación, restricciones de acceso) para proporcionar seguridad y privacidad de los registros de salud	40	4	
	Estoy obligado a informar sobre cualquier uso indebido de la información (de la que estoy a cargo) o su acceso inapropiado	33	11	
4	**Intrusión no autorizada en la red del sistema.**	**39,00**	**5,00**	**0,11**
	El acceso al sistema se basa en el rol que desempeño dentro del Hospital	42	2	
	En el Hospital, tengo comunicación frecuente sobre temas de ingeniería social y soy consciente de cómo tales tácticas pueden crear vulnerabilidad para nuestro sistema	36	8	
5	**Infección de equipos por virus**	**41,33**	**2,67**	**0,06**
	En el Hospital, entiendo qué información tengo acceso y por qué?	42	2	
	En el Hospital, tengo que tomar permiso para usar sitios de redes sociales	43	1	
	Tengo conocimiento del procedimiento sobre qué hacer cuando mi sistema tiene malware en el Hospital	39	5	
6	**Perdidas de los sistemas centrales**	**40,50**	**3,50**	**0,08**
	La disponibilidad de comunicación con el sistema MIS-AS400 es permanente	39	5	
	Las políticas y procedimientos de seguridad alojadas en el repositorio del Hospital, son fácilmente accesibles y comprensibles en el Hospital	42	2	
7	**Sustracción o robo de información**	**40,33**	**3,67**	**0,08**
	Existe una estructura clara para la acción disciplinaria en caso de incumplimiento de las políticas y procedimientos en el Hospital	39	5	
	Tengo que acceder a la información de salud sólo a través de dispositivos y software aprobados en la organización	40	4	
	Tengo permiso para usar medios de almacenamiento extraíbles desde el exterior en mi máquina en la organización	42	2	
8	**Confidencialidad por exposición al internet**	**39,00**	**5,00**	**0,11**
	Se establece dentro del Hospital la importancia de administrar la información que no debemos divulgar salvo en casos de emergencia	40	4	
	Con frecuencia recibo información sobre la legislación vigente que trata sobre la confidencialidad de los datos del paciente	38	6	
9	**Privacidad por uso de redes compartidas**	**41,50**	**2,50**	**0,06**
	El Hospital, posee una estructura clara para el procedimiento de entrega de información de salud	40	4	
	Tengo conocimiento de la directiva de contraseñas que tengo que cumplir, en el Hospital	43	1	
10	**Integridad**	**34,00**	**10,00**	**0,23**
	La auditoría se considera una acción complementaria necesaria para mejorar la seguridad Iniciativas en el Hospital	35	9	
	En el Hospital, las políticas y procedimientos de seguridad son revisados periódicamente	33	11	
11	**Procedimientos adecuados**	**36,00**	**8,00**	**0,18**
	Hay un liderazgo visible sobre la seriedad de los esfuerzos de seguridad en el Hospital	38	6	
	La auditoría es vista como una acción complementaria necesaria para mejorar las iniciativas de seguridad en el Hospital	30	14	
	Tengo que leer las políticas de seguridad con frecuencia (trimestral, bi-anual, anual) en el Hospital	40	4	

Realizado por: Ing. Christian Barragán, 2016

De esta forma se puede obtuvo la ponderación siguiendo la misma metodología, para lo cual se obtiene los siguientes datos:

Tabla 5-4 *Ponderación de ocurrencia de riesgos identificados Post-Implementación*

Ítem	Amenazas	Probabilidad	Impacto	Ponderación
1	Divulgación accidental	0,14	4	0,55
2	Empleado curioso.	0,14	4	0,58
3	Violación de la privacidad de los datos por un trabajador.	0,17	4	0,68
4	Intrusión no autorizada en la red del sistema.	0,11	4	0,45
5	Infección de equipos por virus	0,06	1	0,06
6	Perdidas de los sistemas centrales	0,08	3	0,24
7	Sustracción o robo de información	0,08	4	0,33
8	Confidencialidad por exposición al internet	0,11	4	0,45
9	Privacidad por uso de redes compartidas	0,06	3	0,17
10	Integridad	0,23	3	0,68
11	Procedimientos adecuados	0,18	3	0,55

Realizado por: Ing. Christian Barragán, 2016

Gráficamente se observa en la siguiente ilustración la tendencia de la ponderación de los riesgos luego de la implementación de la adaptación de las normas estudiadas.

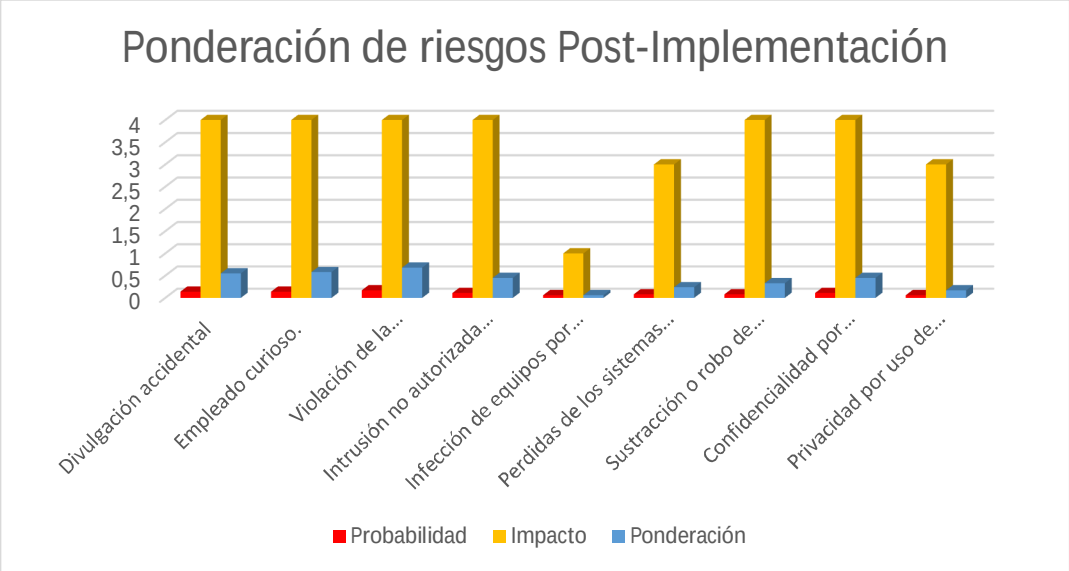

Gráfico 2-4 *Ponderación de riesgos Post-Implementación*

Realizado por: Ing. Christian Barragán, 2017.

Como nos podemos dar cuenta en el gráfico antes descrito ha mejorado sustancialmente la ponderación de los riesgos estudiados.

En base a este análisis se puede establecer que los riesgos de ponderación superior a los 2.5 que se establecieron en el estudio inicial han disminuido notablemente:

Tabla 6-4 *Riesgos de mayor prevalencia Post-Implementación*

Ítem	Amenazas	Ponderación Inicial	Ponderación Post-Implementación
2	Empleado curioso.	3,42	0,58
3	Violación de la privacidad de los datos por un trabajador.	3,18	0,55
8	Confidencialidad por exposición al internet	3,05	0,45
10	Integridad	2,93	0,68
1	Divulgación accidental	2,73	0,55

Realizado por: Ing. Christian Barragán, 2016

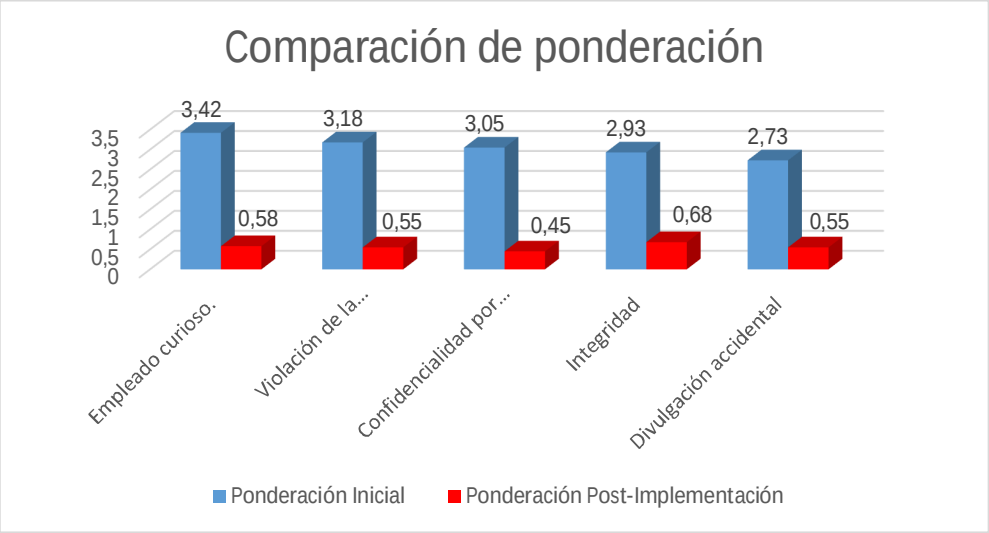

Gráfico 3-4 *Comparación de ponderación Post-Implementación*

Realizado por: Ing. Christian Barragán, 2017.

La misma tabla puede ser expresada en función de porcentaje tomando en consideración que el máximo valor de ponderación podría ser el valor de cuatro (4) lo que significa que el riesgo se produce con frecuencia.

Tabla 7-4 *Porcentaje de reducción de riesgos*

Item	Amenazas	Porcentaje Ponderación Inicial	Porcentaje Ponderación Post-Implementación	Porcentaje de reducción de riesgo
2	Empleado curioso.	85,61%	14,39%	71,21%
3	Violación de la privacidad de los datos por un trabajador.	79,55%	17,05%	62,50%
8	Confidencialidad por exposición al internet	76,14%	11,36%	64,77%
10	Integridad	73,30%	17,05%	56,25%
1	Divulgación accidental	68,18%	13,64%	54,55%

Realizado por: Ing. Christian Barragán, 2016

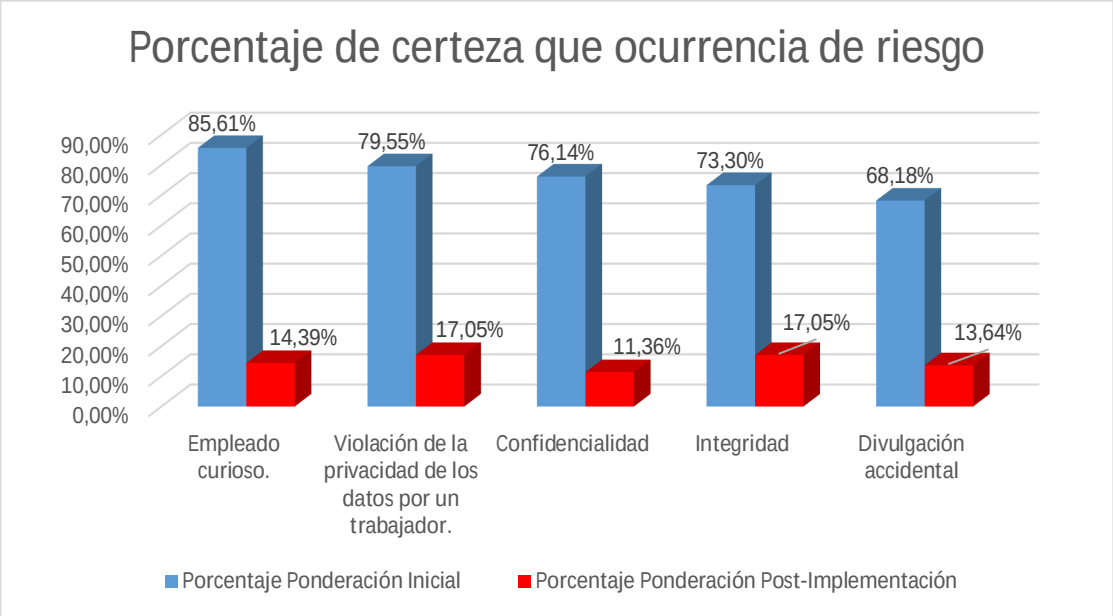

Gráfico 4-1 *Comparación de ponderación de riesgos expresado en porcentaje.*

Realizado por: Ing. Christian Barragán, 2017.

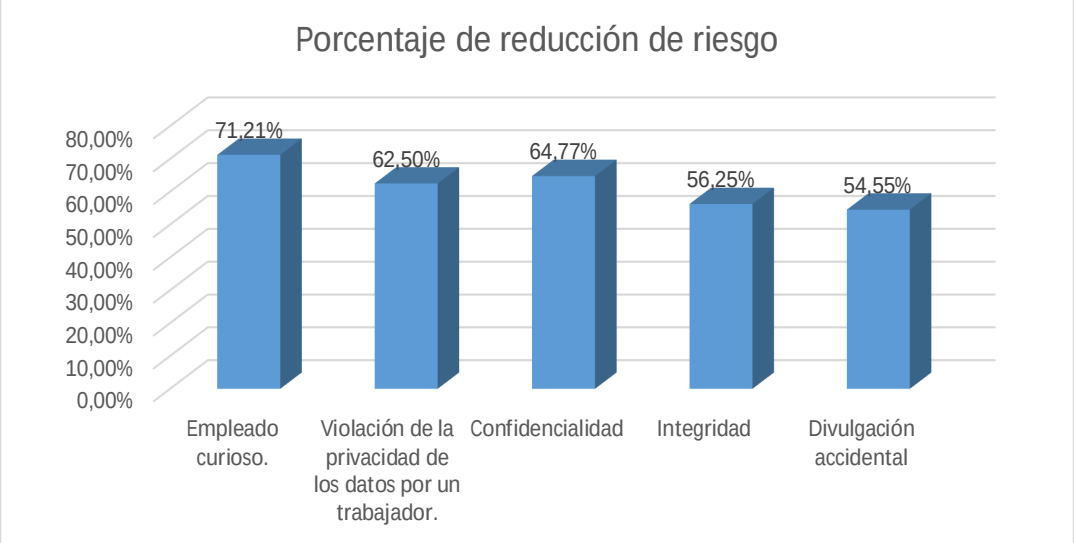

Gráfico 5-4 *Porcentaje de reducción de riesgos*

Realizado por: Ing. Christian Barragán, 2017.

Como se observa claramente en la ilustración del Porcentaje de reducción de riesgos, las ponderaciones tomadas como las de mayor prevalencia en el análisis inicial, luego de haber aplicado el modelo generado con las políticas solicitadas, se ha reducido sustancialmente la

ponderación de la probabilidad de que los riesgos en un sesenta y un punto 86 por ciento (61,86%) como promedio, frente a la situación inicial.

4.3. Comprobación de Hipótesis.

Las hipótesis científicas o de investigación son sometidas a prueba para determinar si son apoyadas o refutadas de acuerdo con los resultados obtenidos argumentando que fue apoyada o no puesto que no podemos probar que una hipótesis sea verdadera o falsa.

Existen pruebas estadísticas que permiten determinar algunos límites de confianza, una de estas es la prueba T de Student que es cualquier prueba en la que el estadístico utilizado tiene una distribución T de Student si la hipótesis nula es cierta. Se aplica cuando la población estudiada sigue una distribución normal pero el tamaño de la muestra es demasiado pequeño como para que el estadístico en el que está basada la inferencia esté normalmente distribuido, utilizándose una estimación de la desviación típica en lugar del valor real.

4.3.1. Hipótesis de investigación (Hi):

La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS.

4.3.2. Hipótesis de Nula (H0):

La Adaptación de las Normas ISO 27001 e HIPAA no permitirá la reducción de riesgos de seguridad de la información en el Hospital Nivel I del IESS Guaranda.

$$H_o: \mu_{\bar{d}} = 0$$

4.3.3. Hipótesis Alternativa (H1):

La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos de seguridad de la información en el Hospital Nivel I del IESS Guaranda.

$$H_1: \mu_{\bar{d}} \neq 0$$

Donde $\mu_{\bar{d}}$ es la media de las medidas.

4.3.4. Nivel de significancia

Se debe elegir un nivel de significancia para la prueba que permite juzgar si los resultados de la prueba son estadísticamente significativos y también determina la probabilidad de error que es inherente a la prueba.

Para nuestra investigación se establece un nivel de significancia (denotado como α o alfa) de 0.05. Un nivel de significancia de 0.05 indica un riesgo de 5% de concluir que existe una diferencia cuando no hay una diferencia real.

$$\alpha = 0.05$$

4.3.5. Definir estadístico de prueba

En función de los datos obtenidos durante la investigación se define que utilizamos la distribución T de Student para muestras pareadas, donde se establece que:

$$t_c = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}$$

$$S_d = \sqrt{\frac{\sum_{i=1}^{n}(d - \bar{d})^2}{n - 1}}$$

Donde:

t_c = valor estadístico del procedimiento calculado.

$\bar{d}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después.

S_d = desviación estándar de las diferencias entre los momentos antes y después.

n = tamaño de la muestra.

4.3.6. Regla de decisión

Caso 1.

$$t_c > t_\alpha, rechaza\ la\ hipotesis\ nula\ H_0$$

Caso 2.

$$Valor\ p < \alpha, se\ rechaza\ la\ hipotesis\ nula\ H_0$$

4.3.7. Análisis

Los datos obtenidos en la investigación fueron evaluados en el software SPSS que permite de forma automática ejecutar las formulas antes descritas, obteniendo los siguientes resultados:

Normalidad

Para la prueba de Normalidad en la que se debe aceptar la hipótesis nula y se consideran todas las categorías de riesgos ponderadas según la siguiente tabla:

Tabla 8-4 *Datos de respuestas Probabilidad de ocurrencia de riesgos identificados Post-Implementación*

Item	Amenazas	Inicial	POST
1	Divulgación accidental	2,73	0,55
2	Empleado curioso.	3,42	0,58
3	Violación de la privacidad de los datos por un trabajador.	3,18	0,68
4	Intrusión no autorizada en la red del sistema.	2,32	0,45
5	Infección de equipos por virus	0,18	0,06
6	Perdidas de los sistemas centrales	0,41	0,24
7	Sustracción o robo de información	1,97	0,33
8	Confidencialidad	3,05	0,45
9	Privacidad	1,50	0,17
10	Integridad	2,93	0,68
11	Procedimientos adecuados	2,25	0,55

Realizado por: Ing. Christian Barragán, 2016

Al analizar los datos obtenidos en la tabla mencionada en el software SPSS se obtuvieron los siguientes resultados:

Descriptivos

			Estadístico	Error estándar
INICIAL_TOT	Media		2,1764	,32785
	95% de intervalo de confianza para la media	Límite inferior	1,4459	
		Límite superior	2,9069	
	Media recortada al 5%		2,2182	
	Mediana		2,3200	
	Varianza		1,182	
	Desviación estándar		1,08735	
	Mínimo		,18	
	Máximo		3,42	
	Rango		3,24	
	Rango intercuartil		1,55	
	Asimetría		-,911	,661
	Curtosis		-,201	1,279
POST_TOT	Media		,4309	,06235
	95% de intervalo de confianza para la media	Límite inferior	,2920	
		Límite superior	,5698	
	Media recortada al 5%		,4377	
	Mediana		,4500	
	Varianza		,043	
	Desviación estándar		,20681	
	Mínimo		,06	
	Máximo		,68	
	Rango		,62	
	Rango intercuartil		,34	
	Asimetría		-,541	,661
	Curtosis		-,800	1,279

Gráfico 6-4 *Tabla de Descritivos de la Normalidad*

Realizado por: Ing. Christian Barragán, 2017.

Nota.- En promedio de los riesgos de amenazas inicial es 2.17 mayor que los riesgos de amenaza post implementación igual 0.43; además las amenazas de riesgo inicial presenta una variabilidad de 1.08 la cual es mayor que la variabilidad de la amenaza post implementación igual a 0.20.

Ahora analizamos la prueba de normalidad dada la distribución de Kolmorogov-Smirnov y Shapiro-Wilk obtenida del SPSS:

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
INICIAL_TOT	,163	11	,200*	,896	11	,163
POST_TOT	,173	11	,200*	,933	11	,440

*. Esto es un límite inferior de la significación verdadera.

a. Esto es un límite inferior de la significación verdadera.

Gráfico 7-4 *Normalidad distribución de Kolmorogov-Smirnov y Shapiro-Wilk*

Realizado por: Ing. Christian Barragán, 2017.

Nota.- Dada las pruebas de normalidad de Kolmorogov-Smirnov y Shapiro-Wilk se obtiene un valor p igual a 0.200, 0.163 para los riesgos de amenaza inicial y 0.200, 0.446 para los riesgos de amenaza post implementación los cuales son mayores que el valor de α igual a 0.05 por lo que se acepta la hipótesis nula H_0. Concluyéndose que los resultados de amenaza inicial y post implementación se aproximan a una distribución normal.

Distribución T de Student (se debe rechazar la H0)

Una vez que hemos demostrado que los datos obtenidos se aproximan a una distribución normal podemos hacer el análisis de la distribución T de Student para datos pareados, para lo cual se estableció en la ponderación de los datos que los riesgos cuya ponderación sea superior a los 2.5 puntos son los riesgos más críticos y a los que más atención se debe prestar, y es por eso que se considera únicamente para el análisis los datos establecidos en la tabla de los Riesgos de mayor prevalencia Post-Implementación ya definida, de la cual se obtiene lo siguiente:

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	INICIAL_CRITICO	3,0950	4	,28758	,14379
	POST_CRITICO	,5325	4	,05679	,02839

Gráfico 8-4 *Estadísticas de muestras emparejadas*

Realizado por: Ing. Christian Barragán, 2017.

Al identificar los riesgos más críticos para la amenaza inicial y post implementación se obtiene un valor promedio de 3.09 y 0.53 respectivamente, los cuales presentan una variabilidad para las amenazas más críticas inicial tomando un valor de 0.28 y riesgos de amenaza critica post implementación menor de 0.056

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	INICIAL_CRITICO - POST_CRITICO	2,5625	,27645	,13823	2,12261	3,00239	18,539	3	,000

Gráfico 9-4 *Pruebas de muestras emparejadas*

Realizado por: Ing. Christian Barragán, 2017.

Nota.- dada la prueba para muestras pareadas de T de Student se obtiene un valor promedio de 2.56 y una desviación estándar de 0.27, además se obtiene un valor de p igual a 0.000343 el cual es menor al valor determinado para α de 0.05 por lo que nos lleva a rechazar la hipótesis nula H0 y aceptar la alternativa H1. Concluyéndose que la diferencia de medias de los riesgos de amenaza inicial y los riesgos de amenaza post implementación, son significativamente diferentes con un nivel de confianza del 95%.

Tomando en consideración todos y cada uno de los cálculos anteriores se presenta esta propuesta de implementar el modelo de adaptación de las Normas ISO 27001e HIPAA las mismas que permitirán la reducción de riesgos de seguridad de la información en Hospitales Nivel I del IESS, puesto que se obtuvieron resultados favorables dentro del Hospital Nivel 1 del IESS Guaranda "Dr. Humberto del Pozo".

CAPITULO V

5. PROPUESTA: MODELO DE LA ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPAA.

NORMA DE SEGURIDAD HOSPITALARIA IESS

1. Alcance

El alcance de esta norma está establecida para los Hospitales de Nivel 1 del IESS (homologados como Hospitales Básicos ante el Ministerio de Salud Pública) quienes generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada buscando asegurar la información de salud perteneciente a los afiliados del Instituto Ecuatoriano de Seguridad Social y que se encuentra registrada en las Historias Clínicas en el sistema MIS-AS400.

A este tipo de Hospitales también se los referirá como unidad médica, hospital o nosocomio.

2. Organización de la Seguridad de la Información

Los Hospitales de Nivel 1 del IESS deben formar un comité de coordinación de la seguridad de la información que deberá convocarse de forma periódica o cuando las circunstancias lo ameriten, debiendo llevar un registro documentado de:

- Compromiso del Director Administrativo del Hospital con la seguridad de la información.
- Nombrar y establecer las responsabilidades de la Coordinación de la Gestión de la Seguridad de la Información.
- Asignación de responsabilidades para la seguridad de la información para cada uno de los puestos del Hospital incluyendo a los servicios contratados, si los hubieren.
- Proceso de autorización para nuevos servicios de procesamiento de la información.
- Acuerdos de Confidencialidad.
- Revisión independiente de la seguridad de la información
- Identificación de los riesgos relacionados con las partes externas
- Consideraciones de la seguridad cuando se trata con ciudadanos o clientes
- Consideraciones de la seguridad en los acuerdos con terceras partes

3. Gestión de los Activos

El activo primordial definido y especificado esta norma son los datos clínicos pertenecientes a los afiliados que han recibido una prestación de salud en las Unidades médicas del IESS, además de

los activos de soporte Hardware, Software y de Redes presentes en los nosocomios de Nivel 1 del IESS especialmente los sistemas locales de los servicios auxiliares del Hospital.

4. Seguridad de los Recursos Humanos

Las unidades médicas que están bajo esta norma deben definir y documentar claramente las Funciones y responsabilidades, forma de selección, términos y condiciones laborales, sensibilización en seguridad de la información, proceso disciplinario, responsabilidades de terminación del contrato, devolución de activos y el retiro de los privilegios de acceso cualquier sistema de información que el funcionario del nosocomio tenga.

La forma de documentación debe ser realizada utilizando los formularios establecidos a nivel central por la Dirección Nacional de Talento Humano, tales y como los documentos del proceso de vinculación de personal, formulario de Paz y Salvo para la desvinculación del funcionario, etc.

5. Seguridad Física y del Entorno

Las unidades médicas deben manejar un perímetro de seguridad física estableciendo documentación de soporte y verificación para:

- Mecanismos de control de acceso a oficinas y áreas críticas como el Laboratorio Clínico, Imagen, Data Center, Emergencia, Hospitalización, Archivo, Farmacia, Grupo Electrógeno.
- Protección contra amenazas externas y ambientales.
- Servicios de suministro.
- Mantenimiento de los equipos.
- Seguridad en la reutilización o eliminación de equipos tecnológicos.

6. Gestión de Comunicaciones y Operaciones

Se establece registros documentados de los procedimientos de funcionamiento normal del activo principal del Hospital, considerándose:

- Distribución de funciones
- Capacitación y Producción
- Monitoreo y revisión de los servicios, por terceros.
- Aceptación del Sistema.
- Controles contra código malicioso.
- Respaldo de la información.
- Seguridad de los servicios de la red.
- Procedimientos para el manejo de la información.

- Políticas y procedimientos para el intercambio de información.
- Registros de auditorías.
- Monitoreo de uso del sistema.
- Registro de fallas.

7. Control de Acceso

Se establece una Política de control de acceso y registro de usuarios mediante una gestión de perfiles y contraseñas para usuarios para el sistema MIS-AS400 como principal repositorio de información de la Historia Clínica como principal activo del Hospital, tomando como política la:

- Revisión de los derechos de acceso de los usuarios.
- Uso de contraseñas.
- Bloqueo de pantalla para equipos de usuario desatendido.
- Política de puesto de trabajo despejado y pantalla limpia.
- Política de uso de los servicios de red.
- Identificación de los equipos en las redes.
- Separación en las redes.
- Procedimiento de registro de inicio seguro.
- Control de acceso a las aplicaciones y a la información.

8. Gestión de los incidentes de la Seguridad de la Información

Se establece procedimientos formales para la elaboración de Reporte sobre los eventos de seguridad de la información emitiéndose Reportes sobre:

- Debilidades en la seguridad
- Responsabilidades y procedimientos
- Aprendizaje debido a los incidentes de seguridad de la información
- Recolección de evidencias.

9. Gestión de la continuidad

Las unidades médicas están obligadas a asegurar la disponibilidad de recursos de los sistemas de información con una evaluación de los riesgos que permitan el desarrollo e implementación de planes de continuidad o contingencia.

10. Cumplimiento

Es de complimiento obligatorio que todo el personal de las Unidades Médicas cumplan a cabalidad Legislación vigente que asegura la protección de registros o datos y privacidad de la

información personal, con una prevención del uso inadecuado de servicios de procesamiento tecnológico de información, según lo dispuesto en el Reglamento de Información Confidencial del Sistema Nacional de Salud, mediante el cual se establece la obligatoriedad de contar con un sistema adecuado de custodia digital y física de los datos pertenecientes a la esfera de la intimidad de las personas, y sus datos de carácter confidencial contenidos en el Sistema MIS o demás documentación clínica, en concordancia con el Art. 66, numeral 9 de la Constitución de la República; Art. 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, Art. 4 de la Ley de Derechos y Amparo del Paciente y el Art. 178 del Código Orgánico Integral Penal vigente, mediante el:

- Cumplimiento con las políticas y las normas de la seguridad.
- Verificación del cumplimiento técnico.
- Controles de auditoría de los sistemas de información.
- Protección de las herramientas de auditoría de los sistemas de información.

5.1. Guía de buenas prácticas de seguridad informática para el personal de atención primaria.

En la siguiente tabla se presenta la guía de buenas prácticas informáticas obtenida de las recomendaciones, normas y estándares revisados, dividida en bloques según la temática que abarca. La guía está orientada tanto al personal sanitario como al no sanitario, siempre y cuando empleen un ordenador con acceso a datos personales del paciente. La tercera columna indica la amenaza que previene cada recomendación, atendiendo a la clasificación presentada en la tabla 2 de este estudio. En la última columna se indica la fuente de la que se ha extraído la recomendación en base a la numeración dada en la tabla de Estándares, normas y recomendaciones de seguridad para el ámbito de los centros de atención primaria. En las siguientes líneas se justifica cada bloque y se ofrecen recomendaciones prácticas para los profesionales.

Tabla 1-5 *Guía de buenas prácticas para la seguridad informática en centros de salud.*

Bloque	Recomendación	Amenaza Prevenida	Estándares, normas y recomendaciones
Formación	Se debe conocer y aplicar la política de seguridad de la organización sanitaria que debe estar definida según lo dispuesto en el artículo 11 del Esquema Nacional de Seguridad Nivel	Nivel 1, 4, 5	1,2,16,20,22
Fortaleza contraseñas	La contraseña se debe modificar cada 40días	Nivel 1, 2, 4, 5	11,16
	La contraseña debe estar compuesta por 8 dígitos como mínimo	Nivel 1, 2, 4, 5	4, 11, 15, 16

	Componerla de letras mayúsculas y minúsculas, algún número y algún carácter especial.	Nivel 1, 2, 4, 5	1, 4, 11, 15, 16
	La contraseña no debe constar de fechas, nombres o información personal	Nivel 1, 2, 4, 5	1, 4, 11, 15, 16
	La contraseña no debe apuntarse en ningún sitio ni enviarla por correo electrónico	Nivel 1, 2, 4, 5	1, 4, 11, 15, 16
	La contraseña debe ser diferente de la que protege cuentas de carácter personal.	Nivel 1, 2, 4, 5	1, 4, 11, 15, 16
	No compartir la contraseña con nadie ni solicitar la de otro compañero	Nivel 1, 2, 3, 4, 5	1, 4, 11, 15, 16,22
	No guardar la contraseña en el navegador de internet	Nivel 1, 2, 3, 4, 5	1, 4, 11, 15, 16,22
Uso de certificados digitales	Los certificados digitales deben protegerse con contraseña y aplicarle a esta las mismas del bloque anterior	Nivel 1, 2, 3, 4, 5	20,22
Uso del correo electrónico	No consultar cuentas de correo personal desde el centro sanitario por ser una posible entrada de virus y fuga de información.	Nivel 1, 3, 5	1,22
	No enviar desde cuentas de correo personal información persona de salud, ni proporcionar la dirección para recibir este tipo de datos.	Nivel 1, 3, 5	1,22
	No utilizar su cuenta de correo electrónico corporativa para fines personales, y extremar las medidas de seguridad si va a acceder a ella desde un domicilio particular	Nivel 1, 3, 5	1, 9,22
	No responder a correos electrónicos que le soliciten la remisión de datos de salud	Nivel 1, 2, 3, 5	1, 9, 16,22
	Extremar la precaución, al abrir adjuntos de un correo electrónico para no introducir virus en el centro.	Nivel 1, 5	1, 9, 16,22
	Encriptar o codificar los correos electrónicos que contengan datos personales de salud	Nivel 1, 2, 5	1, 2, 9, 16,22
	Incluir en el pie de los faxes y correos electrónicos enviados una cláusula informando de la naturaleza y privacidad de los datos	Nivel 1	1, 2, 9, 16,22
Acceso a Internet	Evitar navegar por: redes sociales, páginas de descargas, páginas de almacenamiento de archivos, mensajería instantánea y juegos online por ser entrada potencial de amenazas.	Nivel 1,3, 5	1, 16,22
	Precaución en la descarga de archivos de internet	Nivel 1,2, 5	1, 16,22
Uso de dispositivos y medios extraíbles	Consultar con el responsable de la información la conveniencia o no de sacar información personal de salud del centro en un medio extraíble	Nivel 1,3, 4, 5	1, 6, 16, 19,22
	Encriptar o codificar la información personal de salud que salga del centro en medios extraíbles o dispositivos portátiles	Nivel 1,3, 4, 5	2, 10, 16, 19,22

	Precaución en el uso de medios extraíbles (USB, CD, etc.) para evitar la entrada de virus	Nivel 1,3, 5	1, 16, 19,22
	Borrado seguro de medios extraíbles con información personal de salud al desecharse para evitar que puede recuperarse	Nivel 1,3, 4, 5	1, 2, 10, 16, 19, 22
Uso de equipos	Cerrar la sesión, bloquearla o apagar la pantalla del ordenador cuando vaya a ausentarse del mismo durante 5 minutos o más	Nivel 1, 2, 3, 4, 5	1,2,7,16,22
	Evitar que los datos desplegados en pantallas sean vistos por personas no autorizadas	Nivel 1, 2, 3, 4, 5	1,2,16,22
	No colocar información sensible en unidades del ordenador compartidas con trabajadores que no tengan autorización a acceder a dichos datos	Nivel 1, 2, 3, 4, 5	1, 22
	Acceder únicamente a la información indispensable para desempeñar el trabajo. Si se accede a información que no deba ser vista, se debe informar al departamento de informática del centro	Nivel 1, 2, 3, 4, 5	1,16, 22
	Borrar la memoria de las fotocopiadoras de alta capacidad del centro tras fotocopiar información que contenga datos personales de salud.	Nivel 1, 2, 3, 4, 5	1, 22
	Retirar los documentos con datos sensibles de la bandeja de impresión de las impresoras y faxes para que no puedan ser consultados por personal no autorizado.	Nivel 1, 2, 3, 4, 5	1,7,16, 22
Instalación de software	No instalar software no relacionado con las funciones del puesto de trabajo por ser una posible entrada de amenazas	Nivel 1, 3, 5	7,16
	Cuidar que el software a instalar esté libre de virus	Nivel 1, 3, 5	1,16
Incidencias de seguridad	Conocer el protocolo de actuación frente a la detección de amenazas informáticas	Nivel 1, 2, 3, 4, 5	1,16
	Informar de cualquier anomalía en el funcionamiento del ordenador a quien corresponda según el procedimiento que debe ser definido por la organización para la notificación de incidencias	Nivel 1, 2, 3, 4, 5	1,16

Fuente: (Sánchez-Henarejos et al., 2014), Modificado por Christian Barragán

5.2. POLITICAS QUE REGULAN ACTIVIDADES RELACIONADAS USO DE TECNOLOGIAS

5.2.1. GENERALIDADES

PLT. 1.- Finalidad.- Las Políticas de Tecnología de la Información y Comunicación tienen como finalidad el proteger la información, a la Institución y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la Institución.

PLT. 2.- Ámbito.- Las Políticas de Tecnología de la Información y Comunicación serán aplicadas de manera obligatoria por las y los funcionarios, servidores y trabajadores que integran el IESS a nivel nacional, que utilicen el hardware, software y comunicaciones, para el cumplimiento de sus actividades diarias.

La Dirección Nacional de Tecnología de la Información será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su cargo el uso de recursos tecnológicos de forma desconcentrada.

PLT. 3.- Recursos Tecnológicos.- Las Políticas de Tecnología de la Información regularán y estandarizarán el uso de los recursos informáticos que el IESS pone a disposición de todo el personal para desarrollar sus actividades y cumplir con la misión de la Institución. Anexo B.

PLT. 4.- Términos.- Se definen los siguientes términos:

1. TECNOLOGIAS DE INFORMACION Y COMUNICACIONES.- Equipo de cómputo personal y centralizado, software y dispositivos de impresión que serán utilizadas para almacenar, procesar, convertir, proteger, transferir y recuperar: información, datos, voz, imágenes y video.
2. DOS.- Denegación de Servicios, por sus siglas en Inglés (Denial of services).
3. SOFTWARE (DE APLICACION).- Componentes lógicos (intangibles) de un computador. Programas de computadora que sirven para interactuar y controlar el sistema operativo, proporcionando control sobre el hardware y dando soporte a otros programas. Es una herramienta que realiza tareas de mantenimiento, soporte para la construcción y ejecución de programas.
4. HARDWARE.- Componente físico de un computador y dispositivos externos.
5. INFORMACION.- Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
6. USUARIOS.- Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

7. SEGURIDAD INFORMATICA.- Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.
8. INTEGRIDAD.- Se refiere a la corrección y complementación de los datos en una base de datos.
9. CONFIDENCIALIDAD.- La información solo debe accesible únicamente a personal autorizado.
10. DISPONIBILIDAD.- Debe estar disponible cuando se necesita, es decir, accesible.
11. IRREFUTABILIDAD (No repudio).- El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que usuario no puede negar dicha acción.
12. AREA INFORMATICA.- Es el lugar donde se lleva a cabo el procesamiento de información (programación, análisis y diseño de sistemas de información, ingreso de datos, procesos de back-ups, etc.).
13. AMENAZA.- Es un evento que pueden desencadenar en un incidente en el organismo, produciendo daños materiales o pérdidas inmateriales en sus activos.
14. IMPACTO.- Medir la consecuencia al materializarse una amenaza.
15. VULNERABILIDAD.- Posibilidad de ocurrencia que mediante una exploración se viole la seguridad del sistema.
16. ATAQUE.- Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
17. BACKUP.- Respaldo de información.
18. PASSWORDS.- Clave que se le asigna a los usuarios.
19. FILESYSTEMS.- Punto de montaje de sistemas UNIX.
20. RETENCION.- Tiempo que vigencia de un respaldo.
21. DIRECCION MAC- Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.
22. DIRECCION IP- Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, Tablet, Laptop, Smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.
23. PC- Computador personal.
24. CD.- Disco compacto para almacenar información.
25. URL.- Dirección web.
26. TI.- Tecnologías de la Información.
27. SHAREWARE.- Modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales.
28. FREEWARE.- Tipo de software que se distribuye sin costo, disponible para su uso y por tiempo ilimitado.
29. QA.- Equipo de trabajo de Control de Calidad perteneciente a la Dirección Nacional de Tecnología.

5.2.2. POLITICA PARA EL USO ADECUADO DE LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

PLT. 5.- Generales.- Los usuarios internos para el uso adecuado de los recursos tecnológicos tomarán en cuenta lo siguiente:

1. Para el hardware (equipos, impresoras, escáneres, servidores y demás recursos tecnológicos) de propiedad del IESS, de conformidad con el Reglamento Orgánico del Instituto Ecuatoriano de Seguridad Social, la Dirección Nacional de Tecnología de la Información es la única autorizada para realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipo de cómputo con ayuda del personal técnico en situ previa coordinación con la Dirección Nacional de Tecnología de la Información. En el caso de actividades de mantenimiento efectuadas por terceros, éstas serán previamente aprobadas por la Dirección Nacional de Tecnología de la Información.
2. En caso de equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada a realizar las labores de mantenimiento y cambio de hardware o en su caso autorizar dichas labores, previa coordinación con la Dirección Nacional de Tecnología de la Información o la Subdirección Provincial de Apoyo a la Gestión Estratégica en cada provincia.
3. El acceso al área de infraestructura informática es restringido y únicamente ingresará personal autorizado.
4. Se restringirá el acceso a los equipos tecnológicos, a aquellos usuarios que no cuenten con una autorización previa de su superior inmediato para laborar fuera de horario.
5. La información de trabajo se almacenará en los discos de red asignados por usuario, garantizando así la integridad de la información.
6. Las y los usuarios autorizados de los sistemas informáticos del IESS, no harán uso indebido, suministro, manejo, de la información institucional, datos en general y datos considerados como confidenciales.
7. Las bases de datos de la Institución estarán centralizadas en el Data Center de la Dirección Nacional de Tecnología de la Información, de existir bases de datos aisladas o no compatibles con la infraestructura tecnológica se implementarán proyectos de integración y/o migración de aplicativos y base de datos a cargo de la Dirección Nacional de Tecnología de la Información con participación de las unidades de negocio involucradas.
8. Los sistemas de información desarrollados internamente o adquiridos a terceros, estarán instalados en la infraestructura disponible en la Dirección Nacional de Tecnología de la Información (licenciamiento, software, código fuente, hardware,).
9. Previo al acceso a las bases de datos del IESS, se contará con la autorización de las Unidades de Negocio y la definición del tipo de acceso a otorgarse.
10. La entrega de información a entidades externas gubernamentales o privadas, contará con la autorización de las unidades de negocio dueñas de la información.
11. De no especificar permisos a direcciones web o a direcciones específicas, se proporcionará acceso solamente a la página web institucional y a su intranet.
12. La identidad de los usuarios externos y los derechos de acceso otorgados, se mantendrán en un repositorio central, en un documento que contenga al menos los siguientes campos como: nombres y apellidos, número de cédula de ciudadanía/identidad, empresa o entidad en la que labora, nombre del proyecto, nombre del responsable del proyecto, fecha de solicitud de los

permisos, fecha de expiración de los permisos, sitios a los que se otorgó el acceso, dirección IP de la máquina desde donde se realiza el acceso, dirección MAC de la máquina desde donde se realiza el acceso, nombre de la persona que autoriza el acceso y de la persona que otorga el acceso, notas.

13. Se prohíbe a los usuarios utilizar los permisos otorgados para fines distintos a los especificados en la solicitud de acceso, así como también se prohíbe el intercambio de direcciones IP con otros usuarios que no consten en la solicitud.
14. En caso de que el usuario tenga la sospecha que sus accesos han sido comprometidos, solicitará inmediatamente su bloqueo a la Dirección Nacional de Tecnología de la Información o a la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel provincial.
15. Para el caso de conexiones inalámbricas, por defecto se otorgará un acceso a la red pública de la Institución. Si se especifican accesos puntuales, se otorgará acceso a una red específica de acuerdo a sus necesidades.
16. Se mantendrá un inventario actualizado de los recursos tecnológicos.
17. Todos los computadores de las unidades administrativas y médicas del IESS a nivel nacional, se sujetarán a la versión del software antivirus institucional, que determine la Dirección Nacional de Tecnología de la Información. Este software tendrá activada la protección en tiempo real al sistema operativo y mantendrá instalada la última definición de virus o una que haya estado vigente en los últimos 15 días. La actualización de las definiciones de antivirus se realizará de manera automática. Si por alguna razón no se dispone del servicio de actualización automática, se las instalará manualmente, si fuera el caso.
18. Bajo ninguna circunstancia las y los funcionarios/as, servidores/as y trabajadores/as de la Institución, podrán utilizar los recursos informáticos para realizar actividades prohibidas por las políticas establecidas o por las disposiciones jurídicas nacionales o internacionales.

PLT. 6.- Hardware.- El hardware de propiedad del IESS o arrendado, se utilizará únicamente para actividades relacionadas con los objetivos y metas de la Institución, para lo cual se observará lo siguiente:

1. Para el correcto funcionamiento del hardware se realizará mantenimiento preventivo, de acuerdo al plan de mantenimiento preventivo del equipo de cómputo anual, elaborado por los técnicos informáticos de cada dependencia, mismo que deberá ser notificado al titular de la Dirección Nacional de Tecnología de la Información a principio de cada ejercicio.
2. La Dirección Nacional de Adquisiciones, Bienes y Servicios en coordinación con la Dirección Nacional de Tecnología de la Información es la responsable de la asignación y distribución del hardware institucional. A nivel provincial serán las Subdirecciones Provinciales de Apoyo a la Gestión Estratégica y de Servicios Corporativos, o las áreas que hagan sus veces.
3. La adquisición de bienes tecnológicos y la contratación de servicios de soporte técnico y/o mantenimiento se llevarán a cabo de acuerdo con los lineamientos, especificaciones técnicas que emita la Dirección Nacional de Tecnología de la Información a nivel nacional, basándose en la necesidad institucional y en la normativa vigente sobre la materia.
4. Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa al hardware del IESS, se notificará de inmediato a la Dirección Nacional de Adquisiciones, Bienes y Servicios, a nivel provincial a la Subdirección Provincial de Apoyo a la Gestión Estratégica o, al área que haga sus veces.

5. Solamente el personal del IESS autorizado por la Dirección Nacional de Tecnología de la Información o Subdirección Provincial de Apoyo a la Gestión Estratégica en las provincias, está facultado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad institucional, que NO cuenten con la garantía técnica vigente.

Para los equipos cuya garantía técnica aún se encuentre vigente, lo efectuará únicamente el personal técnico calificado de la Contratista, previa coordinación con la o el Administrador de Contrato designado.

Para los equipos de cómputo en esquema de arrendamiento, la empresa arrendadora es la única autorizada para abrir los gabinetes de dichos equipos o en su caso consentirá la apertura de ellos, previa coordinación con la o el Administrador de Contrato del IESS.

PLT. 7.- Centro de Cómputo.- En el Centro de Cómputo del IESS se alojarán los servidores y equipos de comunicaciones necesarias para la operación de las actividades informáticas de la Institución y se observará lo siguiente:

1. El acceso a los centros de cómputo institucionales es restringido y sólo personal autorizado por la Dirección Nacional de Tecnología de la Información o la máxima autoridad de la dependencia en donde se encuentran ubicados, puede tener acceso a él.
2. El acceso a los servidores de los centros de cómputo institucionales, ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por la Dirección Nacional de Tecnología de la Información o la máxima autoridad de la dependencia en donde se encuentran ubicados. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de los servidores se considera una violación de las políticas de seguridad.

PLT. 8.- Propiedad de la información.- Las y los usuarios de cualquier equipo de cómputo del IESS deben estar informados y conocer que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son de propiedad y responsabilidad del IESS, para lo cual se respetará lo siguiente:

1. Los derechos patrimoniales de un programa de computación, hojas de cálculo, archivos de Word, macros, etc., y su documentación, creados por uno o varios empleados en el ejercicio de sus actividades laborales corresponden al IESS.
2. Los respaldos que contengan información del IESS y que fueron realizados o solicitados por el usuario del equipo de cómputo, se tendrán exclusivamente bajo resguardo, debiendo entregarlos al jefe inmediato al finalizar su relación laboral con la institución, mediante la respectiva acta de entrega recepción.

PLT. 9.- Usos inadecuados.- Las siguientes actividades están prohibidas:

1. Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuada adquirida por el IESS (Políticas de Uso de Software).
2. Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información. Anexo C.
3. Introducir software malicioso en la red o en los servidores (virus, gusanos, troyanos, ráfagas de correo electrónico no solicitado, etc.).
4. Utilizar la infraestructura de tecnología de información del IESS para conseguir o transmitir material con ánimo de lucro.
5. Utilizar el sistema de comunicaciones del IESS con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
6. Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios del IESS.
7. Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
8. Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal de la Dirección Nacional de Tecnología de la Información, responsable de la Seguridad Informática puede realizar estas actividades siempre y cuando cuente con la aprobación por parte del Director.
9. Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
10. Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación o, deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).
11. Usar comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).
12. Instalar cualquier tipo de software en los equipos de cómputo del IESS sin la previa autorización de la Dirección Nacional de Tecnología de la Información o la Subdirección Provincial de Apoyo a la Gestión Estratégica.
13. Modificar la configuración del software antivirus, firewall personales o políticas de seguridad en general implantadas en los equipos de cómputo del IESS sin consultar previamente con la Dirección Nacional de Tecnología de la Información o la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel provincial, la que analizará la viabilidad de los cambios solicitados.
14. Queda estrictamente prohibido compartir un repositorio de información con derecho a todos. El área de informática puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas definidas.
15. Reproducir música de cualquier formato que no esté ubicada en el disco duro de la PC del usuario o en CD. No se permite la reproducción de archivos de música si éstos están ubicados en recursos compartidos de la red privada del IESS o en cualquier URL de Internet (aplicable para los usuarios que hacen uso del servicio de Internet).

PLT. 10.- Excepción.- Para propósitos de mantenimiento de la red y de seguridad, por excepción el personal debidamente autorizado, podrá estar exento de seguir algunas de las restricciones anteriores, debido a las responsabilidades bajo su cargo o a eventos programados. Estos privilegios de accesos deberán ser solicitados a la Dirección Nacional de Tecnología de la Información anexando la justificación respectiva, vía correo electrónico y/o de manera escrita.

5.2.3. POLITICA DE CONTRASEÑAS

PLT. 11.- Generales.- El cumplimiento de la política de contraseñas por parte de las y los usuarios internos (funcionarios, servidores y trabajadores) del IESS, es extremadamente importante ya que constituyen la primera línea de defensa para garantizar que el acceso a los aplicativos informáticos sólo sea ejecutado por personal autorizado. Tanto equipos, sistemas y datos utilizan mecanismos de contraseñas para controlar el acceso, como al inicio de sesión en la computadora, ingreso a la red institucional, para utilizar sistemas internos y externos, etc. No existe ninguna tecnología que pueda prevenir el acceso no autorizado a la información si un usuario viola esta política.

PLT. 12.- Administración.- Se acatará lo siguiente:

1. Todos los usuarios internos del IESS requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que tiene asignado y servicios de red como correo electrónico, impresión, archivos compartidos, Intranet, Internet etc.
2. Todas las contraseñas son personales e intransferibles. Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña, quien así lo hiciere debe considerar que sigue siendo el único responsable de las actividades que se realicen con su identificación de usuario y contraseña.
3. Todas las contraseñas del sistema (cuentas de administrador, cuentas de aplicaciones, etc.), se cambiarán con una periodicidad de al menos cada seis meses.
4. Todas las contraseñas del usuario (cuentas de usuario, cuentas de servicios web, etc.) se cambiarán al menos cada seis meses.
5. En caso de que el usuario sospeche que su contraseña ha sido comprometida deberá cambiar su contraseña o solicitar al responsable informático de cada dependencia.
6. En caso de olvido o bloqueo de su contraseña, el usuario deberá coordinar el restablecimiento de la misma con el responsable informático de cada dependencia.
7. Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirá la Dirección Nacional de Tecnología de la Información con el objeto de evitar que los usuarios elijan contraseñas débiles. No se utilizarán contraseñas que resulten obvias, fáciles de adivinar o descubrir, o predecibles para un atacante: (el mismo identificador de usuario, palabras de diccionario, fechas o nombres de personas allegadas, secuencias de números repetidos o consecutivos).
8. Las contraseñas para acceso al correo electrónico deberán ser modificadas por el usuario la primera vez que acceda a su cuenta.
9. Las contraseñas de los sistemas internos contarán con contraseñas independientes de la utilizada para iniciar sesión en la red institucional. La administración funcional, incluyendo creación de usuarios y contraseñas de los sistemas internos serán ejecutadas por la Unidad de Negocio a cargo del mismo.

10. Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única.
11. Los derechos de acceso al correo electrónico, red institucional, servidores de archivos y otros servicios provistos por la Dirección Nacional de Tecnología de la Información, deben ser solicitados por el jefe de la dependencia del usuario y estarán alineados con necesidades de negocio definidas firmadas, con requerimientos de trabajo.
12. Los usuarios internos del IESS, deberán negar la opción de recordar contraseñas que se presentan en los navegadores a fin de evitar la autenticación automática de acceso a los sistemas informáticos que operan en la intranet como en el Internet.
13. Cuando un usuario se desvincule de la Institución o se le asigne un rol diferente para el que tiene permisos de acceso, el Jefe inmediato deberá notificar a la Dirección Nacional de Tecnología de la Información para suspender los usuarios de la red institucional, sistemas especializados, etc. De la misma manera, la Dirección Nacional de Gestión de Talento Humano, reportará de forma mensual a la Dirección Nacional de Tecnología de la Información el listado de traspasos, renuncias, y otros movimientos de personal con el fin de coordinar la cancelación de los derechos de acceso a servicios e información que dispongan dichos usuarios.
14. Las y los funcionarios, servidores y trabajadores, deberán suscribir un compromiso de responsabilidad en seguridad y uso de usuario y claves de acceso a la información de recursos tecnológicos administrados por la Dirección Nacional de Tecnología de la Información.

PLT. 13.- Prohibiciones.- Las actividades que se detallan a continuación están prohibidas:

1. Revelar o compartir su contraseña de cualquier forma.
2. Escribir la contraseña o almacenarla en archivos sin que sean encriptados, comunicarla en el texto de mensajes de correo electrónico, o en cualquier otro medio de comunicación electrónica.
3. Comunicar las contraseñas en conversaciones telefónicas.

5.2.4. POLITICA DE USO DE CORREO ELECTRONICO

PLT. 14.- Lineamientos Generales.- El Correo Electrónico (email) es un recurso que la institución pone a disposición de las y los funcionarios, servidores y demás trabajadores del IESS, como una herramienta de comunicación, colaboración e intercambio de información oficial, se observará lo siguiente:

1. El acceso a estos recursos, estará condicionado a la aceptación de la presente Política de Uso.
2. El acceso a este servicio, se lo realiza por medio de la página web institucional (https://correo.iess.gob.ec), cliente de correo o a través de la intranet.
3. Las comunicaciones institucionales efectuadas por correo electrónico, solo podrán ser realizadas por las cuentas institucionales creadas en la Dirección Nacional de Tecnología de la Información.

4. Las cuentas de correo asignadas a los funcionarios y demás personal de cada área, deberán ser utilizadas sólo para actividades laborales que estén relacionadas con los propósitos y funciones institucionales.
5. Los buzones de correo electrónico, creados para las y los funcionarios, servidores y demás trabajadores del IESS, y toda la información contenida en los mismos, son de exclusiva propiedad de la Institución.
6. La Dirección Nacional de Tecnología de la Información se reserva el derecho para modificar las condiciones de uso establecidas cuando lo considere necesario. También podrá modificar o bloquear servicios relacionados al servicio de correo electrónico cuando sea necesario, por razones administrativas, de mantenimiento, por causas de fuerza mayor o por necesidad institucional.
7. La Dirección Nacional de Tecnología de la Información puede, en cualquier momento, cancelar o inhabilitar la cuenta de cualquier usuario sin previo aviso e incluso eliminar ésta por falta de uso, o bien; si considera que el usuario ha contravenido las reglas aquí mencionadas; en tales casos la Dirección Nacional de Tecnología de la Información no se hace responsable de la información ni de eventuales repercusiones por dicha cancelación o inhabilitación.

PLT. 15.- Tipos de Cuentas.- Son:

1. Cuentas Personales: El personal del IESS, contará con una cuenta de correo, en el servidor de la Institución con capacidad de bandeja asignada, cuya dirección electrónica estará formada por la inicial del nombre, el apellido y la inicial del segundo apellido; salvo sus debidas excepciones (xapellidox@iess.gob.ec).
2. Cuentas Temporales: Estas cuentas se crearán bajo propósitos específicos, que serán detallados en el campo de texto "Notas" al momento de crearla. Además se especificará el tiempo de validez, para que sea borrada una vez que ya no se la necesite. El formato para este tipo de cuenta será el siguiente: proposito@iess.gob.ec.
3. Cuentas Departamentales: Estas cuentas serán creadas, con el objetivo de comunicación a todos los miembros de una determinada dirección o lista de usuarios específica, el formato para este tipo de cuentas será el siguiente: nombredirecciónolista@iess.gob.ec.

PLT. 16.- Responsabilidad.- Son:

1. Los servicios de correo electrónico serán administrados por la Dirección Nacional de Tecnología de la Información y será la responsable de velar por el correcto funcionamiento y operación de dichos servicios.
2. La Dirección Nacional de Gestión de Talento Humano deberá comunicar a la Dirección Nacional de Tecnología de la Información, sobre el personal que haya ingresado a laborar en la Institución, así como el personal que ha dejado de laborar, para la activación o desactivación de las cuentas de correo respectivas.
3. Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.

4. La información transmitida mediante el servicio de correo electrónico, es responsabilidad única y exclusiva de cada usuario. La Dirección Nacional de Tecnología de la Información no garantiza la veracidad, integridad o calidad del contenido de los mensajes enviados mediante este servicio.
5. La cuenta de correo es intransferible, por lo que la información correspondiente al inicio de sesión (usuario, contraseña) no debe proporcionarse a otras personas.
6. La información que se recibe de manera personal y confidencial por correo electrónico, no se puede reenviar a otra persona, sin la autorización del remitente.

PLT. 17.- Gestión del buzón de correo.- El usuario deberá:

1. Velar por que la gestión de la información contenida en su cuenta de correo electrónico sea adecuada. Para lo cual debe revisar periódicamente sus bandejas de correo. En este sentido, se recomienda eliminar los mensajes que no deban conservarse y archivar el resto en la carpeta o subcarpeta apropiada.
2. Respaldar periódicamente la información contenida en su buzón de correo, para lo cual podrán solicitar soporte a la Dirección Nacional de Tecnología de la Información para la gestión de sus respaldos.
3. Resguardar la seguridad del buzón de correo, por lo cual deberán evitar la recepción de correo cuando se desconozca al remitente ya que en ocasiones este puede ser un mensaje con contenido potencialmente peligroso o un virus.

La Dirección Nacional de Tecnología de la Información definirá el espacio y los servicios asignados para cada buzón de correo, de acuerdo a las necesidades institucionales.

PLT. 18.- Uso Inaceptable.- Se considera como mal uso del correo electrónico las siguientes actividades:

1. Utilizar el correo electrónico para actividades comerciales ajenas a la institución.
2. Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo institucional.
3. Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.
4. Enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
5. Utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad del emisor del correo electrónico.
6. Distribuir mensajes con contenidos definidos como inapropiados y/o lesivos que atenten contra la moral o las buenas costumbres. Son considerados contenidos inadecuados todo aquello que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento, lenguaje obsceno, virus o código hostil, en general.
7. La saturación y falta de mantenimiento del buzón electrónico por parte del usuario.
8. Apropiarse de alguna(s) cuenta(s) de correo diferente a la asignada a su persona.
9. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, "spam".

10. Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.

5.2.5. POLITICA DE USO DE SEGURIDAD INFORMATICA Y DE LA INFORMACION

PLT. 19.- Generales.- Las y los usuarios internos cumplirán las siguientes recomendaciones:

1. Si no va a estar cerca de su estación de trabajo, bloquee el equipo o active el protector de pantalla. Se recomienda activar el bloqueo automático de la pantalla del computador para que cuando detecte inactividad no pueda ser utilizado, sin el ingreso de una contraseña.
2. Si va dejar su equipo encendido por periodos extendidos, el usuario deberá asegurarse de no dejar aplicaciones con su usuario activo en los sistemas de la Institución (Correo, Correspondencia, Aplicaciones de Administración de equipos y/o sistemas).
3. No modificar las configuraciones de dirección IP, DNS, hora, nombre de equipos y demás. En caso de requerir un cambio deberán notificar a los técnicos informáticos de su dependencia.
4. No modificar las configuraciones del equipo como fondo de pantalla y protector de pantalla, así como la configuración de software y hardware establecidos por la Dirección Nacional de Tecnología de la Información. Si en su equipo se han realizado modificaciones, debe notificar a los técnicos informáticos de su dependencia, para que se realice la re-configuración del mismo.
5. Está prohibido instalar aplicaciones, programas, utilitarios, que no sean aprobados por su línea de supervisión o que difieran del software base determinado por la Dirección Nacional de Tecnología de la Información, que no tengan licencias o que para su uso se deba romper la seguridad de licenciamiento del mismo.
6. En caso de funcionarios y/o servidores que tengan a su cargo computadores portátiles, estos deberán permanecer con el candado de seguridad durante todo el tiempo que el computador esté sin supervisión de dichos funcionarios y/o servidores. En caso de no disponer del candado, se deberá gestionar la adquisición del mismo a través de la Dirección a la que pertenece.
7. Para evitar pérdida de información, la o el usuario es responsable de respaldar su máquina periódicamente en medios magnéticos externos y verificar que los respaldos generados se encuentren disponibles, e íntegros para su uso de ser requerido.
8. No pueden moverse los equipos o reubicarlos sin permiso. En caso de que necesite movilizar un equipo fuera de la Institución se requiere autorización del Director de la Dependencia por escrito.
9. Está prohibido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios y/o dañar o alterar los recursos informáticos.
10. Todo el personal que accede a los sistemas de información del IESS debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de uso.

PLT. 20.- Compromiso de Confidencialidad.- Las y los servidores de las institución deberán firmar compromisos de confidencialidad y de no-divulgación de información de conformidad con

lo dispuesto en la Constitución, las leyes y las necesidades de protección de información de la institución.

La Dirección Nacional de Gestión de Talento Humano será la encargada de controlar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, gestionar la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción.

El personal de otras entidades públicas o privadas; deberán de igual manera suscribir el compromiso de confidencialidad previo a acceder a la información. Anexo C.

PLT. 21.- Responsables de la seguridad.- Los responsables de la seguridad informática de los activos bajo su custodia serán la Dirección Nacional de Tecnología de la Información y la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, y los responsables de la seguridad de la información serán las Unidades de Negocio hasta que se conforme y formalice la Unidad de Seguridad de la Información Institucional.

PLT. 22.- Responsables de la Información.- Los responsables de la información se definen para asegurar adecuadamente la pertenencia, custodia y salvaguarda de los recursos, teniendo en cuenta una correcta distribución de funciones, que se diferencian entre:

a) Responsables Directos: Los Responsables Directos de la información son aquellos que por la naturaleza de su posición en la Institución conocen el tipo de información que se genera o comunica o ingresen en los diversos sistemas o aplicativos, pueden ser las Gerencias, Seguros Especializados, Direcciones Nacionales, Direcciones Provinciales, Jefaturas o aquellos designados por el Director General o su delegado para dicha actividad, son responsables de:
   - La clasificación directa de la información, de la organización y autorización del acceso a la información.
   - Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.
   - Monitoreo del uso de la información por parte de personal a su cargo
   - Asignar a los responsables del uso y manejo de la información.
b) Monitorear el uso de la información por parte de los Responsables Directos: Los Responsables Directos de la información por tener una relación directa en el manejo de la información serán responsables de monitorear el uso que le dé el personal a su cargo.
c) Responsables Secundarios: Los Responsables Secundarios de la información son aquellos que por la naturaleza de su cargo en la organización deben acceder, modificar o almacenar información. Son responsables de:
   - Manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.
d) Custodios: Los Custodios de la información son aquellos que por la naturaleza de su cargo en la organización deben custodiar, respaldar o almacenar la información. Se convierten en

custodios el personal que tenga acceso a bases de información. Entre sus responsabilidades constan:

- El manejo, transmisión, comunicación y almacenamiento de la información a la que se le dé acceso.
- Mantener la disponibilidad e integridad de la información custodiada.
- Mantener el acceso y permisos de acceso a la información custodiada.
- Brindar soporte para evaluar e identificar la información para su clasificación.

PLT. 23.- Clasificación de la Información.- Los Responsables Directos de la información deberán clasificar adecuadamente la información que manejan y deben asegurarse de que se respete el acceso a la misma por parte del personal a su cargo.

Los activos de información de la organización deben ser clasificados en una de las categorías definidas en el punto Niveles de Clasificación de Información de la Política de Seguridad de la Información.

Para clasificar la información dentro de uno de los niveles determinados o cambiar su categoría, se deben utilizar los criterios de clasificación de información mencionados en el punto Criterios de Clasificación de la Política de Seguridad de la Información.

La información será rotulada claramente con la clasificación que le sea otorgada. Esta rotulación debe ser clara y visible.

Toda la información generada en la organización y que no se le dé una clasificación específica, mantendrá el nivel de PRIVADA y deberá ser tratada como tal.

1. Criterios de Clasificación.- Son:
   a) Valor: Es el principal criterio de clasificación, está basada en el valor del activo desde el punto de vista del negocio (valor propio del activo o producto del mismo).
   b) Edad: Donde la clasificación de cierta información puede cambiar si el valor de la información se reduce con el tiempo.
   c) Vida útil: Cuando la información se vuelve obsoleta en base a nueva información generada, cambios organizacionales u otros motivos.
2. Niveles de clasificación de la Información.- Son:
   a) PUBLICA: Es la información que por su naturaleza, puede ser visible o divulgada por el personal general de la organización, clientes o el público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad o economía de la organización.

      Esta información puede ser, entre otras, publicaciones, anuncios de prensa o medios de comunicación, página web Institucional, etc.

      Nivel de visualización y acceso: Este tipo de información debe obtener su clasificación por niveles autorizados.
   b) SENSIBLE: Solo para uso interno, destinada al uso exclusivo por parte de los empleados de la organización en el desarrollo rutinario de los procesos de negocio.
      La divulgación y visibilidad de la misma dentro de la organización es segura. Esta información debe ser mantenida dentro de la organización, pues su divulgación fuera de

la misma puede tener un impacto leve o moderado a la privacidad del personal o causar un daño leve al negocio o la imagen de la organización.

Esta información puede ser, entre otras, memorandos, avisos, comunicaciones, informativos, etc.

Nivel de visualización y acceso: Todo el personal de la organización, tiene acceso a esta información para su visualización. La modificación de la misma debe darse por el dueño de la información o por autorización escrita.

c) RESTRINGIDA: Información por su naturaleza es destinada solo para uso exclusivo de la organización. Esta información debe ser accedida y visualizada solo por el personal de la organización que cuente con la autorización y extenderse a las dependencias del IESS en general.

La divulgación o visualización no autorizada dentro de la organización o fuera de ella podría violar la privacidad de personas, reducir la ventaja competitiva de la organización o causar un daño significativo al negocio o la imagen de la organización.

Nivel de visualización y acceso: Departamentos, Áreas, Seguros o personas con autorización en base a la tabla de autorizaciones. La autorización debe ser explícita para visualización y/o para modificación.

d) CONFIDENCIAL: Es la información considerada como sensible y está destinada a uso solamente interno y por parte del personal específico que debe tener permisos y autorización para su visualización y/o manejo. La divulgación o visualización no autorizada causaría violación de la privacidad de las personas, reduciría la ventaja competitiva de la organización o produciría un daño grave o irreparable al negocio o la imagen de la organización.

Esta información puede ser, pero no limitarse a: Información de decisión de negocio, información secreta de Afiliados, Pensionistas, Empleadores (pines, contraseñas, historial, etc.),

Información de productos nuevos, información de negocios nuevos, etc.

Nivel de visualización y acceso: El acceso, modificación o visualización de la misma es permitido solo para los dueños de la información y para personal expresamente autorizado de forma escrita por los mismos.

3. Acceso a recursos y privilegios.- Los usuarios deberán tener el nivel necesario de privilegios para acceso a las aplicaciones, configuración de perfil o acceso a recursos para cumplir con las actividades de su cargo.
4. Gestión de Incidentes de Seguridad.- La gestión de incidentes de seguridad debe realizarse considerando los siguientes tres objetivos básicos:
    - Responder rápida y eficientemente.
    - Contener y reparar el daño causado por los incidentes.
    - Prevenir daños futuros.
5. Segregación Funcional.- Ningún proceso crítico debe ser conocido y ejecutado por una sola persona o que una misma persona tenga privilegios o accesos en diferentes fases de un proceso. Los distintos procesos del negocio deben ser claramente descritos, de tal forma que

cualquier persona de la organización pueda ser capaz de asumir los roles y responsabilidades de otra.

6. Prevención y Entrenamiento Continuo.- Las políticas, reglamentos y normas referentes a Seguridad de Información deberán ser conocidos por todos los miembros de la organización y para el efecto, la Institución proveerá recursos necesarios para realizar capacitaciones a los diferentes usuarios de aplicaciones, personal técnico y demás personal de la institución en general.

PLT. 24.- Almacenamiento.- La información obtenida de cualquiera de los servicios y que sea almacenada localmente en el equipo de cómputo del usuario y de propiedad institucional, no podrá ser distribuida o transmitida por la red institucional, o por otros medios de comunicación sin la autorización del inmediato superior.

Es responsabilidad del usuario solicitar de forma periódica a la Dirección Nacional de Tecnología de la Información y/o informáticos de cada dependencia, el respaldo de dicha información.

La Dirección Nacional de Tecnología de la Información revisará el aprovechamiento óptimo de los recursos compartidos en la red para mantener la integridad y para asegurar que los usuarios utilicen los recursos de manera responsable.

PLT. 25.- Transmisión de datos.- A fin de garantizar la integridad y confidencialidad de la información obtenida de los sistemas y aplicativos informáticos de la institución y en razón de que los dispositivos móviles, magnéticos y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada de datos, robo de datos, datos dañados o comprometidos, por la facilidad de uso, alta movilidad y capacidad de almacenamiento, la Dirección Nacional de Tecnología de la Información y la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, de forma programada y bajo pedido de las unidades administrativas, procederá a salvaguardar la información que mantiene la institución, proporcionando el mecanismo tecnológico de encriptación y des encriptación a las Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial. Y las unidades administrativas de forma programada y bajo pedido solicitarán a las Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial la encriptación y/o des encriptación de la información digital.

PLT. 26.- Propiedad y Derechos de contenidos.- La información disponible en Internet, incluyendo textos, software, música, sonido, fotografía, video, gráficos u otro material contenido, está protegida por copyright, marcas registradas, patentes u otros derechos de propiedad y leyes. Sólo se permite el uso de este material bajo autorización expresa del autor.

El bajar, cargar, archivar, copiar, imprimir o enviar cualquier material debe ser realizado solamente bajo la autorización del autor.

Los usuarios no deben descargar ni instalar ningún tipo de software comercial, shareware o freeware en las unidades de disco o en cualquier disco, sin la autorización de los técnicos informáticos de cada dependencia.

PLT. 27.- Conducta del Usuario Interno.- El Usuario Interno observará lo siguiente:

1. El usuario es el único responsable del contenido de transmisiones a través de cualquier servicio.
2. El usuario debe cumplir con las leyes de transmisión de datos técnicos de los países desde los cuales y hacia donde se envían los mensajes de correo electrónico.
3. El usuario no debe usar el servicio para propósitos ilegales o de entretenimiento.
4. El usuario debe cumplir con todas las regulaciones, políticas y procedimientos del uso del internet en la Institución.
5. La comunicación de los usuarios se debe conducir con respecto y consideración, evitando los abusos y el uso del lenguaje inapropiado.
6. Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades del IESS o con las actividades del usuario.

PLT. 28.- Respaldo de la información tecnológica.- La Dirección Nacional de Tecnología de la Información y la Subdirección Provincial de Apoyo a la Gestión Estratégica a nivel territorial, así como las unidades negocio, propietarias de la información como correspondan, determinarán el procedimiento de resguardo y contención de la información obtenida de los sistemas y/o aplicativos informáticos, considerando al menos los siguientes ítems:

a) Etiquetado de las copias de respaldo, contenido, periodicidad y retención.
b) Extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución.
c) Vida útil recomendada por el proveedor y la destrucción de estos medios magnéticos.
d) Guardado de los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.
e) Grado apropiado de protección física y ambiental.
f) Eventos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.
g) Protección de la información confidencial por medio de encriptación.
h) Generación de respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

5.2.6. POLITICA DE USO DE SOFTWARE

PLT. 29.- Administración.- La Dirección Nacional de Tecnologías de la Información será la única dependencia encargada, a nivel nacional, de la administración, instalación, soporte y funcionamiento del software instalado en el IESS. Dentro de las responsabilidades de la administración e instalación de software se describen las siguientes:

1. Mantener el resguardo de las licencias de uso de software de la Institución.

2. Mantener actualizado el catálogo de software de la Institución, desinstalar el software de las computadoras que no posean licencias o que no estén aprobadas por la Dirección Nacional de Tecnología de la Información.
3. Revisar periódicamente la vigencia de uso de las licencias adquiridas.
4. Generación de estándares de software institucional.
5. Establecer los procedimientos para el uso de software.
6. Realizar el análisis de necesidades y requerimientos de negocio, con la finalidad de planificar la adquisición o desarrollo de una solución de software.
7. Efectuar el registro de derechos de autor de los sistemas del IESS, desarrollados directamente o a través de terceros (contratados), en cumplimiento con las disposiciones de la Ley de Propiedad Intelectual.

PLT. 30.- Uso/Instalación de Software.- Para el uso e instalación de software se observará lo siguiente:

1. La Dirección Nacional de Tecnología de la Información es la única autorizada, así como responsable, de realizar la instalación de software y proporcionar soporte técnico del mismo en las computadoras de la Institución.
2. El software utilizado por la Institución, deberá ajustarse a las especificaciones técnicas y arquitectura de la plataforma tecnológica disponible en la Dirección Nacional de Tecnología de la Información. Se exceptuarán los casos debidamente justificados mediante informe técnico del área de desarrollo de software.
3. El software adquirido debe cumplir con los procesos formales de recepción, validación técnica y pruebas, previos a la aceptación técnica del producto.

PLT. 31.- Restricciones.- Se prohíbe la instalación y/o uso del software en los siguientes casos:

1. Copias ilegales de cualquier sistema informático, software o programa.
2. Software descargado de Internet.
3. Software que no se haya identificado como institucional.
4. Instalaciones no autorizadas o que no hayan sido solicitadas a la Dirección Nacional de Tecnología de la Información.
5. Software adquirido para uso personal del usuario (sin fines institucionales).
6. Software de entretenimiento o que no tenga relación con las actividades institucionales.
7. Software sin licencia.

PLT. 32.- Requerimientos de Software.- Todo usuario interno que requiera la instalación de un determinado software deberá solicitarlo a la Dirección Nacional de Tecnología de la Información de acuerdo al procedimiento y formatos que para el efecto se establezcan.

La Dirección Nacional de Tecnología de la Información determinará, de acuerdo a las características del software solicitado, si existe disponibilidad de licencias para atender la petición o, en su caso, si se cuenta con el software adecuado para atender a las necesidades del usuario.

En caso de ser necesaria la adquisición de nuevo software la Dirección Nacional de Tecnología de la Información será la encargada de remitir al usuario las especificaciones técnicas generales y específicas de dicho software. Para la continuación del trámite respectivo, el usuario será el encargado de realizar los estudios completos (incluye estudio de mercado) y demás documentación de sustento para el procedimiento de contratación de conformidad con la Ley Orgánica del Sistema Nacional de Contratación Pública, su Reglamento General, Resoluciones del Servicio Nacional de Contratación Pública y del IESS.

5.2.7. POLITICA DE DESARROLLO DE SOFTWARE

PLT. 33.- Generales- Para el desarrollo de software se requiere:

1. Toda solicitud de desarrollo, evaluación o modificación de programas informáticos deberá empezar con el pedido formal a la Dirección Nacional de Tecnologías de la Información, para su análisis y aprobación.
2. La unidad requirente será la responsable de contar con la siguiente documentación, previa al inicio del proceso de desarrollo:
    - Proceso oficializado y aceptado por la unidad requirente y la Dirección Nacional de Procesos.
    - Documentación del flujo de procesos, procedimientos y actividades.
    - Formularios relacionados con el proceso.
    - Reglas y excepciones de negocio.
    - Responsables de las áreas involucradas para el acompañamiento en el proceso de desarrollo.
    - Documentación adicional que se deba tomar en cuenta para el proceso de desarrollo de software.
3. Los desarrollos o modificaciones de software deben estar de acuerdo a la arquitectura de aplicaciones definida por la Dirección Nacional de Tecnología de la Información, y deben seguir estándares y buenas prácticas de la industria.
4. El ciclo de desarrollo de software debe contar con un proceso de aseguramiento de la calidad (QA), que garantice que el producto sea desarrollado cumpliendo con criterios de calidad. Para lo cual, la Dirección Nacional de Tecnología de la Información deberá realizar las pruebas necesarias para garantizar la seguridad, rendimiento y confiabilidad de los aplicativos.
5. La unidad requirente deberá validar que el software cumpla con las funcionalidades y requerimientos solicitados, previo a la liberación en ambiente de producción.
6. Todo software desarrollado debe garantizar el registro de pistas de auditoría, donde se evidencien los eventos realizados por un usuario dentro de una aplicación.

PLT. 34.- Entorno de Trabajo.- La Dirección Nacional de Tecnología de la Información utilizará los siguientes ambientes para el proceso de desarrollo de software:

a) Desarrollo. Ambiente utilizado para la construcción de los productos de software. El ambiente es administrado por el área de desarrollo.

b) Pre producción (Pruebas). Establecido como un ambiente idéntico al de producción, utilizado para control de calidad y pruebas del sistema. El ambiente es administrado por el área de calidad.
c) Producción. Ambiente utilizado para la operación de los sistemas. El ambiente es administrado por el área de Operaciones y el área de Base de Datos.

La información almacenada en el ambiente de producción no debe ser utilizada, ni visible a los ambientes de pre producción y desarrollo, con el fin de precautelar la confidencialidad de los datos.

PLT. 35.- De la implantación de un sistema en ambiente de producción.-

1. El área de desarrollo de software, conjuntamente con el área de QA y el área de operaciones, seguirán el procedimiento determinado y aprobado por la Dirección Nacional de Tecnología de la Información para la implantación o modificación de los sistemas que se encuentran en ambiente de producción.
2. La implantación o modificación de los sistemas desarrollados por la Dirección Nacional de Tecnología de la Información debe ser validada y aprobada formalmente por el área requirente, previamente a la liberación en el ambiente de producción.

5.2.8. POLITICA DE USO DE INTERNET E INTRANET

PLT. 36.- Generales.- Los servicios de Internet e Intranet son recursos que la institución pone a disposición de las y los funcionarios, servidores y demás trabajadores del IESS, como una herramienta de consulta de información, investigación y acceso a los sistemas institucionales, facilitando la realización de las labores cotidianas, tomando en cuenta lo siguiente:

1. El acceso y uso de los servicios de Internet e Intranet está condicionado a la aceptación de las presentes políticas.
2. El uso del servicio de Internet e Intranet está limitado a la realización de actividades laborales que estén relacionadas con los propósitos y funciones institucionales.
3. El acceso a estos servicios debe ser solicitado a la Dirección Nacional de Tecnología de la Información, previa autorización del titular de la unidad administrativa o médica a la que pertenezca el usuario. Anexo D.
4. En caso de que la solicitud sea aprobada, se realizará la configuración necesaria en el equipo del usuario y le asignará un perfil de acceso con un nivel de navegación (acceso a sitios web) determinado, de acuerdo a las actividades que el usuario desempeña dentro de la Institución.
5. En caso de que el usuario requiera acceder a un sitio web restringido por el nivel de navegación otorgado, deberá solicitar a la Dirección Nacional de Tecnología de la Información la habilitación de dicho sitio, adjuntando las justificaciones necesarias.
6. En caso de que un usuario externo, ajeno a la Institución, requiera el acceso al servicio de Internet, se le asignará un perfil de acceso limitado, con navegación básica y a través de una conexión de red que no ponga en riesgo la seguridad de los equipos internos de la Institución.

7. El intercambio de información entre las dependencias administrativas y médicas del IESS se lo realizará a través de red local, Intranet o una conexión privada virtual.

PLT. 37.- Responsabilidades.- Los servicios de enlaces de datos y de Internet e Intranet son administrados por el personal de la Dirección Nacional de Tecnología de la Información a través del área de Infraestructura. El proveedor del servicio enlace de datos y de Internet es responsable de garantizar la disponibilidad y los anchos de banda del enlace, de acuerdo a los acuerdos de nivel de servicio contratados, tomando en cuenta lo siguiente:

- Los servicios de Internet contratados por las Unidades Administrativas y Médicas a nivel nacional, su uso y administración estarán de acuerdo a los lineamientos o especificaciones que marque la Dirección Nacional de Tecnología de la Información; la Subdirección Provincial de Apoyo a la Gestión Estratégica en las jurisdicciones provinciales solventarán los problemas técnicos y errores de recepción y envío y gestionarán su atención inmediata.
- La Dirección Nacional de Tecnología de la Información es responsable de monitorear periódicamente el uso de Internet e Intranet del IESS, con la finalidad de vigilar el cumplimiento de las presentes políticas, manteniendo la confidencialidad de la información.
- La información y mensajes que se envíen a través de Internet, serán de completa responsabilidad del usuario emisor. En ningún momento dichos mensajes podrán atentar contra la imagen y reputación de la Institución
- El usuario será el único responsable por los sitios web visitados desde su perfil de acceso a Internet, por lo tanto, será también responsable de mantener en privado las credenciales de su cuenta de acceso a Internet.

PLT. 38.- Prohibiciones.- Se prohíbe lo siguiente:

1. Utilizar el Internet como un medio para realizar cualquier actividad comercial o lucrativa de carácter individual o la participación y distribución de actividades o materiales que vayan en contra de la Ley.
2. Utilizar el Internet para propósitos que puedan influir negativamente en la imagen del IESS, de sus autoridades o funcionarios.
3. Realizar cualquier actividad que pueda comprometer la seguridad de los servidores y recursos informáticos de la Institución.
4. Accesos a sitios web que puedan ser percibidos como obscenos, que distribuyan, emitan o promocionen material pornográfico, material ofensivo o con humor inapropiado; que vaya en contra de la moral y buenas costumbres.
5. Acceso a sitios de juegos y actividades recreativas o de promoción de intereses personales tales como redes sociales, chat, encuestas, concursos, mensajes no solicitados, etc.
6. Transmitir amenazas, material indecente o de hostigamiento. Así como intimidar, insultar, difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios.
7. Distribuir por Internet de material que cause daños, como la piratería, el sabotaje, específicamente la distribución de software malicioso.
8. Descargar e instalar programas o archivos vía Internet. Únicamente se podrá llevar a cabo esta tarea en situaciones previamente convenidas con la Dirección Nacional de Tecnología de la información.

9. Congestionar, afectar, interferir o paralizar el uso del servicio.
10. La instalación o uso de programas P2P (este tipo de programas, utiliza una red común para comunicar entre si las computadoras de los usuarios, donde se encuentran los archivos a intercambiar), como por ejemplo: Ares, Torrent, Blubster, Computwin, E-Donkey, Emule, entre otros.
11. Descargar música, fotos, videos, u otro material que no esté relacionado con las actividades o propósitos laborales.

5.2.9. SANCIONES

PLT. 39.- Incumplimiento de las Políticas.- Ante el incumplimiento de las obligaciones contempladas en este instrumento, dependiendo de la gravedad de la infracción cometida, se iniciarán las respectivas acciones y procedimientos administrativos y jurisdiccionales, de conformidad a las normas que las regulan, a fin de que se determine la responsabilidad civil, administrativa y penal, a que haya lugar, en contra de las personas imputables. El Instituto Ecuatoriano de Seguridad Social podrá iniciar las acciones de oficio o a petición de parte, a través de los órganos competentes.

Además de las acciones y procedimientos que se ejerzan en contra de los sujetos responsables de la violación de este instrumento, el Director Nacional de Tecnología de la Información o quien haga sus veces en territorio, dependiendo de la gravedad del incumplimiento y luego de seguir el debido proceso de acuerdo a la normativa legal vigente, en especial a la Ley Orgánica de Servicio Público su reglamento de aplicación y más normativa conexa, calificará motivadamente la falta e impondrá las siguientes acciones:

1. Ante un incumplimiento leve de las Políticas, se notificará por escrito recordándole la vigencia de las Políticas al usuario responsable de la falta, así como se pondrá en conocimiento del Titular de la dependencia a la que pertenezca el usuario y a la Dirección Nacional de Gestión de Talento Humano para su seguimiento y control.
2. En el evento de presentarse un incumplimiento moderado en las Políticas, o una reincidencia en un incumplimiento leve, se notificará por escrito al Titular de la dependencia a la que pertenezca la o el servidor y a la Dirección Nacional de Gestión de Talento Humano, así como de considerarlo necesario se podrá disponer la suspensión temporal del servicio a la o el usuario responsable hasta que el Titular del área apruebe por escrito la restauración del servicio.
3. En caso de presentarse un incumplimiento grave de las Políticas, causará el retiro de los equipos, bienes, servicios y herramientas informáticas.

CONCLUSIONES

- En las normativas Ecuatorianas aplicadas en el sector de la salud para la seguridad de los sistemas de información no se posee un conjunto de políticas claras que asegure los datos contenidos en las historias clínicas de manera electrónica, la adaptación de la Norma ISO 27001 e HIPAA generada permite asegurar la información contenidas en las Historias Clínicas en Hospitales de Nivel I del IESS.

- Las Normas ISO 27001 e HIPAA tienen puntos en común dentro de las políticas de seguridad de la información como políticas de sanciones, copias de seguridad, establecimiento de responsabilidades, el análisis y gestión de riesgos que permitieron establecer ventajas de cada una como la generalidad de la ISO y la orientación al sector de la salud con la HIPAA; y las desventajas de no tener un marco de trabajo y políticas de seguridad de la información que permitan reducir la probabilidad de ocurrencia de los riesgos o vulnerabilidades presentes en los nosocomios de Nivel I del IESS.

- La reducción de vulnerabilidades presentes en los riesgos detectados, producto de la implementación de esta adaptación que fue realizada en el Hospital del IESS de Nivel 1 de la ciudad Guaranda, es muy aceptable logrando reducir los riesgos en un 61,86% frente a la situación inicial evaluado en dos fases: antes y post implementación; mejorando las características principales de los objetivos de la seguridad de la información basadas en la confidencialidad y privacidad de los datos críticos de las historias clínicas.

RECOMENDACIONES

Tomando en consideración todos y cada uno de los cálculos obtenidos en esta investigación, se recomienda implementar esta propuesta de modelo de adaptación de las Normas ISO 27001 e HIPAA para la reducción de riesgos de seguridad de la información en los Hospitales Nivel I del IESS a nivel nacional, puesto que se obtuvieron resultados favorables dentro del Hospital del Guaranda “Dr. Humberto del Pozo”, además de cumplir irrestrictamente a las normas generales emitidas por la Dirección Nacional de Tecnologías de la Información del IESS.

Se recomienda realizar la implementación del modelo y de las políticas generadas en unidades médicas de diferente nivel de atención a los Hospitales de Nivel I escogidas por el Instituto Ecuatoriano de Seguridad Social, con el objeto de evaluar la posibilidad implementación en todos los centros médicos de la institución.

Se recomienda que el nivel de seguridad que se puede alcanzar ante la implementación de este modelo de adaptación de las normas debe ser administrado por un Oficial de Seguridad de la Información, oficial que debe ser incorporado a la plantilla de personal de cada Hospital.

BIBLIOGRAFÍA

ASAMBLEA NACIONAL REPUBLICA DEL ECUADOR. (2014, febrero 3). Código Orgánico Integral Penal. Suplemento -- Registro Oficial Nº 180.

BENITEZ K., & MALIN B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. *Journal of the American Medical Informatics Association*, *17*(2), 169–177.

CHACÓN P. (2012). *Propuesta de un modelo de sistema de gestión de seguridad de la información para institutos superiores tecnológicos de educación aeronáutica*. Quito, 2012. Recuperado a partir de http://bibdigital.epn.edu.ec/handle/15000/7807

COMISIÓN INTERVENTORA DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL. (2000, enero 26). Reglamento General de las Unidades Médicas del IESS.

CONTRERAS. P.(2004),Gestión de recursos informáticos. Unidad 5. Chile.

CONGRESO NACIONAL. (1995, de enero de). Ley De Derechos Y Amparo Al Paciente.

HASH J. (2005). *An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule*. National Institute of Standards and Technology.

HERN P. POR J., HERN, EZ, & EZ. (s/f). Escala de la probabilidad. Eventos complementarios, eventos mutuamente excluyentes e independientes. Recuperado el 8 de mayo de 2017,

INTECO. (s. f),Instituto Nacional de tecnologías de la comunicación. Implantación de un SGSI en la empresa. Conceptos básicos sobre seguridad de la información. España.

ISO 27001. (2013, febrero 10).

ISO 27001 - INFORMATION SECURITY MANAGEMENT. (s/f). Recuperado el 17 de febrero de 2015.

ISO IEC. (2005, octubre 15). Estándar Internacional ISO/IEC 27001. ISO/IEC.

LA PROTECCIÓN DE DATOS PERSONALES - Derecho Ecuador. (s/f).

LÓPEZ P. (2010). *Seguridad informática*. Editex.

MINISTERIO DE SALUD PÚBLICA. (2015a, enero 16). Tipologia Para Homologar Establecimientos De Salud Por Niveles.

MINISTERIO DE SALUD PÚBLICA. (2015b, enero 29). Reglamento De Informacion Confidencial En Sistema Nacional De Salud.

MINISTERIO DE SALUD PÚBLICA, INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL, INSTITUTO DE SEGURIDAD SOCIAL DE LAS FUERZAS ARMADAS, & INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICIA

NACIONAL. (2012, abril 10). Convenio marco Red Integral Pública de Salud. Registro Oficial.

MISHRA, S., LEONE, G., CAPUTO, D., CALABRISI, R., & MORRIS, R. (2011). Security awareness for healthcare information systems: A HIPAA compliance perspective. *Issues in Information Systems*, *12*(1), 224–236.

MOSQUERA G., SARAVIA J, & PACHECO J. (2015). *Elaboración de políticas de seguridad física y ambiental basados en el estándar internacional iso/iec 27002:2013 en el hospital regional josé david padilla villafañe ese. De la ciudad de aguachica-cesar*. Universidad francisco de paula santander ocaña.

MUÑOZ, D. R. (2012). *Manual de Estadística*. España: B - EUMED.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2008, octubre). An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (último). (2011, octubre 31). HIPAA Security Rule Toolkit User Guide. National Institute of Standards and Technology.

NATIONAL FORENSIC SCIENCE TECHNOLOGY CENTER, NFSTC. (s. f.) A Simplified Guide to Digital Evidence. Florida: El Centro.

PEÑAHERRERA C, & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA. (2013, septiembre 25). Acuerdo Ministerial 166. Registro Oficial Suplemento 88.

SANCHEZ, L. E., OLMO, A. S., ALVAREZ, E., MEDINA, E. F., & PIATTINI, M. (2012). LOPD Compliance and ISO 27001 legal requirements in the Health Sector. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, *10*(3), 1824–1837.

SÁNCHEZ-HENAREJOS, A., FERNÁNDEZ-ALEMÁN, J. L., TOVAL, A., HERNÁNDEZ-HERNÁNDEZ, I., SÁNCHEZ-GARCÍA, A. B., & CARRILLO DE GEA, J. M. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atención Primaria*, *46*(4), 214–222.

ANEXOS

ANEXO A. Modelo de encuesta aplicada.

	INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL **HOSPITAL IESS GUARANDA**
	ENCUESTA

El Hospital está realizando un estudio que permitirá evaluar parámetros concernientes a la seguridad de la información presente en las Historias Clínicas de nuestros afiliados, motivo por el cual le solicitamos conteste la siguiente las siguientes preguntas con total sinceridad .

Preguntas	SI	NO
¿En el Hospital, hay un plan acordado para los esfuerzos de seguridad y cumplimiento de la privacidad de los datos clínicos?		
¿Se le proporciona regularmente capacitación sobre medidas de seguridad?		
¿El acceso al sistema se basa en el papel que desempeño en el Hospital?		
¿Crear conciencia de seguridad es un proceso continuo en el Hospital?		
¿En el Hospital, los controles de seguridad (control de acceso, política de contraseñas) se consideran un componente necesario para la seguridad?		
¿Existe una estructura clara para la acción de observación y manipulación de la información del afiliado?		
¿En el Hospital, hay controles internos adecuados (políticas, procedimientos, capacitación, restricciones de acceso) para proporcionar seguridad y privacidad de los registros de salud		
¿Estoy obligado a informar sobre cualquier uso indebido de la información (de la que estoy a cargo) o su acceso inapropiado		
¿El acceso al sistema se basa en el rol que desempeño dentro del Hospital		
¿En el Hospital, tengo comunicación frecuente sobre temas de ingeniería social y soy consciente de cómo tales tácticas pueden crear vulnerabilidad para nuestro sistema		
¿En el Hospital, entiendo qué información tengo acceso y por qué?		
¿En el Hospital, tengo que tomar permiso para usar sitios de redes sociales		
¿Tengo conocimiento del procedimiento sobre qué hacer cuando mi sistema tiene malware en el Hospital		
¿La disponibilidad de comunicación con el sistema MIS-AS400 es permanente		
¿Las políticas y procedimientos de seguridad alojadas en el repositorio del Hospital, son fácilmente accesibles y comprensibles en el Hospital		
¿Existe una estructura clara para la acción disciplinaria en caso de incumplimiento de las políticas y procedimientos en el Hospital		
¿Tengo que acceder a la información de salud sólo a través de dispositivos y software aprobados en la organización		
¿Tengo permiso para usar medios de almacenamiento extraíbles desde el exterior en mi máquina en la organización		
¿Se establece dentro del Hospital la importancia de administrar la información que no debemos divulgar salvo en casos de emergencia		
¿Con frecuencia recibo información sobre la legislación vigente que trata sobre la confidencialidad de los datos del paciente		
¿El Hospital, posee una estructura clara para el procedimiento de entrega de información de salud		
¿Tengo conocimiento de la directiva de contraseñas que tengo que cumplir, en el Hospital		
¿La auditoría se considera una acción complementaria necesaria para mejorar la seguridad Iniciativas en el Hospital		
¿En el Hospital, las políticas y procedimientos de seguridad son revisados periódicamente		
¿Hay un liderazgo visible sobre la seriedad de los esfuerzos de seguridad en el Hospital		
¿La auditoría es vista como una acción complementaria necesaria para mejorar las iniciativas de seguridad en el Hospital		
¿Tengo que leer las políticas de seguridad con frecuencia (trimestral, bi-anual, anual) en el Hospital		

ANEXO B. Estandarización de equipos.

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL
HOSPITAL IESS GUARANDA

PROCEDIMIENTO PARA LA INSTALACIÓN DE COMPUTADORES PERSONALES DENTRO DE DOMINIOS DE CONTROL.

1. Verificar, instalar o activar sistema operativo.
2. Configurar la etiqueta genérica de cada equipo. El formato varía de acuerdo a la ubicación y será especificado en coordinación con el respectivo responsable técnico del lugar. El formato es el siguiente:

   PCUIODP01HL01

   a) **PC**. Determina el tipo de equipo (PC - Computador, PR - Impresora, etc.), máximo 2 caracteres.
   b) **UIO**. Determina la ciudad donde se encuentra, máximo 3 caracteres.
   c) **DP**. Determina el edificio donde se encuentra (DP – Dirección Provincial de Pichincha, DG – Dirección Provincial del Guayas, ZZ – Edificio Zarzuela, etc.), máximo 2 caracteres.
   d) **01**. Determina en que piso se encuentra (PB – Planta Baja, MZ – Mezanine, 01 – Primer Piso, etc.)
   e) **HL**. Determina el área de trabajo u oficina donde pertenece (SC – Seguro Social Campesino, PE – Pensiones, RT – Riesgos del Trabajo, etc.), máximo 2 caracteres.
   f) **01**. Determina el número secuencial de equipos.
3. Configurar el protocolo TCP/IP, de manera que el DNS se encuentre con la dirección 172.16.0.88 (*En caso de no existir DHCP*).
4. Ingresar como administrador del equipo, configurar el computador dentro del dominio.
5. Establecer contraseña de administrador local y eliminar las cuentas que no sean necesarias.
6. Ingresar como usuario del dominio para instalar aplicaciones básicas y parches del sistema operativo de acuerdo al siguiente orden:
   a) Instalar el ultimo Service Pack para el Windows.
   b) Instalar la última versión de Internet Explorer, Firefox o Chrome
   c) Instalar la última versión de Acrobat Reader.
   d) Instalar 7 Zip
   e) Instalar la última versión disponible de Ultra VNC.
   f) Instalar Antivirus McAffe corporativo con su respectivo agente EPO:
   g) Instalar WPS Office o Microsoft Office licenciado.
7. Configurar el navegador de manera que:
   a) La página de inicio por defecto sea:
      i) ***hl.iess.gov.ec*** En el caso de equipos ubicados en los kioscos de Historia Laboral y Recaudación.
      ii) ***www.iess.gov.ec*** En computadores de cualquier otra área u oficina.
   b) En la Configuración de Archivos Temporales de Internet se encuentre establecido:
      i) Cada vez que se visita la página
      ii) El mínimo almacenaje de archivos temporales (1 MB).
   c) Se encuentre activada la opción Java Virtual Machine.
   d) Se encuentren instalados los certificados electrónicos para el acceso al correo electrónico del IESS.
8. Probar el acceso a las páginas WEB del IESS.

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL
HOSPITAL IESS GUARANDA

PROCEDIMIENTO PARA LA INSTALACIÓN DE COMPUTADORES PERSONALES FUERA DE DOMINIOS DE CONTROL.

1. Verificar, instalar o activar sistema operativo.
2. Configurar la etiqueta genérica de cada equipo. El formato varía de acuerdo a la ubicación y será especificado en coordinación con el respectivo responsable técnico del lugar. El formato es el siguiente:

   PCUIODP01HL01

   a) **PC**. Determina el tipo de equipo (PC - Computador, PR - Impresora, etc.), máximo 2 caracteres.
   b) **UIO**. Determina la ciudad donde se encuentra, máximo 3 caracteres.
   c) **DP**. Determina el edificio donde se encuentra (DP – Dirección Provincial de Pichincha, DG – Dirección Provincial del Guayas, ZZ – Edificio Zarzuela, etc.), máximo 2 caracteres.
   d) **01**. Determina en que piso se encuentra (PB – Planta Baja, MZ – Mezanine, 01 – Primer Piso, etc.)
   e) **HL**. Determina el área de trabajo u oficina donde pertenece (SC – Seguro Social Campesino, PE – Pensiones, RT – Riesgos del Trabajo, etc.), máximo 2 caracteres.
   f) **01**. Determina el número secuencial de equipos.
3. Configurar el protocolo TCP/IP, de manera que el DNS se encuentre con la dirección 172.16.0.88 (*En caso de no existir DHCP*).
4. Crear la cuenta *invitado1* con la contraseña *invitado1*.
5. Ingresar como usuario local (*invitado1*), contraseña que deberá ser cambiada por el usuario una vez entregado el equipo.
6. Establecer la contraseña del administrador local (*administrador*) y eliminar las cuentas que no sean necesarias.
7. Ingresar como usuario del dominio para instalar aplicaciones básicas y parches del sistema operativo de acuerdo al siguiente orden:
   a) Instalar el ultimo Service Pack para el Windows.
   b) Instalar la última versión de Internet Explorer, Firefox o Chrome
   c) Instalar la última versión de Acrobat Reader.
   d) Instalar 7 Zip
   e) Instalar la última versión disponible de Ultra VNC.
   f) Instalar Antivirus McAffe corporativo con su respectivo agente EPO:
   g) Instalar WPS Office o Microsoft Office licenciado.
8. Configurar el navegador de manera que:
   a) La página de inicio por defecto sea:
      i) ***hl.iess.gov.ec*** En el caso de equipos ubicados en los kioscos de Historia Laboral y Recaudación.
      ii) ***www.iess.gov.ec*** En computadores de cualquier otra área u oficina.
   b) En la Configuración de Archivos Temporales de Internet se encuentre establecido:
      i) Cada vez que se visita la página
      ii) El mínimo almacenaje de archivos temporales (1 MB).
   c) Se encuentre activada la opción Java Virtual Machine.
   d) Se encuentren instalados los certificados electrónicos para el acceso al correo electrónico del IESS.
9. Probar el acceso a las páginas WEB con los cambios realizados.

ANEXO C. Acuerdo de confidencialidad.

HOSPITAL BÁSICO DEL IESS GUARANDA
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
ACUERDO DE CONFIDENCIALIDAD

FECHA: _____

APELLIDOS Y NOMBRES: _____

CÉDULA DE IDENTIDAD: _____

Según lo dispuesto en el Reglamento de Información Confidencial del Sistema Nacional de Salud, mediante el cual se establece la obligatoriedad de contar con un sistema adecuado de custodia digital y física de los datos pertenecientes a la esfera de la intimidad de las personas, el usuario se obliga y compromete a: Respetar los datos de carácter confidencial contenidos en el Sistema AS-400 o demás documentación clínica, en concordancia con el Art. 66, numeral 19 de la Constitución de la República "*Se reconoce y garantizará a las personas: (…) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley*"**; Art. 6 de la Ley Orgánica de Transparencia y Acceso de la Información Pública** "*Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 (66) y 24 (76) de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas." (se aclara que los artículos aludidos corresponden actualmente a los artículos 66 y 76, respectivamente de la Constitución)*." **y Art. 4 de la Ley de Derechos y Amparo del Paciente** "*Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información…*"**. Por tanto, entiende que es de su exclusiva responsabilidad la utilización de la clave de acceso de dicho sistema; y, que se encuentra expresamente prohibido el uso, divulgación por cualquier medio, reproducción, o cualquier acto que infrinja el dispositivo legal vigente y que atente contra la intimidad de las personas; hecho susceptible de ser sancionado con la pena privativa de libertad de uno a tres años, según el Art. 178 del Código Orgánico Integral Penal Vigente.**

_____
FIRMA ACEPTACIÓN USUARIO

ANEXO D. Solicitud de permisos de internet.

HOSPITAL BÁSICO DEL IESS GUARANDA
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

SOLICITUD DE PERMISOS DE INTERNET

FECHA: _____

Yo, Nombre Completo. (Autoridad) como Cargo que se ocupa (Autoridad). en Departamento/Área., autorizo se solicite la habilitación de los siguientes permisos de internet para la(s) siguiente(s) persona(s) a mi cargo.

Nombre Completo: Nombre completo usuario.
Dirección ip:
Motivo Laboral para este servicio: Motivo laboral.
Tipo de Internet:

☐ Internet Básico ☐ Internet con Correos Externos

Información adicional: ☐Conexión con cable de Red ☐Conexión Inalámbrica

Firma de Responsabilidad del solicitante: _____

AUTORIZACIÓN
Nombre completo. (Autoridad):
Cargo que ocupa. (Autoridad):
Departamento / Área:
FIRMA

ANEXO E. Plan de Contingencias.

PLAN DE CONTINGENCIAS TIC's

INTRODUCCIÓN

En la actualidad los cambios tecnológicos adquieren cada vez mayor importancia al interior de las organizaciones, no menos importante es también el cuidado de la integridad del recurso humano, por lo cual se hace necesario o indispensable contar con un plan de contingencias, que garantice el restablecimiento del correcto funcionamiento de los servicios en el menor tiempo posible, ante cualquier eventualidad.

Conscientes de ello, se pretende definir en este documento, las políticas más asertivas aplicables al Hospital Básico del IESS Guaranda, en materia de recuperación de la normalidad para aquellas eventualidades no previstas en las que algún recurso informático se vea amenazado o afectado.

Los fallos técnicos y humanos han hecho recapacitar a las organizaciones sobre la necesidad de auxiliarse con herramientas que le permitan garantizar una rápida vuelta a la normalidad ante la presencia de cualquier eventualidad.

El Hospital IESS Guaranda es una entidad que por su carácter misionario de atención en salud y por su ubicación geográfica concentra la atención de cientos de usuarios del sector; por lo tanto, el hecho de diseñar y preparar un plan de contingencias no implica un reconocimiento de la ineficiencia en la gestión de la Institución, sino todo lo contrario, los mecanismos de seguridad de la información buscan proteger a la información de las diversas amenazas a las que se ve expuesta y supone un importante avance a la hora de superar todas aquellas adversidades que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del Hospital durante un período más o menos prolongado en donde se vea afectado o interrumpido la prestación de servicio al usuario, razón de ser de la Institución.

Todo esto conlleva a que la función de definir los planes a seguir en cuestión de seguridad se conviertan en una tarea realmente compleja y dispendiosa.

OBJETIVOS GENERALES Y ESPECÍFICOS

Generales:

- Garantizar la continuidad de las actividades del Hospital Básico del IESS Guaranda, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones – TICs, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales con el menor impacto posible a los afiliados y usuarios internos.

Específicos:

- Contar con documentación práctica y actualizada que garantice al Hospital Básico del IESS Guaranda la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
- Contar con personal debidamente capacitada y organizada para afrontar adecuadamente las contingencias que puedan presentarse en las actividades del Hospital.

1. ALCANCE

La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

2. MARCO TEORICO

El Plan de Contingencia informático es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones – TIC's del Hospital Básico del IESS Guaranda, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Acciones a ser consideradas:

- **Antes**, como un plan de respaldo o de prevención para mitigar los incidentes.
- **Durante**, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- **Después**, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término "**incidente**" en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en el Hospital Básico del IESS Guaranda.

2.1. Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

2.2. Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá remplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia. Ver Anexo A01: Formato de ocurrencia de evento.

2.3. Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Todo Plan de Contingencia informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

2.4. Plan de Pruebas

El Plan de Pruebas, será presentado a la Dirección Administrativa del Hospital Básico del IESS Guaranda para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas a este plan, se ejecutaría semestralmente, mes de Junio y Diciembre con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

3. METODOLOGÍA

La presente metodología es el resultado de la experiencia práctica del responsable del área de Sistemas en la elaboración de planes de contingencia, mitigación de riesgos y seguridad, también en base a experiencias en otras instituciones, lo cual garantiza que el documento final sea necesariamente objetivo y práctico, a fin de contar con una herramienta efectiva en caso de una contingencia real.

Para elaborar el Plan de Contingencia se seguirá una metodología que tiene las siguientes fases:

- Fase 1: Organización
- Fase 2: Identificación y priorización de riesgos
- Fase 3: Definición de eventos susceptibles de contingencia
- Fase 4: Elaboración del Plan de Contingencia
- Fase 5: Definición y Ejecución del Plan de Pruebas
- Fase 6: Implementación del Plan de Contingencia

3.1. Organización del Plan de Contingencia

Uno de los aspectos que evidencia un carácter formal y serio en toda organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la organización en el Plan de Prevención, Ejecución y Recuperación, pero definiendo un grupo responsable para su elaboración, validación y mantenimiento.

Por lo que se propone la siguiente organización según gráfico 1:

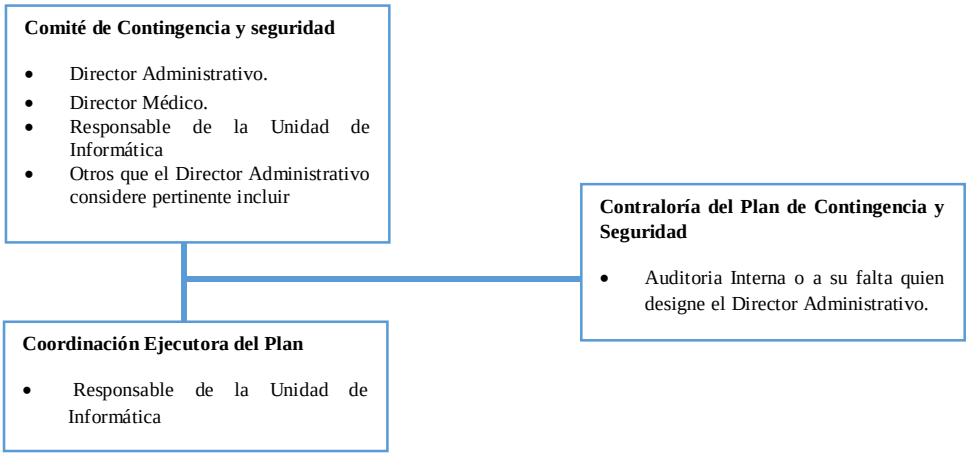

Gráfico 1: Organización Administrativa del plan de Contingencia

A continuación se describe las funciones y roles de la Organización Administrativa del Plan de Contingencia:

Comité de Contingencia

El Comité de Contingencias es el órgano donde se coordinan y aprueban todas las actividades previamente planificadas para ejecutarse en el caso de contingencias del servicio.

Este comité se reunirá por lo menos con una periodicidad semestral y en él se definirán los lineamientos a través de los cuales se sustentará el Plan de Contingencia.

Dicho comité estará integrado por los siguientes miembros:

- Director Administrativo
- Director Médico
- Responsable de la Unidad de Informática
- Otros que el Director Administrativo considere pertinente incluir

Funciones y Roles del Comité del Plan de Contingencia:

- Participar en las reuniones periódicas propuestas por el Coordinador del Plan de Contingencia.
- Proponer la incorporación y/o modificaciones del Plan de contingencia.

- Aprobar y/o rechazar las incorporaciones y/o modificaciones del Plan de Contingencia propuesta por el coordinador de contingencia o sus miembros.
- Verificar que el personal a su cargo se encuentre debidamente capacitado en la ejecución del plan de contingencia.
- Coordinar la ejecución de las actividades del plan de pruebas.
- Aprobar los informes presentados por la coordinación del plan respecto a cualquier evento relacionado con el mismo.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.
- Coordinar con los recursos y/o proveedores externos necesarios para soportar y restaurar los servicios afectados por la contingencia.
- Coordinar y ejecutar la capacitación al personal nuevo del servicio sobre las actividades que deben ejecutar cuando se presenta la contingencia.

Coordinación Ejecutora del Plan

La Coordinación ejecutora del Plan de Contingencia será responsabilidad del Responsable de la Unidad de Informática, definiendo todas las políticas y acciones a llevarse a cabo durante un evento de contingencia, también será responsable de que todas las actividades se cumplan de acuerdo a lo planeado. Dicha coordinación será asistida y ejecutada en colaboración del responsable del Área de Mantenimiento y/o de los coordinadores de otros servicios.

Funciones y Roles de la Coordinación Ejecutora del Plan:

- Mantener permanentemente actualizado el Plan de Contingencia.
- Responsable de la ejecución del plan de contingencia, cuando se presenten los eventos que lo activan.
- Evaluar el impacto de las contingencias que se presenten.
- Elaborar los informes referidos al Plan de contingencias
- Proponer incorporaciones de eventos al plan de contingencia al Comité de Contingencia.
- Proponer la capacitación al personal nuevo del servicio, sobre las actividades que deben ejecutar cuando se presente la contingencia.
- Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el plan de contingencia.
- Proponer reuniones periódicas sobre el plan de contingencia.

Contraloría del Plan de Contingencia

La Oficina de Auditoría Interna o a falta de esta quien designe el Director Administrativo, sería el órgano que supervise todos los elementos y recursos descritos para intervenir en una situación de contingencia estén disponibles y sean perfectamente viables de modo tal que se garantice que no se presenten carencias y/o fallas en una situación real bajo las Funciones y Roles siguientes:

- Verificar que el plan de contingencia se encuentre actualizado.

- Revisar y verificar que el documento de plan de contingencia se enmarque dentro del alcance establecido.
- Velar por suministrar los recursos necesarios para la viabilidad del plan de Contingencia y Seguridad.
- Corroborar que el plan de contingencia se cumpla correctamente.
- Presentar los informes del Plan de Contingencia al Comité de Contingencia del Hospital Básico del IESS Guaranda.
- Certificar que todos los recursos descritos en el Plan de Contingencia (materiales, humanos, externos, etc.) sean viables y se encuentren disponibles para su uso cuando un evento de contingencia lo requiera.
- Auditar los procesos que forman parte del Plan de Contingencia, corroborando que se cumpla correctamente. Participar y visar las pruebas de validación del Plan de Contingencia. Informar al Comité respecto a cualquier evento o anomalía encontrada que ponga en riesgo la ejecución de todo o parte del plan.
- Proponer y recomendar actividades o procesos de mejora que permitan minimizar los riesgos de operación.

3.2. Identificación y Priorización de Riesgos

Denominamos **INCIDENCIA** al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

Riesgo: Es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.

Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la *probabilidad, impacto y exposición* del riesgo. Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio. Asimismo, la probabilidad debe ser inferior a “1” o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

Condiciones definidas para la escala de Probabilidad del Riesgo:

- Insignificante de 0 a 0.10
- Mínima de 0.11 a 0.30
- Media de 0.31 a 0.50
- Alta de 0.51 a 0.70
- Muy Alta de 0.71 a 0.90

Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia.

Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto. Para nuestro caso, clasificaremos el impacto con una escala numérica del 1 al 4.

Exposición al Riesgo

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

Definición de eventos controlables y no controlables

Como parte de la identificación de los riesgos, estos deben categorizarse en función a las acciones de prevención que pueden estar en manos del hospital, o cuya ocurrencia no puede predecirse con antelación. Así tenemos que los eventos pueden ser:

- **Eventos Controlables**, si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.
- **Eventos No Controlables**, cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.

Esta identificación se hará en la matriz de riesgo explicada a continuación.

Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy objetivos en su análisis. El factor numérico asignado es directamente proporcional y va en ascenso con respecto al impacto o gravedad que su ocurrencia pueda generar sobre los diferentes alcances del servicio y se clasificarán como se indica en el cuadro N° 1.

Cuadro N °1: Cuadro de Impactos

IMPACTO	DESCRIPCION	VALOR
Poco Impacto	Pérdida de Información y/o equipamiento no Sensitivo	1
Moderado Impacto	Pérdida de información sensible	2
Alto Impacto	Pérdida de información sensible, retraso o interrupción	3
Gran Impacto	Información crítica, daño serio, patrimonial	4

Cuadro N °2: Cuadro de Probabilidad de Ocurrencia

PROBALIDAD DE OCURRENCIA	DESCRIPCION
Frecuente	Incidentes repetidos
Probable	Incidentes aislados

Ocasional	Sucede alguna vez
Remoto	Improbable que suceda

Así mismo, la probabilidad de ocurrencia de un evento resulta de gran importancia para determinar qué tan posible es que dicho evento se presente en la realidad. La determinación de esta probabilidad se obtendrá de la estadística recogida de los eventos que se hayan presentado a lo largo de la administración del servicio por otros proveedores, así como la información obtenida de otros planes de contingencia para servicios similares.

Exposición = Impacto X Probabilidad

Cuadro N°3: Exposición al Riesgo

		Poco	Moderado	Alto	Gran
Probabilidad de ocurrencia	**Frecuente**				
	Probable				
	Ocasional				
	Remoto				
		Impacto			

Finalmente, después de haber ponderado y validado objetivamente las probabilidades de ocurrencia y los impactos asociados, se establecerán las políticas que se han de considerar para determinar cuáles son aquellos eventos que formarán parte del Plan de Contingencia, como sigue:

- Todo evento cuya calificación sea de “Gran Impacto: 4”, será considerado obligatoriamente dentro del Plan de Contingencia.
- Todo evento cuya exposición al riesgo sea mayor o igual a 0.15 será también considerado en el Plan de Contingencia (ver Cuadro N °4).

Después de todo lo expuesto, se elaborará la “Matriz de Riesgo de Contingencia” en la cual se tendrá en cuenta todos los eventos susceptibles de entrar en contingencia, indicando su ponderación y categorización (controlable/ no controlable) para la elaboración del Plan de Contingencia. Así mismo, se utilizarán los siguientes tópicos como una forma de agrupar a dichos eventos:

- Contingencias relacionadas a Siniestros
- Contingencias relacionadas a los Sistemas de Información
- Contingencias relacionadas a los Recursos Humanos
- Plan de Seguridad Física

3.3. Definición de eventos susceptibles de contingencia

El Plan de Contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos, que serán considerados para su evaluación son los siguientes:

- **Hardware**
  - ✓ Servidores
  - ✓ Estaciones de trabajo(laptops y PC´s)

- ✓ Impresoras, fotocopiadoras, scanner
- ✓ Equipos multimedia

- **Comunicaciones**
  - ✓ Equipos de comunicaciones switch y conectores RJ-45
  - ✓ Equipo de comunicaciones Router y LAN.
  - ✓ Equipo de Telefonía fija
  - ✓ Enlaces de cobre y fibra óptica.
  - ✓ Cableado de Red de Datos.
- **Software**
  - ✓ Software de Base de Datos.
  - ✓ Aplicativos utilizados por el Hospital (SIH - DATALAB).
  - ✓ Software Base (Sistemas operativos y Ofimática).
  - ✓ Antivirus para protección de servidores y estaciones de trabajo.
- **Información sobre Sistemas Informáticos**
  - ✓ Respaldo de información generada con Software Base y de Ofimática.
  - ✓ Respaldo de las Aplicaciones utilizadas por el Hospital.
  - ✓ Respaldos de Base de Datos.
  - ✓ Respaldos de información y configuración de los Servidores.
- **Equipos diversos**
  - ✓ Grupo electrógeno
  - ✓ UPS
- **Infraestructura Física**
  - ✓ Oficinas y consultorios del Hospital.
- **Operativos**
  - ✓ Logística operativa (suministros Informáticos).
- **Servicios Públicos**
  - ✓ Suministro de Energía Eléctrica.
  - ✓ Servicio de Telefonía Fija analógico/digital.
  - ✓ Suministro de Agua.
- **Recursos Humanos**
  - ✓ Disponibilidad de personal de dirección.
  - ✓ Disponibilidad de personal operativo.

3.4. Elaboración de los Planes de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento por el personal del Hospital Básico del IESS Guaranda.

Es por ello, que una fase importante de la metodología considera un formato estándar de registro de todos los eventos definidos que forman parte del plan, así se tendrá finalmente un entregable acorde con los requerimientos y políticas definidas para tal fin.

El contenido de todos los eventos que conformarán el Plan de Contingencia son:

Formato de Registro del Plan de Contingencia

Para una lectura fácil y rápida del Plan de Contingencia, se ha diseñado un formato, Ver Anexo A02: "Formato Registro Plan de Contingencia", el mismo que describimos a continuación y que se compone de las siguientes partes:

Encabezado:

El formato tiene un encabezado, cuyo contenido se presenta como sigue:

Elaborado: En todos los casos se indica "HOSPITAL BÁSICO DEL IESS GUARANDA".

Código del Formato: FPC – XX (ver matriz de riesgo de Contingencia).

Nombre del evento: Claro y de fácil entendimiento.

Cuerpo Principal

En el cual se desarrollará cada uno de los eventos que formarán parte del Plan de Contingencia y se describe el contenido que deberá ir en cada campo.

3.5. Definición y ejecución del plan de pruebas

Conscientes que una situación de contingencia extrema puede presentarse en cualquier momento, y por ende convertirse en un problema prioritario de atender si éste se produjera en el horario de oficina que pueda resultar impactante durante las actividades del Hospital; es que se hace necesario definir de manera específica todas las acciones necesarias para asegurar que, en caso real de contingencia tener un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de recuperación de manera rápida y segura.

En este sentido, la garantía del "éxito" del Plan de Contingencia se basa en una validación y certificación anticipada del mismo, en cada uno de sus procesos.

Alcance y Objetivos

Dado que la mayor parte de los planes de contingencia están orientados a temas de Siniestros, Seguridad y Recursos Humanos, cuyas situaciones son imposibles de reproducir en la vida real (Ej.: terremotos, robos, accidentes, problemas logísticos, etc.), es que el plan de pruebas estará enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

En este contexto previo, podemos precisar los siguientes objetivos a alcanzar en la realización de las pruebas:

- Programar la prueba y validación de todas las actividades que se llevarán a cabo como parte del Plan de Ejecución del Plan de Contingencia respecto a una posible interrupción de los procesos identificados como críticos para el servicio del Hospital Básico del IESS Guaranda.
- Identificar por medio de la prueba, las posibles causas que puedan atentar contra su normal ejecución y las medidas correctivas a aplicar para subsanar los errores o deficiencias que se deriven de ella (retroalimentación del plan).

- Determinar los roles y funciones que cumplirán los responsables en la prueba, los mismos que serán los asignados para su ejecución en caso de una situación real de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por un grupo determinado de usuarios de las diferentes direcciones y coordinaciones del Hospital, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

OBJETIVOS DE LA PRUEBA DEL PLAN DE CONTINGENCIA
Definición Objetivos
ALCANCES
Áreas Afectadas (relación)
Personal involucrado (relación)
DESCRIPCIÓN DE LA PRUEBA A EFECTUARSE
Evaluación de una situación de Emergencia
Medios disponibles para operar
Fechas y horas
RESULTADOS ESPERADOS DE LAS PRUEBAS
Relación de posibles acciones

Validación y Registro de Pruebas

Todas las actividades generales que forman parte de la prueba, deberán validarse, registrarse (incluyendo observaciones) y firmarse por todos los responsables que participaron en cada una de ellas, a fin de dar fe de su ejecución y certificación.

En el Anexo A03 “Control y Certificación de Pruebas de Contingencia” se muestra el formato que se usará para la validación y registro de dichas pruebas, así como el detalle de la información que deberá ser ingresada en cada campo.

3.6. Implementación del Plan de Contingencia

La implementación del presente plan se realizará en el segundo mes de su aprobación.

4. DESARROLLO DE LAS FASES, ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS

4.1. Fases

Como parte del presente capítulo, la Unidad de Informática, plantea el desarrollo de los tópicos, utilizando la metodología expuesta anteriormente. Este desarrollo incluirá las siguientes fases de la metodología:

- Identificación y Priorización de riesgos
- Definición de Eventos susceptibles de Contingencia.
- Elaboración del Plan de Contingencia.

Identificación y Priorización de Riesgos

El cuadro N° 4 se muestra la matriz de Riesgo de Contingencia, ponderado de acuerdo a los valores de riesgo e impacto en el servicio (operatividad), usando el conocimiento y la experiencia práctica del responsable de Informática en Gestión de Sistemas de Información:

Cuadro N° 4: Matriz de Riesgo de Contingencia

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta	Categoría
	Sub Factor. Riesgos relacionadas a Siniestros					
	INFRAESTRUCTURA					
1	Incendio	0.4	4	1.6		**C**
2	Sismo	0.39	4	1.56		**NC**
3	Inundación por desperfecto de los servicios sanitarios	0.2	1	0.2		**C**
	SERVICIOS PÚBLICOS					
4	Interrupción de energía eléctrica	0.5	4	2.0		**NC**
5	Falta de suministro de agua	0.1	3	0.3		**NC**
6	Interrupción de servicios de telefonía	0.1	3	0.3		**NC**
	EQUIPO					
7	Falla de generador eléctrico	0.05	4	0.20		**C**
	Sub Factor. Riesgos relacionadas a Sistemas de Información					
	INFORMACIÓN					
8	Extravío de documentos	0.2	3	0.6		**C**
9	Sustracción o robo de información	0.2	3	0.6		**C**
	SOFTWARE					
10	Infección de equipos por virus	0.7	4	2.8		**C**
11	Perdidas de los sistemas centrales	0.5	4	2.0		**C**
12	Perdida del servicio de correo	0.1	2	0.2		**C**
13	Falla del Motor de la base de datos	0.4	4	1.6		**C**
14	Falla del sistema operativo	0.4	4	1.6		**C**
	COMUNICACIONES					
15	Fallas en la red de comunicaciones interna	0.2	4	0.8		**C**
16	Falla en el enlace de datos (CNT)	0.6	4	2.4		**C**
	HARDWARE					
17	Fallas de equipos personales	0.2	2	0.4		**C**
	RECURSO OPERATIVOS Y LOGÍSTICOS					
18	Falla de equipos multimedia, impresoras, scanner y otros	0.1	2	0.2		**C**
	Sub factor: Riesgos relacionadas a recursos humanos					
	RECURSO HUMANO					
19	Ausencia imprevista del personal de soporte técnico	0.5	3	1.5		**C**
20	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	0.5	3	1.5		**C**

21	Falta de idoneidad del personal en la reserva de información de la Base de Datos.	0.1	4	0.4		**NC**
Sub factor: Plan de seguridad Física						
	INFRAESTRUCTURA					
22	Sustracción de equipos y software diversos	0.2	2	0.4		**C**
23	Sabotaje	0.1	2	0.2		**NC**
24	Vandalismo	0.1	3	0.3		**NC**
25	Actos terroristas	0.1	4	0.4		**NC**

Nota: El color rojo de la alerta representa que el evento es altamente impactante en el servicio por lo tanto debe ser obligatoriamente controlado.

En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (C), y No Controlables (NC).

En los cuadros N° 5 y N° 6 se resumen los eventos según la categorización de eventos controlables y no controlables:

Cuadro N °5: Eventos Controlables

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta
1	Incendio	0.4	4	1.6	
3	Inundación por desperfecto de los servicios sanitarios	0.2	1	0.2	
7	Falla de generador eléctrico	0.5	4	2.0	
8	Extravío de documentos	0.2	3	0.6	
9	Sustracción o robo de información	0.2	3	0.6	
10	Infección de equipos por virus	0.7	4	2.8	
11	Perdidas de los sistemas centrales	0.5	4	2.0	
12	Perdida del servicio de correo	0.1	2	0.2	
13	Falla del Motor de la base de datos	0.4	4	1.6	
14	Falla del sistema operativo	0.4	4	1.6	
15	Fallas en la red de comunicaciones interna	0.2	4	0.8	
16	Falla en el enlace de datos (CNT)	0.6	4	2.4	
17	Fallas de equipos personales	0.2	2	0.4	
18	Falla de equipos multimedia, impresoras, scanner y otros	0.1	2	0.2	
19	Ausencia imprevista del personal de soporte técnico	0.5	3	1.5	
20	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	0.5	3	1.5	
22	Sustracción de equipos y software diversos	0.2	2	0.4	

Cuadro N °6: Eventos no Controlables

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta
2	Sismo	0.39	4	1.56	
4	Interrupción de energía eléctrica	0.5	4	2.0	
5	Falta de suministro de agua	0.1	3	0.3	
6	Interrupción de servicios de telefonía	0.1	3	0.3	
21	Falta de idoneidad del personal en la reserva de información de la Base de Datos.	0.1	4	0.4	
23	Sabotaje	0.1	2	0.2	
24	Vandalismo	0.1	3	0.3	
25	Actos terroristas	0.1	4	0.4	

Definición de Eventos susceptibles de Contingencia

Una vez identificados los eventos de contingencia, presentamos el cuadro N° 7 “Elementos VS. Subfactores”, donde se muestra la relación existente entre los elementos mínimos definidos por la Unidad de Informática, haciendo una referencia de todos los Planes de Contingencia relacionados al mismo e indicando a que subfactor desarrollado pertenecen.

Cuadro N° 7: Elementos Vs. Subfactores a desarrollar

ELEMENTO	PLAN DE CONTINGENCIAS DESARROLLADO		
	CÓDIGO	ALCANCE	SUBFACTOR / CONTINGENCIA
Hardware			
Servidores	FPC-04	Servicios Públicos	Siniestros
	FPC-07	Equipo	Siniestros
	FPC-09	Información	Sistemas de Información
	FPC-10	Software	Sistemas de Información
	FPC-11	Software	Sistemas de Información
	FPC-13	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
	FPC-23	Infraestructura	Plan de Seguridad Física
Estaciones de trabajo(laptops y PC´s)	FPC-04	Servicios Públicos	Siniestros
	FPC-07	Equipo	Siniestros
	FPC-08	Información	Sistemas de Información
	FPC-10	Software	Sistemas de Información
	FPC-12	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
	FPC-15	Comunicaciones	Sistemas de Información
	FPC-16	Comunicaciones	Sistemas de Información
	FPC-17	Comunicaciones	Sistemas de Información
	FPC-24	Infraestructura	Plan de Seguridad Física
	FPC-25	Infraestructura	Plan de Seguridad Física
Impresoras, fotocopiadoras, scanner y/o Equipos multimedia	FPC-18	Rec. Operativo y logístico	Sistemas de Información
Comunicaciones			
Equipos de comunicaciones switch y conectores RJ-45	FPC-15	Comunicaciones	Sistemas de Información
Equipo de comunicaciones Router y LAN.	FPC-15	Comunicaciones	Sistemas de Información
	FPC-16	Comunicaciones	Sistemas de Información
Equipo de Telefonía fija	FPC-15	Comunicaciones	Sistemas de Información
Enlaces de cobre y fibra óptica.	FPC-16	Comunicaciones	Sistemas de Información
Cableado de Red de Datos.	FPC-15	Comunicaciones	Sistemas de Información
Software			
Software de Base de Datos	FPC-13	Software	Sistemas de Información
	FPC-15	Comunicaciones	Sistemas de Información
	FPC-16	Comunicaciones	Sistemas de Información
Aplicativos utilizados por el Hospital.	FPC-08	Información	Sistemas de Información
	FPC-09	Información	Sistemas de Información
	FPC-10	Software	Sistemas de Información
	FPC-11	Software	Sistemas de Información
	FPC-13	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
	FPC-15	Comunicaciones	Sistemas de Información
	FPC-16	Comunicaciones	Sistemas de Información
Software Base (Sistemas operativos y Ofimática).	FPC-14	Software	Sistemas de Información
	FPC-15	Comunicaciones	Sistemas de Información
Antivirus para protección de servidores y estaciones de trabajo.	FPC-11	Software	Sistemas de Información
	FPC-12	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
	FPC-15	Comunicaciones	Sistemas de Información
	FPC-16	Comunicaciones	Sistemas de Información

Información sobre Sistemas Informáticos			
Respaldo de información generada con Software Base y de Ofimática.	FPC-11	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
Respaldo de las Aplicaciones utilizadas por el Hospital.	FPC-11	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
Respaldos de Base de Datos.	FPC-11	Software	Sistemas de Información
	FPC-13	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
Respaldos de información y configuración de los Servidores	FPC-13	Software	Sistemas de Información
	FPC-14	Software	Sistemas de Información
Equipos diversos			
Grupo Electrógeno	FPC-07	Equipo	Siniestros
UPS	FPC-04	Servicios Públicos	Siniestros
Infraestructura Física			
Oficinas y consultorios del Hospital.	FPC-01	Infraestructura	Siniestros
	FPC-02	Infraestructura	Siniestros
	FPC-03	Infraestructura	Siniestros
	FPC-24	Infraestructura	Plan de Seguridad Física
	FPC-25	Infraestructura	Plan de Seguridad Física
Servicios Públicos			
Suministro de Energía Eléctrica.	FPC-04	Servicios Públicos	Siniestros
Servicio de Telefonía Fija analógico/digital.	FPC-06	Servicios Públicos	Siniestros
Suministro de Agua.	FPC-05	Servicios Públicos	Siniestros
Recursos Humanos			
Disponibilidad de personal de dirección.	FPC-20	Recurso Humano	Recursos Humanos
	FPC-21	Recurso Humano	Recursos Humanos
	FPC-23	Infraestructura	Plan de Seguridad Física
	FPC-24	Infraestructura	Plan de Seguridad Física
Disponibilidad de personal operativo.	FPC-19	Recurso Humano	Recursos Humanos
	FPC-20	Recurso Humano	Recursos Humanos
	FPC-21	Recurso Humano	Recursos Humanos
	FPC-23	Infraestructura	Plan de Seguridad Física
	FPC-24	Infraestructura	Plan de Seguridad Física

Elaboración del Plan de Contingencia

Una vez identificados los eventos de contingencia y los elementos considerados afectados o causantes de los mismos, pasamos a desarrollar los Planes de Contingencia agrupados por los Subfactores.

A manera de resumen, presentamos un flujo general que explica la forma de responder ante la ocurrencia de un evento de contingencia:

Los cuadros siguientes muestran los funcionarios responsables de cada evento de contingencia identificado:

Ítem	Descripción del Evento de Contingencia	Responsable(s) Titulares o sus Representantes	Teléfonos
Sub Factor. Riesgos relacionadas a Siniestros			
FPC-01	Incendio	Director Administrativo. Director Médico.	03 2980 239
FPC-02	Sismo	Director Administrativo. Sistemas	03 2980 239

FPC-03	Inundación por desperfecto de los servicios sanitarios	Director Administrativo. Mantenimiento Sistemas	03 2980 239
FPC-04	Interrupción de energía eléctrica	Director Administrativo. Mantenimiento. Sistemas.	03 2980 239
FPC-05	Falta de suministro de agua	Director Administrativo. Mantenimiento	03 2980 239
FPC-06	Interrupción de servicios de telefonía	Director Administrativo. Mantenimiento Sistemas	03 2980 239
FPC-07	Falla del Grupo Electrógeno	Director Administrativo. Mantenimiento. Sistemas	03 2980 239
Sub Factor. Riesgos relacionadas a Sistemas de Información			
FPC-08	Extravío de documentos	Director Administrativo. Director Médico. Sistemas	03 2980 239
FPC-09	Sustracción o robo de información	Director Administrativo. Director Médico. Sistemas	03 2980 239
FPC-10	Infección de equipos por virus	Sistemas	03 2980 239
FPC-11	Perdidas de los sistemas centrales	Sistemas	03 2980 239
FPC-12	Perdida del servicio de correo	Sistemas	03 2980 239
FPC-13	Falla del Motor de la base de datos	Sistemas	03 2980 239
FPC-14	Falla del sistema operativo	Sistemas	03 2980 239
FPC-15	Fallas en la red de comunicaciones interna	Sistemas	03 2980 239
FPC-16	Falla en el enlace de datos (CNT)	Sistemas	03 2980 239
FPC-17	Fallas de equipos personales	Sistemas	03 2980 239
FPC-18	Falla de equipos multimedia, impresoras, scanner y otros	Sistemas	03 2980 239
Sub factor: Riesgos relacionadas a recursos humanos			
FPC-19	Ausencia imprevista del personal de soporte técnico	Director Administrativo. Director Médico. Talento Humano. Sistemas	03 2980 239
FPC-20	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	Director Administrativo. Director Médico. Talento Humano. Sistemas.	03 2980 239
FPC-21	Falta de idoneidad del personal en la reserva de información de la Base de Datos.	Director Administrativo. Director Médico. Talento Humano. Sistemas.	03 2980 239
Sub factor: Plan de seguridad Física			
FPC-22	Sustracción de equipos y software diversos	Director Administrativo. Sistemas	03 2980 239
FPC-23	Sabotaje	Director Administrativo. Director Médico.	03 2980 239
FPC-24	Vandalismo	Director Administrativo. Director Médico.	03 2980 239
FPC-25	Actos terroristas	Director Administrativo. Director Médico.	03 2980 239

Los siguientes puntos de este capítulo, tratarán del desarrollo de los Planes de Contingencia por cada Sub Factor identificado, utilizando el formato anexo A02

4.2. Desarrollo de las Actividades

Subfactor: Contingencias relacionadas a siniestros

Siniestro: Se entiende por Siniestro a las emergencias originadas por la naturaleza (sismos, inundaciones, erupciones volcánicas, deslizamientos, entre otros), y aquellas producidas por causas no controlables tales como choques eléctricos, explosiones, derrames, etc.

A continuación se indica los puntos a desarrollarse para el presente subfactor:

Objetivo

Incluir en el Plan de Contingencia todos los eventos relacionados a siniestros que permitan proveer de un conjunto de acciones destinadas a planificar, organizar, preparar, controlar y mitigar una emergencia que se presente en las instalaciones, con la finalidad de reducir al mínimo las posibles consecuencias humanas y operativas TIC que pudieran derivarse de la misma.

Alcance

El alcance está circunscrito a los eventos de contingencia o emergencias que pudieran afectar, paralizar o dañar las instalaciones, el personal o los recursos TIC's. Una consideración adicional a tenerse en cuenta ante la ocurrencia de un siniestro que inhabilite total o parcialmente el "Centro de Datos", es la coordinación que debe realizarse con la alta Dirección del Hospital para determinar el uso de un ambiente alterno para la continuidad de la operación, hasta que se restablezca el funcionamiento normal.

Por otro lado, consideramos que como parte del desarrollo del subfactor de Siniestros, se debe incluir los elementos relativos a Servicios Públicos, por afectar o ser consecuencia de siniestros que pueden presentarse:

Interrupción de Energía Eléctrica; al momento de restablecerse la energía eléctrica, pudiera realizarse con cargas altas que pudieran ocasionar algún tipo de siniestros, afectando la seguridad física.

El siguiente cuadro es un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Siniestros:

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta
Sub Factor. Riesgos relacionadas a Siniestros					
	INFRAESTRUCTURA				
FPC-01	Incendio	0.4	4	1.6	
FPC-02	Sismo	0.39	4	1.56	
FPC-03	Inundación por desperfecto de los servicios sanitarios	0.2	1	0.2	
	SERVICIOS PÚBLICOS				
FPC-04	Interrupción de energía eléctrica	0.5	4	2.0	
FPC-05	Falta de suministro de agua	0.1	3	0.3	
FPC-06	Interrupción de servicios de telefonía	0.1	3	0.3	
	EQUIPO				
FPC-07	Falla de generador eléctrico	0.5	4	2.0	

Plan de pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del Subfactor Siniestros, seguirá la metodología expuesta en el punto 5.5 del Plan de Contingencia.

El plan de pruebas se determinará luego del análisis de los procesos críticos del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por el Comité de Contingencias de Pruebas previamente a su ejecución.

Descripción de Planes

Se detallarán los Planes de Contingencia de los eventos de mayor impacto identificados en la Matriz de Riesgo de Contingencia.

Hospital Básico del IESS Guaranda	**Evento: Incendio**		**FPC-01 Versión: 1.1**
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros. Este evento incluye los siguientes elementos mínimos identificados por el Hospital Básico del IESS Guaranda, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:

- "Centro de Datos" ubicado en la Oficina de Sistemas.
- "Cuarto de Equipos" ubicado en el área de Estadística.

Recursos Humanos:

- Personal debidamente entrenado para afrontar el evento

b) Objetivo

Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones del Hospital sin exponer la seguridad de las personas.

c) Criticidad

Se determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

Este evento se puede dar en las instalaciones del Hospital IESS Guaranda ubicadas en la Av. Augusto Chavez S/N y Vía a Ambato.

e) Personal Encargado

El Director y/o Coordinador de área de sistemas, es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Charlas sobre el uso y manejo de extintores de cada uno de los tipos.
- Acatar las indicaciones del COE institucional y cantonal, en torno al evento.
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del Hospital responsable de las acciones de prevención y ejecución de la contingencia.
- Igualmente se contará con los siguientes elementos para la detección y extinción de un posible incendio, los cuales cubrirán los ambientes del "Centro de Datos" y áreas afines a Informática
- Implementar detectores de humo en el "Centro de Datos"
- Implementación de la Central de detección de incendios
- Mantener actualizado los extintores

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- La Contingencia se activará al ocurrir un incendio.
- El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos Relacionados antes del evento.

- Identificar la ubicación de las estaciones manuales de alarma contra incendio.
- Identificar la ubicación de los extintores.
- Conocer el número de emergencia del COE del Hospital.

- Tener número de teléfono del personal responsable en seguridad Informática y contingencia del Hospital.
- Conocer el número de emergencia de los bomberos.

c) Personal que autoriza la contingencia.

El Director Administrativo o el personal de sistemas o sus Representantes pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable del Hospital Básico del IESS Guaranda.
- Evacuar el área.
- En todo momento se coordinará con el COE, para las acciones que deban ser efectuadas por ellos.

Luego de extinguido el incendio, se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados al personal, bienes e instalaciones.
- En caso de daños del personal prestar asistencia médica inmediata.
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
- La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Dirección del Hospital en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectado.

e) Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación es la Dirección Administrativa y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones del Hospital.

b) Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

c) Mecanismos de Comprobación

El Coordinador y/o Director del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

d) Mecanismos de Recuperación

Se efectuara de acuerdo a las instrucciones impartidas que se menciona en el punto a.

e) Desactivación del Plan de Contingencia

Director Administrativo o su representante desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

f) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el Director Administrativo y/o Director Científico luego de lo cual se determinará las acciones a tomar.

Hospital Básico del IESS Guaranda	Evento: Sismo		FPC-02 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por Hospital Básico del IESS Guaranda, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Infraestructura:

- Edificio del Hospital Básico del IESS Guaranda

Recursos Humanos

- Personal

b) Objetivo

Establecer las acciones que se tomarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del Hospital evitando exponer la seguridad de las personas.

c) Criticidad

El Hospital determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

Este evento se puede dar en las instalaciones del Hospital.

e) Personal Encargado

El Director y/o Coordinador del área, es quien debe de dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan

f) Condiciones de Prevención de Riesgo

- Contar con un plan de evacuación de las instalaciones del Hospital, el mismo que debe ser de conocimiento de todo el personal que labora.
- Realizar simulacros de evacuación con la participación de todo el personal del Hospital.
- Mantener las salidas libres de obstáculos.
- Señalizar todas las salidas.
- Señalizar las zonas seguras.
- Definir los puntos de reunión en caso de evacuación.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

Sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos Relacionados antes del evento.

- Tener la lista de los empleados por Servicios y/o Oficinas actualizada.
- Mantenimiento del orden y limpieza.
- Inspecciones trimestrales de seguridad interna.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c) Personal que autoriza la contingencia.

El Director Administrativo puede activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones del Director Administrativo y/o Director Médico utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las ventanas para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. En caso requerirse personal especializado, coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias.

- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo.
- En todo momento se coordinará con el personal de mantenimiento del Hospital, para las acciones que deban ser efectuadas por ellos.
- La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Dirección del Hospital en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectados.

e) Duración

- Los procesos de evacuación del personal del Hospital Básico del IESS Guaranda serán calmados y demorará 5 minutos como máximo.
- La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación es la Dirección y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Institución.

b) Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible la producción pendiente durante la interrupción del servicio.

c) Mecanismos de Comprobación

El Director y/o Coordinador del área afectada presentará un informe a la Coordinación Ejecutora del Plan explicando qué parte del Servicio u operaciones ha sido afectada y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El Director Administrativo y/o su delegado desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e) Proceso de Actualización

El proceso de actualización será en base al informe presentado para determinará las acciones a tomar.

Hospital Básico del IESS Guaranda	Evento: Interrupción de energía eléctrica		FPC-04 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos

- Suministro de Energía Eléctrica

Hardware:

- Servidores
- Estaciones de Trabajo

Equipos Diversos

- UPS

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Criticidad

Este evento se considera como CRITICO.

d) Entorno

Se puede producir durante la operatividad, afectando el fluido eléctrico de las instalaciones del Hospital Básico del IESS Guaranda.

e) Personal Encargado

El Director Administrativo y/o Coordinador de Informática del Hospital en coordinación con el responsable de mantenimiento son responsables de realizar las gestiones necesarias para restablecer el suministro de energía eléctrica.

f) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del Hospital Básico del IESS Guaranda se contará con los puntos eléctricos regulados mediante el UPS central, necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.
- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 30 minutos como máximo. El tiempo variará de acuerdo a la carga de equipos conectados al UPS.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Contar con puntos de red eléctrica regulada mediante UPS para proteger los servidores del Hospital, previniendo la pérdida de datos durante las labores.
- Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.
- Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

Corte de suministro de energía eléctrica en los ambientes del Hospital Básico del IESS Guaranda.

b) Procesos Relacionados antes del evento.

Cualquier actividad de servicio dentro de las instalaciones del Hospital.

c) Personal que autoriza la contingencia.

El Director Administrativo y/o Coordinador de Informática pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.

- Informar al Director Administrativo y/o Coordinador de Informática del problema presentado.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del Hospital y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores hasta que regrese el fluido eléctrico o se active el generador o planta eléctrica.

e) Duración
El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
El personal encargado del Plan de Recuperación son el Coordinador de Informática y/o el Director Administrativo, quienes se encargarán de realizar las acciones de recuperación necesarias en conjunto con el área de mantenimiento.

b) Descripción
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.
- Se informará a la Coordinación Ejecutora del Plan el problema presentado y el procedimiento usado para atender el problema.
- En función a esto, se tomarán las medidas preventivas del caso.

c) Mecanismos de Comprobación
El Director Administrativo y/o Coordinador de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d) Desactivación del Plan de Contingencia
El Director Administrativo y/o Coordinador de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

e) Proceso de Actualización
En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

Hospital Básico del IESS Guaranda	Evento: Falla del Grupo Electrógeno		FPC-07 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica proporcionado por el generador eléctrico.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos

- Suministro de Energía Eléctrica

Hardware:

- Servidores
- Estaciones de Trabajo

Equipos Diversos

- UPS
- Grupo Electrógeno.

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Criticidad

Este evento se considera como CRITICO.

d) Entorno

Se puede producir durante la operatividad, afectando el fluido eléctrico de las instalaciones del Hospital Básico del IESS Guaranda proporcionada por el Grupo Electrógeno en ausencia del servicio por parte del proveedor local.

e) Personal Encargado

El Director Administrativo y/o responsable de mantenimiento en coordinación con Informática son responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

f) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del Hospital se contará con los puntos eléctricos regulados mediante el UPS central necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.
- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 20 minutos como máximo en ausencia del generador eléctrico. El tiempo variará de acuerdo a la carga de equipos conectados al UPS.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Contar con puntos de red eléctrica regulada mediante UPS para proteger los servidores del Hospital, previniendo la pérdida de datos durante las labores.
- Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.
- Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

Falla en el grupo electrógeno que brinda el suministro de energía eléctrica en los ambientes del Hospital Básico del IESS Guaranda, en ausencia del servicio por parte del proveedor local.

b) Procesos Relacionados antes del evento.

Cualquier actividad de servicio dentro de las instalaciones del Hospital.

c) Personal que autoriza la contingencia.

El Director Administrativo y/o responsable de mantenimiento pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.

- Informar al Director Administrativo y/o responsable de mantenimiento del problema presentado.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del Hospital y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con el UPS central, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.

- En caso la falla del generador no se resuelva en un máximo de diez minutos, se deberán apagar los servidores hasta que regrese el fluido eléctrico o se reactive el Grupo Electrógeno.

e) Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica, o de la reactivación del generador.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación son el responsable de Mantenimiento y/o el Director Administrativo, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción

- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.
- Se informará a la Coordinación Ejecutora del Plan el problema presentado y el procedimiento usado para atender el problema.
- En función a esto, se tomarán las medidas preventivas del caso.

c) Mecanismos de Comprobación

El Director Administrativo y/o responsable de mantenimiento presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d) Desactivación del Plan de Contingencia

El Director Administrativo y/o responsable de mantenimiento desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

Subfactor: Contingencias relacionadas a los sistemas de información

A continuación se muestra los puntos a desarrollarse para el presente subfactor:

Objetivo

Los planes de contingencia de los eventos relacionados a los Sistemas de Información tienen por objetivo que ante cualquier evento que atente contra la normal operación tanto en hardware, software como en cualquier elemento interno o externo relacionado a los mismos, se dispongan de alternativas de solución frente al problema a fin de asegurar la operación del servicio y/o minimizar el tiempo de interrupción.

Alcance

El alcance de dichos planes se circunscribe a las actividades de uso de sistemas y/o aplicaciones, así como a las operaciones del servicio que son afectadas durante la operatividad del Hospital Básico del IESS Guaranda.

Resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Sistemas de Información que se describirán en detalle más adelante

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta
Sub Factor. Riesgos relacionadas a Sistemas de Información					
	INFORMACIÓN				
FPC-08	Extravío de documentos	0.2	3	0.6	
FPC-09	Sustracción o robo de información	0.2	3	0.6	
	SOFTWARE				
FPC-10	Infección de equipos por virus	0.7	4	2.8	
FPC-11	Perdidas de los sistemas centrales	0.5	4	2.0	
FPC-12	Perdida del servicio de correo	0.1	2	0.2	
FPC-13	Falla del Motor de la base de datos	0.4	4	1.6	
FPC-14	Falla del sistema operativo	0.4	4	1.6	
	COMUNICACIONES				
FPC-15	Fallas en la red de comunicaciones interna	0.2	4	0.8	
FPC-16	Falla en el enlace de datos (CNT)	0.6	4	2.4	
	HARDWARE				
FPC-17	Fallas de equipos personales	0.2	2	0.4	
	RECURSO OPERATIVOS Y LOGÍSTICOS				
FPC-18	Falla de equipos multimedia, impresoras, scanner y otros	0.1	2	0.2	

Plan de Pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del Sub Factor Sistemas de Información, seguirá la metodología expuesta en el punto 5.5 del Plan de Contingencia.

El plan de pruebas se determinará luego del análisis de los procesos críticos de las operaciones y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por el Comité de Contingencias de Pruebas previamente a su ejecución.

Descripción de Planes

Se detallarán los Planes de Contingencia de alguno de los eventos identificados en la Matriz de Riesgo de Contingencia.

Hospital Básico del IESS Guaranda	Evento: Infección de equipos por virus		FPC-10 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Virus informático es un programa de software que se propaga de un equipo a otro y que interfiere el funcionamiento del equipo. Además, Un virus informático puede dañar o eliminar los datos de un equipo.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores
- Estaciones de Trabajo

Software

- Software Base
- Aplicativos utilizados por el Hospital Básico del IESS Guaranda

b) Objetivo

Restaurar la operatividad de los equipos después de eliminar los virus o reinstalar las aplicaciones dañadas.

c) Criticidad

El nivel de éste evento es considerado CRITICO.

d) Entorno

Las estaciones de trabajo PC's, se encuentran instaladas en el edificio del Hospital Básico del IESS Guaranda.

e) Personal Encargado

Coordinador de Informática del Hospital es el responsable en la supervisión del correcto funcionamiento de las estaciones PC´s

f) Condiciones de Prevención de Riesgo

- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo, según lo dispone la DDI
- Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación de disketteras, quemadores de CD, etc. en estaciones de trabajo que no lo requieran.
- Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado y en comunicación permanentemente con el servidor EPO de McAfee localizado en la DDI por intermedio de la ejecución del agente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b) Procesos Relacionados antes del evento.

Cualquier proceso relacionado con el uso de las aplicaciones en las estaciones de trabajo.

c) Personal que autoriza la contingencia.

Coordinador de Informática o el Técnico de Soporte del Hospital.

d) Descripción de las actividades después de activar la contingencia.

- Desconectar la estación infectada de la red Institucional.
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- Eliminar el agente causante de la infección.
- Remover el virus del sistema.
- Probar el sistema.

- En caso no solucionarse el problema :
  - Formatear el equipo previo respaldo de la información del equipo.
  - Personalizar la estación para el usuario
- Conectar la estación a la red del Hospital Básico del IESS Guaranda.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio, mediante la firma del acta de mantenimiento del equipo.

e) Duración

La duración del evento no deberá ser mayor a VIENTE Y CUATRO HORAS en caso se confirme la presencia de un virus. Esperar la indicación del personal de soporte para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Técnico de Soporte de Sistemas, luego de restaurar el correcto funcionamiento de la estación de trabajo (PC), coordinará con el usuario responsable y/o Coordinador del área para reanudar las labores de trabajo con el equipo.

b) Descripción

- Se informará al Coordinador de Informática del Hospital el tipo de virus encontrado y el procedimiento usado para removerlo.
- En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal del Hospital Básico del IESS Guaranda.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c) Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la Coordinación Ejecutora del Plan para su revisión.

d) Desactivación del Plan de Contingencia

Con el aviso del Técnico de Soporte de Sistemas, se desactivará el presente Plan.

e) Proceso de Actualización

El problema de infección presentado en la estación de trabajo, no debe detener la Aplicación de actualización de datos en las Aplicaciones del Hospital.

Hospital Básico del IESS Guaranda	Evento: Perdida de los Sistemas Centrales		FPC-11 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Es la ausencia de interacción entre el Software y el Hardware haciendo inoperativa la máquina, es decir, el Software no envía instrucciones al Hardware imposibilitando su funcionamiento.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores

Software

- Software Base
- Software base de datos
- Aplicativos utilizados por el Hospital Básico del IESS Guaranda

Información

- Respaldo de base de datos
- Respaldo de las aplicaciones utilizadas por el Hospital Básico del IESS Guaranda
- Respaldo De Software Base

b) Objetivo

Mantener operativo los servidores de producción donde se ejecutan las aplicaciones del Hospital a nivel local.

c) Criticidad

El nivel de este evento es considerado crítico.

d) Entorno

Los servidores de aplicaciones están situados en el centro de datos del Hospital Básico del IESS Guaranda.

e) Personal Encargado

Coordinador de Informática del Hospital es el responsable de asegurar el correcto funcionamiento de los servidores durante los servicios. Se coordinarán las acciones necesarias para restablecer el servicio en caso se produzca el evento.

El responsable de Informática del Hospital es el encargado de coordinar las acciones necesarias con la DDI y el personal de las áreas usuarias, para asegurar un servicio continuo de los servidores y sus aplicaciones, de tal forma que no afecten el servicio brindado en el Hospital.

f) Condiciones de Prevención de Riesgo

Tomar las siguientes acciones preventivas que debe implementar la Unidad de Informática del Hospital para asegurar el servicio de las aplicaciones:

- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con mantenimiento preventivo para dichos equipos.
- Contar con los backups de información necesarios para restablecer las aplicaciones Anexo A04: Copias de Respaldo.
- Contar con backups de las aplicaciones y de las bases de datos Anexo A04: Copias de Respaldo.
- Almacenar en un lugar seguro los backups referidos a aplicaciones y datos. Se recomienda el almacenamiento de los backups en un lugar externo fuera de las instalaciones del Hospital.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Falla de Acceso a Aplicaciones.
- Mensaje Pérdida de Conexión a La BD.

b) Procesos Relacionados antes del evento.

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores del Hospital.

c) Personal que autoriza la contingencia.

Coordinador de Informática del Hospital.

d) Descripción de las actividades después de activar la contingencia.

Remitirse a los Procedimientos de recuperación de sistemas del Hospital.

e) Duración

La duración del evento estará en función de la complejidad del problema encontrado.
Esperar la indicación del Coordinador de Informática para reanudar la operación normal con las aplicaciones.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Coordinador de Informática del Hospital, luego de verificar la corrección del problema de acceso a los servidores, coordinará con los Directores y/o Coordinadores de áreas para la reanudación de los trabajos operativos con las aplicaciones del Hospital.

b) Descripción

Se informará a la Dirección la causa que motivó la paralización del servicio.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

d) Desactivación del Plan de Contingencia

Con el aviso del Coordinador de Informática, se desactivará el presente plan.

e) Proceso de Actualización

En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los Directores y/o Coordinadores de áreas, para iniciar las labores de actualización de los sistemas.

Hospital Básico del IESS Guaranda	Evento: Falla del motor de la Base de Datos		FPC-13 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Ausencia del servicio principal para almacenar, procesar y proteger los datos, para acceso controlado y procesamiento de transacciones de las aplicaciones locales del Hospital.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital Básico del IESS Guaranda, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados por el Hospital Básico del IESS Guaranda

Hardware

- Servidores

Información

- Respaldo de Base de Datos
- Respaldo del Software Base

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar los datos de las aplicaciones ejecutadas en los servidores locales.

c) Criticidad

Este evento se considera como CRITICO.

d) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del Hospital Básico del IESS Guaranda.

e) Personal Encargado

El Coordinador de Informática del Hospital encargará al responsable de la base de datos (DBA) las acciones correspondientes.

f) Condiciones de Prevención de Riesgo

- Revisión periódica de los logs de la BD para prevenir mal funcionamiento de la Base de Datos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción en la Institución. Se realizan copias de la información o de los registros con la finalidad de asegurar la información mantenida en la base de datos.
- La copia de seguridad de la información es un proceso diario, en donde se busca asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos de acuerdo a requerimientos antes o después de un determinado proceso Anexo A04: Copias de Respaldo.
- Mantener actualizado el software de gestión de BD, con todos los parches del producto según el fabricante del producto.
- Contar con servicios de soporte vigentes para el software de gestión de BD. En caso sea necesario, este soporte debe incluir actividades de prevención, revisión del sistema y mantenimiento general a la base de datos.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Fallas en la conexión. Indisponibilidad del sistema aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b) Procesos Relacionados antes del evento.

Respaldo disponible para el uso de las aplicaciones en los servidores del Hospital.

c) Personal que autoriza la contingencia.

El Coordinador de Informática es quien considera activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.

- Sistemas de Proveedores.- De producirse una falla al momento de la operación de estos sistemas por efecto del programa ejecutable (cliente) o base de datos, deberá ser comunicado y coordinado inmediatamente con el proveedor, para su corrección.
- Sistemas Desarrollados por el Hospital Básico del IESS Guaranda.- De producirse una falla al momento de la operación de estos sistemas, el Coordinador de Informática asumirá, delegará o coordinará los trabajos de corrección o modificación.

e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las CUATRO horas.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación para las operaciones del Hospital Básico del IESS Guaranda es el Coordinador de Informática.

b) Descripción

Se informará al Coordinador de Informática la causa del problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal del Hospital.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c) Mecanismos de Comprobación

El Coordinador de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d) Desactivación del Plan de Contingencia

El Coordinador de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con la BD de las aplicaciones.

e) Proceso de Actualización

En base al informe presentado que identifica las causas de la pérdida del sistema operativo en las estaciones de trabajo y/o servidores, se determinará las acciones de preventivas necesarias que deberán incluirse en el presente plan.

En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o Coordinadores de áreas, para iniciar las labores de actualización de los sistemas.

Hospital Básico del IESS Guaranda	Evento: Falla del sistema operativo		FPC-14 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla en el control de computadoras, en el interfaz hombre-máquina, recursos hardware y software del Hospital Básico del IESS Guaranda.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados por el Hospital.

Hardware

- Servidores

Información

- Respaldo de Base de Datos
- Respaldo de las Aplicaciones utilizadas por el Hospital.

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar las funciones de los elementos identificados.

c) Criticidad

Este evento se considera como CRITICO.

d) Entorno

Se puede producir durante la operatividad, afectando a las estaciones de trabajo y/o servidores de aplicaciones usados para dar soporte a las operaciones.

e) Personal Encargado

El Coordinador de Informática del Hospital es el responsable de coordinar las acciones necesarias para asegurar el correcto funcionamiento de las aplicaciones.

f) Condiciones de Prevención de Riesgo

Se debe asegurar de cubrir los siguientes aspectos:

- Contar con los backups de datos de las aplicaciones en producción en la institución Anexo A04: Copias de Respaldo.
- Contar con servicios de soporte vigentes para los principales causantes del evento:
- El Hospital debe asegurarse de mantener acuerdos con sus Proveedores de Servicio.
- Revisión periódica de los logs de actividad de los servidores para prevenir su mal funcionamiento.
- Estaciones de trabajo y servidores deberán contar con antivirus actualizados.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

Detención de las funciones de trabajo en estaciones de trabajo y/o servidores de aplicaciones.

Identificación de falla en el monitor de los servidores de aplicaciones y/o estaciones de trabajo.

b) Procesos Relacionados antes del evento.

Respaldo disponible de los sistemas operativos para la ejecución de las aplicaciones en los servidores.

c) Personal que autoriza la contingencia.

El Coordinador de Informática del Hospital es quién considera activar la contingencia

d) Descripción de las actividades después de activar la contingencia.

En el caso de las estaciones de trabajo :

- Proceder a la revisión de la estación de trabajo para determinar la causa de la falla.
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- Remover el virus del sistema.
- Probar el sistema.

En caso no solucionarse el problema :

- Formatear el equipo
- Personalizar la estación para el usuario
- Conectar la estación a la red del institucional.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

En el caso de los servidores de aplicaciones :

- Reportar el problema al área de soporte Técnico.
- Coordinar las acciones a realizarse y el tiempo aproximado de interrupción del servicio.
- Comunicar a los directores y/o Coordinadores de áreas para que se tomen las acciones del caso y no se afecte en sus operaciones.

e) Duración

- El tiempo máximo de la contingencia no debe sobrepasar las CINCO horas

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación para las operaciones del Hospital Básico del IESS Guaranda es el Coordinador de Informática.

b) Descripción

- Se informará al Coordinador de Informática del Hospital la causa del problema presentado y el procedimiento usado para atender el problema.
- En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal del Hospital Básico del IESS Guaranda.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c) Mecanismos de Comprobación

El Coordinador de Informática del Hospital presentará un informe a la Coordinación Ejecutora del Plan, explicando que parte del Servicio ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d) Desactivación del Plan de Contingencia

El Coordinador de Informática del Hospital desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

e) Proceso de Actualización

En base al informe presentado que identifica las causas de la pérdida del sistema operativo en las estaciones de trabajo y/o servidores, se determinará las acciones de prevención a tomar.

En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, se coordinará con los directores y/o coordinadores de áreas, para iniciar las labores de actualización de los sistemas.

4. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del enlace de datos proporcionado por el proveedor.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados por el Hospital.
- Internet.

Hardware:

- Servidores.
- Estaciones de Trabajo.

Información

- Datos de las historias clínicas.
- Facturación.

b) Objetivo

Restaurar las funciones consideradas como críticas dentro del servicio informático.

c) Criticidad

Este evento se considera como CRITICO.

d) Entorno

Se puede producir durante la operatividad, afectando las telecomunicaciones en las instalaciones del Hospital Básico del IESS Guaranda y los servicios proporcionados desde Quito.

e) Personal Encargado

El Coordinador de Informática y/o Director Administrativo del Hospital son responsables de realizar las coordinaciones para restablecer el servicio.

f) Condiciones de Prevención de Riesgo

- Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.
- Contar con un enlace de datos de respaldo.

5. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

Corte de servicio de enlace de datos del Hospital Básico del IESS Guaranda.

b) Procesos Relacionados antes del evento.

Cualquier actividad de servicio dentro de las instalaciones del Hospital.

c) Personal que autoriza la contingencia.

El Director Administrativo y/o Coordinador de Informática pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.

- Informar al Director Administrativo y/o Coordinador de Informática del problema presentado.
- Dar aviso del corte del servicio a todas las áreas del Hospital y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.

e) Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo del enlace de datos.

6. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación son el Coordinador de Informática y/o el Director Administrativo, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción

- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

- Se informará a la Coordinación Ejecutora del Plan el problema presentado y el procedimiento usado para atender el problema.
- En función a esto, se tomarán las medidas preventivas del caso.

c) Mecanismos de Comprobación
El Director Administrativo y/o Coordinador de Informática presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d) Desactivación del Plan de Contingencia
El Director Administrativo y/o Coordinador de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

e) Proceso de Actualización
En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

Subfactor: Contingencias relacionadas a los Recursos Humanos

A continuación se muestra los puntos a desarrollarse para el presente subfactor:

Objetivo

El desarrollo de este tipo de contingencias está relacionado con todos los elementos y factores que pueden afectar y/o ser afectados por el personal del Hospital Básico del IESS Guaranda.

Alcance

La seguridad referida al personal se contemplará desde las etapas de selección del mismo e incluirá en los contratos y definiciones de puestos de trabajo para poder cumplir el objetivo de reducir los riesgos de:

- Actuaciones humanas
- Indisponibilidad por enfermedades
- Emergencias médicas
- Incapacidad temporal o permanente por accidentes
- Renuncias o ceses

Se deberá comprobar que las definiciones de puestos de trabajo contemplan todo lo necesario en cuanto las responsabilidades encomendadas.

A continuación se presenta un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los Recursos Humanos que se describirán en detalle más adelante:

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta
Sub factor: Riesgos relacionadas a recursos humanos					
	RECURSO HUMANO				
FPC-19	Ausencia imprevista del personal de soporte técnico	0.5	3	1.5	
FPC-20	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	0.5	3	1.5	
FPC-21	Falta de idoneidad del personal en la reserva de información de la Base de Datos.	0.1	4	0.4	

Plan de Pruebas

El plan de pruebas correspondiente a los eventos desarrollados como parte del tópico Recursos Humanos, seguirá la metodología expuesta en el punto 5.5 del Plan de Contingencia.

El plan de pruebas se determinará luego del análisis de los procesos críticos del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por la Alta Dirección del Hospital Básico del IESS Guaranda previamente a su ejecución.

Descripción de Planes

Se detallarán los Planes de Contingencia de los eventos identificados en la Matriz de Riesgo de Contingencia.

Hospital Básico del IESS Guaranda	**Evento: Ausencia imprevista del personal de soporte técnico**		**FPC-19 Versión: 1.1**
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Ausencias del personal de Soporte Técnico relevante (enfermedad, renuncias, ceses), en toma decisiones claves que garantice el normal funcionamiento de servidores y redes de la institución.
Este evento incluye los siguientes elementos mínimos identificados por el Hospital Básico del IESS Guaranda, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Recursos Humanos

- Personal

b) Objetivo

Asegurar la continuidad del Servicio Informático del Hospital.

c) Criticidad

El Hospital Básico del IESS Guaranda determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

Este evento se puede dar en las instalaciones del Hospital.

e) Personal Encargado

El Director Administrativo y/o Coordinador de Talento Humano en conjunto con el Coordinador de Informática es quién debe disponer se cumplan las Condiciones de Previsión de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales, por lo que se considera lo siguiente:

- Como primera prevención, el Coordinador de Informática en conjunto con Talento Humano se aseguraran en tener como mínimo a un profesional técnico en el área.
- Como segunda prevención, el Coordinador de Informática, se asegurará en capacitar al personal de soporte técnico con el fin que cumpla el perfil, conocimiento y capacidad para reemplazar la ausencia ante la presencia de este evento.
- Incluir como parte de las funciones del personal el comunicar anticipadamente la inasistencia a su centro de labores.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

Reporte de inasistencia del personal del departamento de Sistemas.
El proceso de contingencia se activa durante las DOS (02) HORAS iniciales del día.

b) Procesos Relacionados antes del evento.

Se podría dar por:

- Conocimiento del Coordinador de Talento Humano y/o de Informática por parte del reporte de inasistencia del Sistema de Control de Asistencia.
- Conocimiento del Coordinador de Talento Humano y/o de Informática por comunicación telefónica por parte del personal de Sistemas ausente o algún familiar.

c) Personal que autoriza la contingencia.
El Coordinador de Informática y/o de Talento Humano

d) Descripción de las actividades después de activar la contingencia.

- Confirmado la inasistencia del personal de Sistemas, el Coordinador de Informática asignará la responsabilidad al Asistente del área de soporte técnico capacitado para reemplazar en las funciones que el personal titular de soporte técnico poseía.
- El Coordinador de Informática solicitará al Director Administrativo del Hospital, el reemplazo del personal.

e) Duración
Máximo OCHO (08) horas. El fin del presente evento es la presencia del reemplazo que asume la responsabilidad; hasta que se confirme la presencia del personal de Sistemas en caso de renuncia u otras por fuerza mayor.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
El personal encargado del Plan de Recuperación es el Director Administrativo y/o Talento Humano, cuyo rol principal es asegurar el normal funcionamiento del Servicio Informático.

b) Descripción

- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

c) Mecanismos de Comprobación
El Coordinador de Informática y/o de Talento Humano presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio Informático ha sido afectado y cual son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El Director Administrativo y/o de Talento Humano desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e) Proceso de Actualización
En base al informe presentado por el Coordinador de Informática y/o de Talento Humano y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

Hospital Básico del IESS Guaranda	Evento: Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático		FPC-20 Versión: 1.1
Fecha: 01-03-2016	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Ausencias del personal de Dirección y/o Coordinaciones (enfermedad, renuncias, ceses), en toma de decisiones claves que garantice el normal funcionamiento de las actividades.

Este evento incluye los siguientes elementos mínimos identificados por el Hospital Básico del IESS Guaranda, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Recursos Humanos

- Personal

b) Objetivo

Asegurar la continuidad de las operaciones en las diferentes Direcciones y/o Coordinaciones del Hospital, evitando el quiebre en la cadena de mandos, a través de reemplazos de personal ejecutivos.

c) Criticidad

El Hospital determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

Este evento se puede dar en las instalaciones del Hospital Básico del IESS Guaranda.

e) Personal Encargado

El Director Administrativo y/o Director Médico, es quién debe de asegurarse de que se cumpla lo descrito en las Condiciones de Previsión de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo

- La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales que se presente a personal Direccional y/o de Coordinaciones, por lo que se considera lo siguiente:
- Como primera prevención, la Dirección asegurará en capacitar a un empleado con más de 5 años de experiencia en la Institución que cumpla el perfil, conocimiento y capacidad para reemplazar ante el evento.
- Incluir como parte de las funciones del personal en comunicar anticipadamente la inasistencia a su centro de labores, siempre y cuando se trate de ocasiones premeditadas.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Reporte de inasistencia de algún Director y/o Coordinador de área.
- El proceso de contingencia se activa durante las DOS HORAS iniciales del día.

b) Procesos Relacionados antes del evento.

Se podría dar por:

- Falta de decisión del Director y/o Coordinador de Área para aplicar soluciones ante algún inconveniente en las actividades u operaciones de su competencia, donde se detecte la ausencia.
- Reporte de Control de Asistencia referente a inasistencias.

c) Personal que autoriza la contingencia.

El encargado de autorizar el proceso de contingencia es el Director Administrativo y/o Director Médico.

d) Descripción de las actividades después de activar la contingencia.

- Confirmado la inasistencia del Director Administrativo, se coordinará el reemplazo con el Director Médico y/o Coordinador de Talento Humano del Hospital.
- Confirmado la inasistencia del Coordinador de área, el Director Administrativo coordinará con Talento Humano el reemplazo correspondiente.

e) Duración

- Máximo tres horas. El fin del presente evento es la presencia del reemplazo, o el empleado más antiguo que esté capacitado para que asuma la responsabilidad; hasta que se confirme la presencia del director y/o Coordinador de área o Nuevo Director y/o Coordinador de área en caso de renuncia u otras por fuerza mayor.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación es el Director y/o Coordinador de área o Nuevo director y/o Coordinador de área, cuyo rol principal es asegurar el normal funcionamiento de las operaciones del Hospital.

b) Descripción

- Regularización en las coordinaciones pendiente durante la ausencia.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

c) Mecanismos de Comprobación

El director y/o coordinador de área presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operaciones ha sido afectado y cual son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El Director Administrativo y/o Coordinador de Talento Humano desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

e) Proceso de Actualización

En base al informe presentado por el Director y/o Coordinador de Área y las causas identificadas en la operatividad, se determinará las acciones a tomar.

Subfactor: Contingencias relacionadas a Seguridad Física

A continuación se muestra los puntos a desarrollarse para el presente subfactor:

Objetivo

Definir acciones de prevención a fin de eliminar o mitigar riesgos de seguridad física tanto de las instalaciones como de todos los elementos que operan en su interior (equipos, documentación, mobiliario, etc.) por motivos de incidentes causados de manera intencional, eventual o natural y que puedan afectar las operaciones normales del servicio.

Alcance

Serán tomados en cuenta los siguientes elementos:

- Ubicación y disposición física
- Elementos de seguridad de los ambientes de trabajo
- Control de accesos de personal interno y externo al servicio
- Actos terroristas o de vandalismo que pudieran afectar infraestructura, personal o documentación.

A continuación se presenta un resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a la Seguridad Física que se describirán en detalle más adelante:

Ítem	Descripción del Riesgos	Probabilidad	Impacto	Ponderación	Alerta
Sub factor: Plan de seguridad Física					
	INFRAESTRUCTURA				
FPC-22	Sustracción de equipos y software diversos	0.2	2	0.4	
FPC-23	Sabotaje	0.1	2	0.2	
FPC-24	Vandalismo	0.1	3	0.3	
FPC-25	Actos terroristas	0.1	4	0.4	

Plan de Prueba

El plan de pruebas correspondiente a los eventos desarrollados como parte del Sub Factor Seguridad Física, seguirá la metodología expuesta en el punto 5.5 del Plan de Contingencia.

El plan de pruebas se determinará luego del análisis de los procesos críticos del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por la Dirección del Hospital Básico del IESS Guaranda previamente a su ejecución.

Descripción de Planes

Estos eventos de contingencia son menores a 0.15.

4.3. Estrategias

La estrategia aplicada para el presente Plan de Contingencia es contar con:

- Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas, desarrollados en el presente Plan de Contingencia.
- Se propone una organización para la gestión del Plan de Contingencia, el mismo que está desarrollado en el presente Plan "5.1 Organización".
- Tener desarrollado y documentado los principales eventos susceptibles planteados en el presente Plan de Contingencia "6.2 Desarrollo de las Actividades"

4.4. Programas

En el presente Plan de Contingencia se ha desarrollado un conjunto de ítems, eventos o programas que permitan añadir valor a los sub-factores que ha priorizado el Hospital Básico del IESS Guaranda. Un resumen de los ítems desarrollados son los siguientes:

Ítem	Descripción del Riesgos	Alcance
Sub Factor. Riesgos relacionadas a Siniestros		
FPC-1	Incendio	INFRAESTRUCTURA
FPC-2	Sismo	INFRAESTRUCTURA
FPC-4	Interrupción de energía eléctrica	SERVICIOS PÚBLICOS
FPC-7	Falla de generador eléctrico	EQUIPO
Sub Factor. Riesgos relacionadas a Sistemas de Información		
FPC-10	Infección de equipos por virus	SOFTWARE
FPC-11	Perdidas de los sistemas centrales	SOFTWARE
FPC-12	Perdida del servicio de correo	SOFTWARE
FPC-13	Falla del Motor de la base de datos	SOFTWARE
FPC-14	Falla del sistema operativo	SOFTWARE
FPC-16	Falla en el enlace de datos (CNT)	COMUNICACIONES
Sub factor: Riesgos relacionadas a recursos humanos		
FPC-19	Ausencia imprevista del personal de soporte técnico	RECURSO HUMANO
FPC-20	Ausencia de personal ejecutivo para la toma de decisiones ante situaciones de riesgo informático	RECURSO HUMANO

4.5. Políticas

- El Plan de Contingencia será actualizado con una periodicidad anual y entregado a la Dirección del Hospital Básico del IESS Guaranda para su validación y aprobación.

- Dicha actualización (a partir de la segunda versión en adelante) incluirá un capítulo donde se especificará las altas y bajas de los planes específicos de contingencia, así como aquellos que por uno u otro motivo fueron modificados respecto a su versión original.
- Se mantendrán 2 copias vigentes de respaldo y se repartirá una copia a todas las áreas involucradas en los planes.
- La implementación del Plan de Contingencia está programado en el bimestre de su aprobación.
- Se realizarán Plan de pruebas semestralmente.

5. Responsables, Recursos y Periodos y/o Plazos

En el literal "6. Desarrollo de las actividades, fases, estrategias, programas y/o políticas" del presente Plan; se ha considerado a los responsables, sus recursos y los plazos a emplear durante la ejecución de los diferentes eventos susceptibles de contingencia. Para esto se ha desarrollado utilizando el formato Anexo A02: "Formato Registro Plan de Contingencia" tanto para el Plan de Prevención, Plan de Ejecución, Plan de Recuperación y Plan de Pruebas.

6. CRITERIOS EMPLEADOS

Disminuir el impacto de los eventos de riesgo que se puedan presentar y que atenten contra la normal operatividad del Hospital Básico del IESS Guaranda, llegándose a detallar los procedimientos a seguir durante la prevención, ejecución, recuperación y pruebas a desarrollarse.

Anexos

Anexo A01: Formato de Ocurrencias de Eventos

Formulario de Ocurrencia de Eventos			
Código del Evento		**Fecha:**	
Descripción de la Ocurrencia:			
Anotaciones al Plan de Prevención:			
Anotaciones al Plan de Ejecución:			
Anotaciones al Plan de Recuperación:			
Observaciones:			
Contingencia Autorizada por:			
Contingencia Desactivada por			

Anexo A02: “Formato Registro Plan de Contingencia”

Hospital Básico del IESS Guaranda	Evento:		FPC-xx Versión: xx.xx
Fecha: dd/mm/aaaa	**Entidad responsable:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Entidad involucrada:** HOSPITAL BÁSICO DEL IESS GUARANDA	**Pág.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento
En este punto se describe el evento producido.

b) Objetivo
En esta sección se describirá el objetivo y funciones principales de un proceso, ejecutándose a condiciones “normales”, es decir, sin que se presente un evento que genere la contingencia.

c) Criticidad
Señala cuan crítico es un proceso, así como el nivel de impacto del mismo dentro del servicio como se clasifica a continuación:

- **Crítico**: El proceso o actividad es altamente crítico, no puede detenerse nunca y no deber ser interrumpido.
- **Importante**: El proceso o actividad puede ser suspendido por un breve lapso de tiempo no mayor a las 2 horas.
- **Menos Importante**: El proceso o actividad puede ser suspendido por un lapso de tiempo no mayor a 24 horas.

d) Entorno
En esta sección se describirá la ubicación y los ambientes, equipos informáticos, equipos diversos (automáticos, mecánicos o manuales) donde se ejecuta el proceso en forma normal, así como las condiciones básicas para su operación.

e) Personal Encargado
Aquí se especificará el (los) nombre(s) y cargo(s) del personal del servicio, encargado de ejecutar el proceso en forma normal, así como sus roles dentro del mismo.

f) Condiciones de Prevención de Riesgo
En esta sección se debe describir detalladamente las acciones que se ejecutan durante el proceso normal y los puntos de control implementados, a efectos de prevenir que se presente el evento que genere la activación de un estado de contingencia.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
Aquí se describen los eventos que deciden la activación de la contingencia. Asimismo, se especifica el lapso de tiempo en el cual se empieza a ejecutar el proceso de contingencia.

b) Procesos Relacionados antes del evento.
Aquí se establecerán en forma secuencial todos los procesos o actividades que se tengan que ejecutar con anterioridad al ingreso al proceso de contingencia.

c) Personal que autoriza la contingencia.
Se especificará los cargos del personal que autorizará el inicio del proceso de contingencia.
Se especificará los cargos del personal que iniciará el proceso de contingencia.
Se especificará el nivel de coordinación con funcionarios o responsables de Hospital Básico del IESS Guaranda.

d) Descripción de las actividades después de activar la contingencia.
Se describirá en forma detallada y secuencial los pasos a realizar para poner en marcha el proceso de contingencia.

e) Duración
Aquí se especificará, de ser posible, el lapso de tiempo por el cual estará activada la contingencia, así como el evento que determine el término del mismo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
Aquí se especificará el (los) nombre(s) y cargo(s) del personal del servicio, encargado del proceso de Recuperación (volver al proceso normal), así como sus roles dentro del mismo.

b) Descripción
Se describirá en forma detallada y secuencial los pasos a ejecutar para retornar al proceso normal, debiendo indicar lo necesario para asegurar la recuperación efectiva del mismo.

Deberá tenerse en cuenta aquellas actividades que permiten actualizar los procesos con la nueva información generada en la contingencia, en caso sea necesario.

c) Mecanismos de Comprobación

En esta sección se describirán todas aquellas actividades a realizar y que permitan asegurar que el proceso recuperado opere en condiciones normales y sin volver a presentar la falla que origino la ocurrencia del evento. Mientras esta etapa se realiza, aún sigue activado el Plan de Contingencia.

d) Desactivación del Plan de Contingencia

Se especificará en forma secuencial y lógica cual es el procedimiento a seguir para desactivar el proceso de contingencia.

e) Proceso de Actualización

Se especificará en forma detallada y secuencial las actividades a ejecutar para actualizar el proceso normal recientemente recuperado.

Anexo A03: “Control y Certificación de Pruebas de Contingencia”

Formulario de Control y Certificación de Pruebas de Contingencia						
					Código del Plan N°	
Proceso en Prueba						
Área responsable						
Fecha		**Hora Inicio**		**Hora Fin**		
Información del Proceso						
Metodología y Alcance:						
Condiciones de Ejecución:	Equipo					
	Aplicación/Software			Versión		
	Fecha de Backup					
De la prueba / Certificación						
Resultado de la Prueba	Satisfactorio		Satisfactorio con Observaciones:		Deficiente	
Observaciones						
Actualización del plan de Contingencia						
Cambios o actualizaciones en el Plan de Contingencia						
Participantes y Aprobación						
Participante		**Cargo**		**Firma**		

Anexo A04: Copias de Respaldo

Todo nuevo desarrollo de aplicaciones que el Hospital Básico del IESS Guaranda realice, considerará un proceso de respaldo de la información que incluye programas fuentes, ejecutables, objetos, base de datos, documentación, configuraciones de los equipos y software entre otros.

La ejecución de los respaldos será responsabilidad del área de la Unidad de Informática, estará basada en una rutina de copias de seguridad tipo Normal o Básico y la frecuencia y contenido de estas copias de respaldo se hará tal como se indica en el cuadro siguiente:

CUADRO 06: Rutinas de Respaldo

RUTINA DE RESPALDOS (BACKUP)					
Frecuencia de Backup	**Contenido**	**Día de entrega**	**Periodo de retención**	**Cantidad de copias**	**Destino**
Diario	Base de Datos	Lunes a domingo	Una semana	01	Uno para la Unidad de Informática
Semanal	Base de Datos	Domingos	Tres meses	01	Uno para la Unidad de Informática.
Anual	Base de datos al cierre del año. Programas fuentes y objetos.	Primer día útil del siguiente año	Tres años	01	Uno para la Unidad de Informática.

Las características de los respaldos de información se mencionan a continuación:

Los respaldos se realizarán en medios magnéticos removibles, y serán etiquetados inmediatamente después de acabada la operación de backup.

La terminología que se utilice para identificación de las carpetas, estará basada principalmente en la fecha de realización del mismo, y también en la naturaleza de la data archivada.

Los medios magnéticos serán almacenados en las instalaciones del Hospital Básico del IESS Guaranda.

Anexo A05: Subfactores entregados como parte del Plan de Instalación

Sistema de Video Vigilancia

Se recomienda un sistema de circuito cerrado compuesto por cámaras de vigilancia IP con grabadora digital que permita almacenar registros durante 30 días; este sistema nos permitirá obtener registro e imagen del área donde se encuentre para detectar intrusiones, eventos no deseados, sabotajes, entre otros.

El presupuesto para este tipo de sistema se encuentra registrado en el PAC para este año.

Sistema Contra Incendio (Extintores)

La institución cuenta con un sistema de protección contra incendios, el cual se basa en extintores de polvo químico seco (PQS) y gas carbónico (CO2) distribuidos en todos los pisos de la institución.

El Hospital Básico del IESS Guaranda cuenta con los siguientes tipos de extintores para las diversas clases de incendios:

- **Incendios de Clase A:** Todo lo referente a Materiales sólidos (Papel, Madera, Cartón).
- **Incendios Clase B y C:** Todo lo referente a Líquidos Inflamables y/o Equipos Eléctricos (Gasolina, Pinturas, Solventes, Equipos eléctricos conectados).

Además cuenta con un sistema de alarma contra incendios con sus respectivos sensores automación de humo.

El sistema contra incendios está distribuido de la siguiente manera:

Lugares	**Extintores**
Área Administrativa	3 CO2 de 10 lb 2 gabinetes completos con un PQS de 6 kg.
Consulta Externa	1 PQS de 10 lb 1 Gabinete completo con un PQS de 6 kg.
Pasillo de sala de espera en Quirófano	1 PQS de 10 lb 1 Gabinete completo con un PQS de 6 kg. 1 Gabinete
Pasillo de Hospitalización	3 PQS de 10 lb 1 Gabinete completo con PQS de 6 kg. 1 Gabinete
Salón de Actos	1 PQS de 10 lb 1 Gabinete competo con un PQS de 6 KG.
Laboratorio	2 CO2 de 10 lb
Imagen	1 CO2 de 10 lb
Farmacia	1 CO2 de 10 lb
Rehabilitación	1CO2 de 10 lb 1PQS de 10 lb 1 Gabinete completo con PQS de kg., en el pasillo
Emergencia	2 PQS de 10 lb 1 Gabinete a la salida
Odontología	1 PQS de 10 lb
Parqueadero	1 PQS de 10 lb
Bodegas Subterráneas	3 PQS de 10 lb
Grupo electrógeno	1CO2 de 20 lb en el generador

	1 PQS de 20 lb en la cámara de generación
Central de oxígeno	1 PQS de 20 lb
Cisternas	1 PQS de 20 lb
Depósito de GAS	2 PQS de 6 kg.
Capilla	1 Gabinete completo con un PQS de 6 kg., en el pasillo

Luces de Emergencia

Se ha instalado sistema de luces de emergencia, las cuales tiene una batería interna que se activan ante un corte de fluido eléctrico con una autonomía de 02 horas y están distribuidos en todas las áreas de pasadizos del Hospital.

Planta Eléctrica.

Existe una Planta Eléctrica que funciona con Diésel modelo DMT-250CLS con serie 944146-1 de las siguientes características:

- PHASES 3
- Frecuencia 60 Hz
- Voltaje 120-208, RPM 1800
- Potencia 313 KVA
- Amperaje 867 Amperios
- 250 Kw

Que forma parte del grupo electrógeno del Hospital, Marca Kumis Engine # 34720387 Date of MIG 03/94, el cual se encuentra ubicado en el área de máquinas del Hospital Básico del IESS Guaranda.

Es recomendable el mantenimiento constante del equipo por parte del área de Mantenimiento y la verificación permanente del funcionamiento de los PLC’s que permiten encender automáticamente la planta en caso de la ausencia del fluido eléctrico por parte del proveedor.