ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

“ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPPA PARA LA REDUCCIÓN DE RIESGOS EN LA SEGURIDAD EN REDES CORPORATIVAS DE SALUD”

VERÓNICA VANESSA BERMEO JIMÉNEZ

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

Agosto 2021

@ 2021 Verónica Vanessa Bermeo Jiménez

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado "ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPPA PARA LA REDUCCIÓN DE RIESGOS EN REDES CORPORATIVAS DE SALUD", de responsabilidad de la Señorita: Verónica Vanessa Bermeo Jiménez, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

ING. LUIS EDUARDO HIDALGO ALMEIDA; MSC.
PRESIDENTE

LUIS EDUARDO HIDALGO ALMEIDA
Firmado digitalmente por LUIS EDUARDO HIDALGO ALMEIDA
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=LUIS EDUARDO HIDALGO ALMEIDA
Fecha: 2020.08.25 09:00:07 -05'00'

ING. ERNESTO BOLÍVAR SERRANO GUEVARA; MSc.
DIRECTOR

ING. PAÚL XAVIER PAGUAY SOXO; MSc.
MIEMBRO

Firmado digitalmente por PAUL XAVIER PAGUAY SOXO
Fecha: 2021.03.08 23:20:47 -05'00'

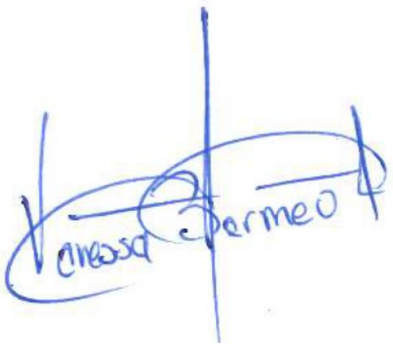
ING. JONNY ISRAEL GUAIÑA YUNGÁN; MSc;
MIEMBRO

Firmado electrónicamente por:
JONNY ISRAEL GUAINA YUNGAN

Riobamba, Agosto 2021

DERECHOS INTELECTUALES

Yo, Verónica Vanessa Bermeo Jiménez, 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.



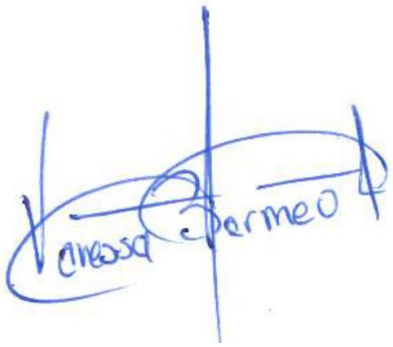
Verónica Vanessa Bermeo Jiménez

Nº de Cédula: 060388282-0

DECLARACIÓN DE AUTENTICIDAD

Yo, Verónica Vanessa Bermeo Jiménez declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.



Verónica Vanessa Bermeo Jiménez

Nº de Cédula: 060388282-0

DEDICATORIA

Dedico el presente trabajo de Investigación

A mí querida Familia en especial a mis pequeñas princesas Paula y Romina

Quienes han sido mi apoyo y mi fuerza incondicional, la fuente de mi motivación

Para poder superarme cada día.

A mi amado esposo quien ha sido mi apoyo incondicional

y el soporte de nuestro hogar.

AGRADECIMIENTO

Agradezco a Dios por bendecir mi camino y

a todas las personas que me han apoyado de una u otra forma especial

a cada uno de mis docentes que han aportado con un granito de arena

en mi formación profesional.

Así también a mis amigos y familiares.

TABLA DE CONTENIDO

CAPITULO IV

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

ACRÓNICO	DESCRIPCIÓN
DHHS	**Departamento de Salud y Servicios Humanos**
EGSI	**Esquema Gubernamental de Seguridad de la Información**
EPHI	**Electronic Protected Health Information**
GFI	**Global Financial Integrity**
HIPAA	**Ley de Transferencia y Responsabilidad de Seguros Médicos**
HSR	**HIPAA Security Rule**
IEC	**Comisión Electrónica Internacional**
ISO	**Organización Internacional para la Estandarización**
LAN	**Red de Área Local**
LOPD	**Ley Orgánica de Protección de Datos**
NIST	**Instituto Nacional de Estándares y Tecnología**
PHI	**Información Protegida de Salud**
PHIPA	**Personal Health Information Protection Act**
SGSI	**Sistema de Gestión de Seguridad de la Información**
VPN	**Red Privada Virtual**
WAN	**Red de Área Amplia**

RESUMEN

El presente proyecto tuvo como objetivo la adaptación de las Normas ISO 27001 e HIPPA para reducción de riesgos de seguridad en las redes de Corporativas de Salud, permitiendo dar mayor seguridad como: confidencialidad, integridad y disponibilidad a la información que utiliza por institución. Para el desarrollo de la adaptación se utilizó la legislación actual vigente, las Normas ISO 27001 e HIPPA; esta adaptación se la hizo en dos fases; antes de implementar la adaptación, donde se pudo conocer los riesgos que afectan la información que se maneja dentro de la institución y dar su valor de acuerdo a la afección o daños que estos pueden causar. En la segunda fase se realizó la misma evaluación y se pudo evidenciar que tuvo una disminución porcentual con respecto a la primera fase; obteniendo mayor seguridad en la información basadas en la confidencialidad, integridad y privacidad de la misma; pilares fundamentales que se deben considerar en toda organización. Mediante el estudio realizado se pudo establecer que las Normas ISO 27001 e HIPAA protegen los activos es decir la información de la organización estableciendo sus ventajas, y desventajas; se ha reducido sustancialmente el promedio de ponderación de probabilidad que los riesgos ocurran en de un 90% en situación inicial contra un 75 % post- implementación. Se recomienda que la implementación sea aplicada en cada uno de los hospitales de las diferentes jurisdicciones a nivel Nacional, con el objetivo de identificar adecuadamente los riesgos y generar políticas de seguridad para lograr un adecuado manejo de la información.

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

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.04.19 16:47:47 -05'00'

0047-DBRAI-UPT-IPEC-2021

ABSTRACT

The objective of this project was to adapt the ISO 27001 and HIPPA Standards to reduce security risks in the Corporate Health networks, allowing greater security such as: confidentiality, integrity and availability to the information used by the institution. For the development of the adaptation, the current legislation in force was used, the ISO 27001 and HIPPA Standards; This adaptation was done in two phases; Before implementing the adaptation, where it was possible to know the risks that affect the information that is handled within the institution and give their value according to the condition or damage that they may cause. In the second phase, the same evaluation was carried out and it could be evidenced that it had a percentage decrease with respect to the first phase; obtaining greater security in the information based on the confidentiality, integrity and privacy of the same; fundamental pillars that must be considered in any organization. Through the study carried out, it was possible to establish that the ISO 27001 and HIPAA Standards protect the assets, that is, the information of the organization, establishing their advantages and disadvantages; The average probability weighting of risks occurring has been substantially reduced by 90% in the initial situation versus 75% post-implementation. It is recommended that the implementation be applied in each of the hospitals of the different jurisdictions at the national level, with the aim of properly identifying risks and generating security policies to achieve adequate information management.

Keywords: <TECHNOLOGY AND ENGINEERING SCIENCES>, <COMMUNICATIONS TECHNOLOGY>, <COMPUTER SECURITY>, <ISO 27001 STANDARDS>, <HIPAA STANDARD> <INFORMATION SECURITY>.

CAPÍTULO I

1. INTRODUCCIÓN

En la actualidad el uso de las Tecnologías de la Información dentro del sector de la Salud ha ido en aumento permitiendo la optimización, mejoramiento y eficacia de sus servicios, convirtiéndose en la herramienta más importante; pero esta información no cuenta con políticas de protección, generando vulnerabilidades que son aprovechadas por diferentes amenazas que se encuentran en el entorno y que afecta la confidencialidad, integridad y disponibilidad de los activos (datos).

La principal falla es la falta de conocimiento de las normas de seguridad de la información por parte del personal que labora dentro de las instituciones públicas y privadas; esta falta de conocimiento va generando una vulnerabilidad y riesgo para la seguridad de los datos (archivos) que se manejan en las instituciones a nivel Nacional; por lo cual se genera un impacto de manera negativa y esto conlleva a sanciones legales y económicas, afectando la imagen de la institución.

Existe otro riesgo que afecta a la institución causando pérdidas de información de manera interna y externa; como por ejemplo falta de procesos en el manejo de la información, sistemas internos obsoletos, tecnologías desactualizadas. Las soluciones que se puede dar son: otorgar permiso solo al personal autorizado, crear copias de la información y gestionar de manera adecuada los perfiles de administradores y usuarios.

Las normas que se puede emplear en el manejo de la seguridad de la información son ISO 27001 y HIPAA, la Norma ISO 27001 es un modelo para la creación y funcionamiento del sistema de gestión para la seguridad de la información (SGSI), permitiendo la protección de los activos, datos financieros, información de los empleados y datos intelectuales.

Otra norma que se puede aplicar para la seguridad de la información médicas es la norma estadounidense HIPAA o también conocida como HIPPA que ha sido difundida 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.

El principal problema que se presenta en el Sistema de Salud es la carencia de políticas que están basadas al régimen de las normas estandarizadas internacionalmente para la seguridad de la información, por lo que no se puede garantizar la confidencialidad, disponibilidad e integridad de los datos (información) que son propiedad de esta organización. A nivel intencional existen normas estandarizadas que son adaptables para el manejo de grandes cantidades de información y estas no puedan sufrir ataques ni ninguna clase; para lo cual se aplica las Normas ISO 27001 e HIPPA para la reducción de riesgos de seguridad con el fin de proporcionar confidencialidad, integridad y disponibilidad de la información de manera segura.

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 INFORMACIÓN 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 et al., 2012).

Según Benítez 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

[1] HIPAA: Health Insurance Portability and Accountability Act

[2] PHI: Protected Health Information

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 en redes corporativas de salud?

1.4. Sistematización del Problema

- ¿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 redes corporativas de salud?
- ¿Cuáles son los riesgos más importantes en la seguridad de los sistemas de información en redes corporativas de salud?

1.5. Justificación de la investigación

1.5.1. 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 INFORMACIÓN (EGSI), donde se dispone el uso obligatorio de las Normas Técnicas Ecuatorianas

[3] SNS: Sistema Nacional de Salud.

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.

1.5.2. 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.

1.5.3. 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 en redes corporativas de Salud.

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 HIPPA para proponer una adaptación entre ellas, para asegurar los sistemas de información en redes corporativas de salud.
- Implementar la adaptación de las normas ISO 27001 e HIPPA en una red corporativa de salud.
- Evaluar la implementación de la adaptación de las normas ISO 27001 e HIPPA en el Hospital de Nivel I del IESS Guaranda

1.7. Hipótesis

La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos en redes corporativas de salud.

[4] SNAP: Secretaria Nacional de Administración Pública

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Amenazas, Ataques, Vulnerabilidades de la Red

2.1.1. Modelo de ataques

El ataque es la culminación de varias amenazas y vulnerabilidades que son realizadas por el intruso hasta que logra ingresar y causar daño al sistema, ocasionando perdida de la información más relevante de la empresa e instituciones o el robo de dinero o activos de la misma. (Villacis Espinosa Miguel Leopoldo, 2016, pág. 6)

El objetivo principal de los ataques es la obtención de la información confidencial, corromper la información del sistema, usar terminales remotos para la instalación de programas maliciosos, modificación del sistema operativo para el robo de activos o capital de la empresa o institución.(Villacis Espinosa Miguel Leopoldo, 2016, pág. 6) y (Mozorra Olmedo Erik Ramiro, 2019, pág. 2-3)

Existen cuatro modelos de ataque:

- Interrupción: Es cuando un activo se destruye o queda inutilizable como, por ejemplo: la destrucción de disco duro.
- Interceptación: Es cuando se accede a la información por medio de terceras personas que no están autorizadas.
- Modificación: Es cuando se accede a la información por medio de tercera persona que no está autorizada y se modifica la información generando un ataque contra la integridad de los datos.
- Fabricación: Es cuando una parte no autorizada inserta objetos falsificados o no autorizados en los activos de la empresa o institución. (Segada Geraldo Silva Coelho Flavia Estelia & Bezerra Edson Kowask, s. f. pág. 25)

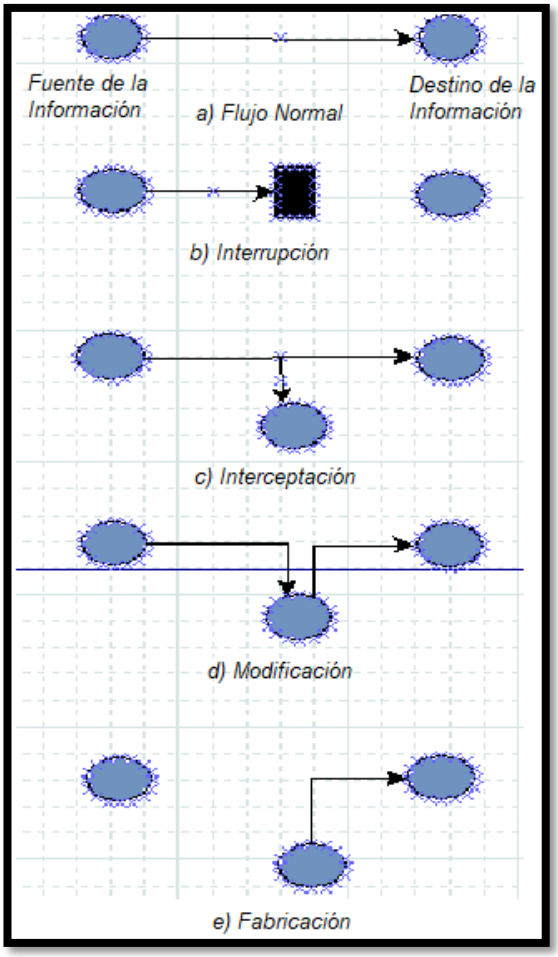


Figura 1: Modelo de Ataques
Fuente: (Segada Geraldo, Silva Flavia & Bezerra Edson Kowask, s. f., 2014, pág. 25)

2.1.2. Amenazas a la Seguridad Informática

Las amenazas que se presenta en la seguridad informática son todos los elementos o acciones de manera premeditada que se hacen para atentar contra la información (datos), estas se presentan cuando existen vulnerabilidades internas y externas que se utiliza en diferentes situaciones como perjudicar o robar información. Las vulnerabilidades se dan desde el usuario con el uso incorrecto de la tecnología, falta de capacitaciones a personal, contraseñas obsoletas, etc. Para un sistema seguro se establece una serie de estándares, protocolos, métodos, reglas y técnicas. (Tigse Moposita Jorge Luis, 2020. pág. 10)

Existen amenazas que deben ser tomadas en cuenta:

- Usuarios: Se considera la causa del mayor problema ligado a la seguridad de un sistema informático, es así porque con sus acciones podrían ocasionar graves consecuencias.
- Errores de programación: Se trata de un mal desarrollo, pero también tiene que ver con los sistemas operativos y aplicaciones estén sin actualizar.(Tigse Moposita Jorge Luis, 2020. pág. 11)
- Intrusos: Cuando personas que no están autorizadas acceden a programas o datos.
- Siniestro: También se puede perder o deteriorar material informático por una mala manipulación o mala intención, tales situaciones como robo, incendio o inundación.
- Fallos electrónicos: Un sistema informático en general puede verse afectado por problemas del suministro eléctrico o por errores lógicos como cualquier otro dispositivo que no es perfecto.
- Catástrofes naturales: Rayos, terremotos, inundaciones.
- Copias de seguridad: Para proteger de forma eficiente los datos son imprescindibles las copias de seguridad o backups.(Tigse Moposita Jorge Luis, 2020, pág. 11)

2.1.3. Vulnerabilidades

Las vulnerabilidades son las debilidades del sistema informático; la presencia de una o varias vulnerabilidades no causan daño por sí solas, se necesita de una amenaza para ocasionar problemas dentro de una organización o institución, se puede considerar que si una vulnerabilidad no tiene ninguna amenaza no será necesario aplicar un control. (Tigse Moposita Jorge Luis, 2020, pág. 11)

2.1.3.1. Las áreas de vulnerabilidad:

- Procesos y procedimientos: los procesos y procedimientos son afectados por su participación en el manejo de la información.

- Personal: es el principal responsable de que las vulnerabilidades que afectan a la organización por ser el que trabaja y manipula la información de manera física o lógica.
- Ambiente: se verá afectado cuando no se siga lineamientos para mantener un espacio estable y libre de amenazas. (Tigse Moposita Jorge Luis, 2020, pág. 11)
- Configuraciones de los sistemas de información: al no existir una correcta configuración de los sistemas, se deja abierto una brecha para posibles vulnerabilidades que sean explotadas por personas mal intencionadas.
- Hardware y Software: el escoger el tipo de tecnología que se vaya a utilizar para las labores de la empresa o institución, debe ser tomando en cuenta la seguridad que ofrece y los beneficios que se obtiene al utilizarlos.

2.1.4. Riesgo

El riego no es más que la suma de las amenazas y vulnerabilidades encontradas o analizadas al sistema de información de una compañía o entidad.

AMENAZA +´VULNERABILIDAD = RIESGO

2.2. Seguridad Informática

La Seguridad Informática engloba cuatro aspectos importantes como la integridad, disponibilidad, confidencialidad y autenticación, su objetivo principal es mantener el mínimo riesgo sobre los recursos informáticos, previniendo el robo de la información como, por ejemplo: contraseñas, información privada, robo de número de tarjeta de créditos, cuentas bancarias entre otros. (Tigse Jorge Luis, 2020, pág. 9-10)

La seguridad de la información presenta cambios tecnológicos en la vida diaria de las organizaciones, estos cambios pueden hacer que se presente nuevas vulnerabilidades y riegos; por lo que debe ir acompañado de una correcta evaluación de riegos de manera dinámica levantando los niveles de riesgo y la forma de tratarlos.

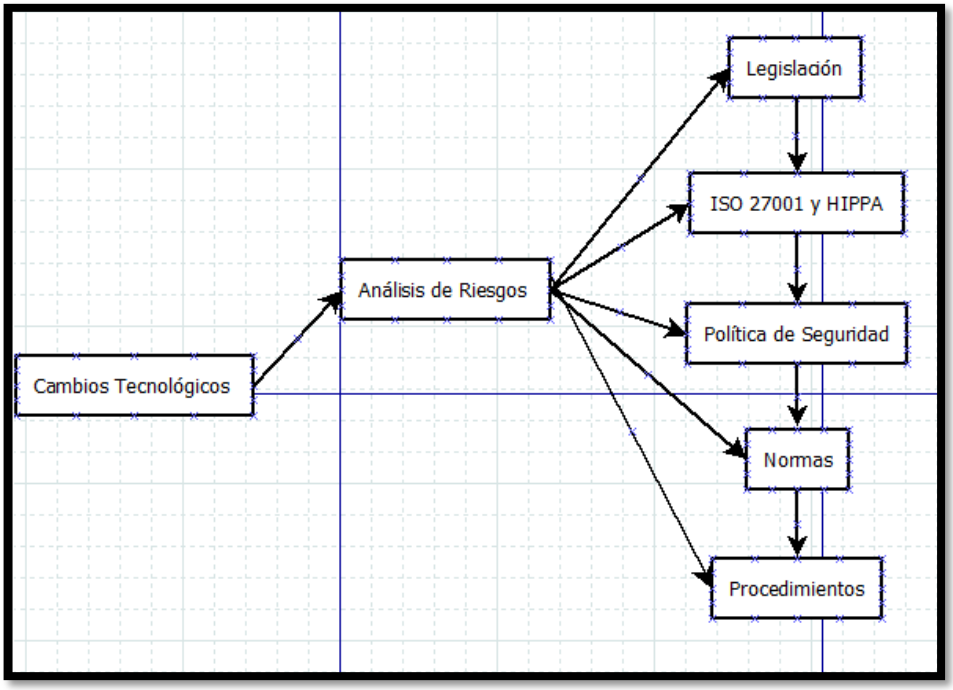


Figura 2: Visión General de la Seguridad Informática
Fuente:(Segada Luiz Geraldo Silva Flavia & Bezerra Edson Kowassk, s. f, 2014, pág. 29)

2.2.1. Servicio de Seguridad

Los servicios de seguridad son medidas preventivas elegidas para hacer frente a las amenazas identificadas haciendo uso de uno o más mecanismos de seguridad. Los servicios y mecanismos de seguridad deben aplicarse con el fin de cumplir con los requisitos de seguridad de la organización, teniendo en cuenta el equilibrio entre las necesidades de seguridad y sus costos; es esencial analizar los riesgos y los impactos probables que comprenden a toda la organización en cuestión.

- Confidencialidad: comprende la protección de los datos transmitidos contra ataques pasivos, es decir, el acceso no autorizado, que incluirá medidas tales como el control de acceso y encriptación.

- Autenticidad: garantiza que la comunicación sea auténtica, entre origen y destino permitiendo verificar la identidad de la otra parte implicada en la comunicación, con el fin de confirmar que la otra parte es quien dice ser. El origen y el destino son normalmente usuarios, dispositivos o procesos.

- Integridad: es importante utilizar un esquema que permite la verificación de la integridad de los datos almacenados y su transmisión. La integridad puede ser considerada bajo dos aspectos: servicio sin y con recuperación. Una vez que los ataques activos se producen se genera la detección, en lugar de la prevención, y este puede ser reportado y el mecanismo de recuperación se activa inmediatamente. (Segada Luiz, Silva Flavia & Bezerra Edson Kowassk, s. f.)

- No repudio: comprende el servicio que impide a una fuente o destino negar la transmisión de mensajes, es decir, cuando se envía el mensaje dado, el destino puede demostrar que éste fue enviado realmente por determinado origen y viceversa.

- Conformidad: se debe cumplir y hacer cumplir las regulaciones internas y externas impuestas a las actividades de la organización. Para eso se está de acuerdo, siguiendo y haciendo cumplir las leyes y reglamentos internos y externos.

- Control de acceso: trata de limitar y controlar el acceso lógico / físico a los activos de una organización a través del proceso de identificación, autenticación y autorización, con el fin de proteger los recursos contra el acceso no autorizado.

- Disponibilidad: determina que los recursos estén disponibles para el acceso por parte de entidades autorizadas, siempre que lo soliciten, representando la protección contra la pérdida o degradación. (Segada Luiz, Silva Flavia & Bezerra Edson Kowassk, s. f.)

2.2.2. Plan de Gestión de Seguridad Informática

Es el conjunto de medios administrativos, técnicos y personales que de manera relacionada garantizan la seguridad informática, de acuerdo a la importancia de los bienes a proteger y los riesgos estimados. El plan de gestión de seguridad informática es el documento básico en donde se establecen los principios organizativos y funcionales de la actividad de seguridad informática para las entidades, agrupando todas las políticas y responsabilidades de los participantes; estas medidas y procedimientos permiten prevenir, detectar y responder a las amenazas que pueden ocurrir sobre el mismo. (Tigse Jorge Luis, 2020, pág. 12)

2.2.2.1. Aspectos Organizativos de la Seguridad de la Información

El objetivo principal de la seguridad de la información es la implementación de normativas y políticas de seguridad que deben ser aplicados al personal que está involucrado directamente e indirectamente con la información. (Uyaguari María Eliza, 2012, pág. 2)

2.2.2.2. Organización Interna

En primer lugar, se debe realizar es una estructura de como iniciar y controlar la implementación de políticas de seguridad dentro de la institución, así como la aprobación y asignación de personal que se va a encargar de manejar la seguridad. (Uyaguari María Eliza, 2012, pág. 2)

Compromiso de la Dirección con la Seguridad de la Información

La dirección debe apoyar de manera activa la seguridad de la información dentro de la organización, las diferentes actividades se podrían manejar mediante comités de dirección donde esta incluidos todos los representantes de las diferentes áreas. (Uyaguari María Eliza, 2012, pág. 2)

Asignación de Responsabilidades para la Seguridad de la Información

Las responsabilidades deben estar definidas claramente para proteger los activos de la información y los responsables están encargados de verificar la ejecución de las tareas asignadas a cada área que están dentro de la Institución. (Uyaguari María Eliza, 2012, pág. 3)

Autorizaciones para los Servicios de Procesamiento de Información

Según la Norma ISO 27001 se debe tener en cuenta las siguientes recomendaciones para el proceso de autorización:

- Los servicios nuevos deben tener la autorización de la dirección.
- El hardware y el software deben ser verificados para asegurar su compatibilidad con los demás componentes del sistema.

- Es necesario identificar e implementar controles contra vulnerabilidades de equipos personales. (Uyaguari María Eliza, 2012, pág. 3)

Acuerdos sobre Confidencialidad

Se debe considerar los siguientes elementos para poder establecer los requisitos:

- Definir la información que se va a proteger.
- Tiempo de duración del acuerdo de confidencialidad.
- Acciones que se debe tomar cuando se termina un acuerdo.
- Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información.
- Propiedad de la información, secretos comerciales y propiedad intelectual.
- Derecho de auditar y monitorear las actividades que involucra información confidencial.
- Términos para la devolución o la destrucción de información confidencial después de terminar el acuerdo.
- Acciones legales que se van a tomar en caso de incumplimiento del acuerdo de confidencialidad.(Uyaguari María Eliza, 2012, pág. 3)

Revisión Independiente de la Seguridad de la Información

Las revisiones deben hacer una persona que no pertenezca al área o a la institución que está siendo revisada, así se puede conseguir eficacia, idoneidad y propiedad del enfoque de la organización para la seguridad de la información. (Uyaguari María Eliza, 2012, pág. 4)J

Organización Externa

Las normas de seguridad de la información no solo deben aplicarse al personal interno, si no deben intervenir el personal externo de la institución los que están implicados por medio de un contrato,

alianza o convenio, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información de la institución. (Uyaguari María Eliza, 2012, pág. 4)

Identificación de los Riesgos relacionados con las Partes externas

Se concede la autorización a personal externos para el procesamiento de la información siempre y cuando se realice una evaluación de riegos, así se puede identificar los controles necesarios para evitar daños sobre el mismo. Para lo cual se considera lo siguiente:

- Los servicios de procesamiento de información a los cuales requiere accesos la parte externa.
- El tipo de acceso que tendrá la parte externa a la información ya a los servicios de procesamiento de información (físico, lógico o conexión real).
- El valor y la sensibilidad de la información involucrada.
- Se debe implementar controles necesarios para que la información no autorizada no esté disponible para la parte externa.
- Se debe implementar mecanismos que permita identificar al personal autorizado a tener acceso, la manera de verificar la autorización y la forma de verificar la autorización.
- Los medios y controles utilizados por la parte externa para almacenar, procesar, comunicar, compartir e intercambiar la información.
- El impacto que se puede generar cuando el acceso es denegado a la parte externa.
- Los procedimientos para tratar los incidentes de seguridad de la Información, los daños potenciales y las condiciones para la continuación del acceso de la parte externa.
- Requisitos legales y obligaciones contractuales que debe tener en cuenta la parte externa para acceder a la información. (Uyaguari María Eliza, 2012, pág. 5)

Seguridad cuando se trata de clientes

Se debe considerar los siguientes términos para abordad la seguridad antes de dar acceso a los clientes para que puedan acedar a los activos de la información de la Institución:

- Protección de los activos de la información.
- Descripción del servicio que se va a ofrecer
- Los requisitos y beneficios que va a obtener el usuario del acceso al sistema.

- Políticas de control de acceso (uso de identificadores, contraseñas, privilegios o revocar derechos cuando se rompa las políticas del servicio).
- Convenios para el reporte, notificación de las inexactitudes de la información (como detalle de personal), incidentes y violaciones de la seguridad de información.
- Descripción de cada servicio que va a estar disponible para los usuarios.
- El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la institución.
- Las respectivas responsabilidades civiles de la organización y del cliente.
- Derecho de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo en colaboración para evitar la divulgación a terceros. (Uyaguari María Eliza, 2012, pág. 5)

Acuerdo con Terceras partes

Existen acuerdo que garantizan que no hay malos entendidos entre la institución y terceras partes para lo cual se tiene en cuenta los siguientes puntos:

- Se debe implementar políticas de seguridad de la información y controles para garantizar la protección del activo.
- Asegurar la concientización del usuario sobre responsabilidades, políticas, normas sobre la seguridad de la información.
- Designar responsabilidades relacionadas con las instalaciones y mantenimiento del software y el hardware.
- Se debe definir el modelo de presentación de informes.
- Políticas de control de acceso.
- Incumplimiento y violaciones de los requisitos establecidos en el acuerdo.
- La descripción de los servicios que van a estar disponibles y sus objetivos.
- Derecho a revocar permisos cuando se ve afectado la integridad de la información.
- El derecho a auditar las responsabilidades definidas en el acuerdo, que las autorías sean realizadas por terceras partes. (Uyaguari María Eliza, 2012, pág. 6)

Administración de Recursos

Es importante llevar un inventario de activos, controlar el uso adecuado y clasificarlos, además se debe asignar responsabilidades al personal que labora en la institución que están encargados de la

manipulación de la información. Se debe proveer de medidas adecuadas para la seguridad de la información y protegerla de manera afectiva.

Responsabilidades sobre los activos

A cada activo de la empresa se le debe asignar un responsable para que le brinde protección y mantenimiento adecuado.

Inventario de Activos: se deben identificar los activos más importantes de la institución y su responsable, así como su valor, ubicación, importancia y sobre todo los niveles de protección que deben tener.

- Uso de los Activos: Se debe implementar reglas para el uso de los activos de la institución, y luego debe ser documentados e implementados. (Uyaguari María Eliza, 2012, pág. 6)

Información

No toda la información tiene el mismo valor, sensibilidad para la institución para lo cual se debe implementar diferentes niveles de protección de acuerdo al grado de importancia, para garantizar la confidencialidad, integridad y disponibilidad de la información en todo momento que el usuario la necesite.

La información se clasifica de acuerdo a su valor, sensibilidad, importancia, criticidad con el objetivo de protegerla y manejarla adecuadamente. (Uyaguari María Eliza, 2012, pág. 7)

2.2.3. Sistema de Gestión de la Seguridad de la Información (SGSI)

El Sistema de Gestión de la Seguridad de la Información (SGSI) se utiliza para la administración de información confidencial de una organización empresarial, instituciones para mantener la integridad y la seguridad de la misma. Para poder ejecutar este sistema de gestión se debe incluir a todo el personal, procesos internos, procesos externos y los sistemas manejados por el departamento de TI.

Este sistema SGSI ayuda a las empresas, instituciones pequeñas, medianas y grandes a mantener seguros los activos de información que permitirá crecer a la empresa en confiabilidad ante sus competidores. (Tigse Jorge Luis, 2020, pág. 13)

La seguridad absoluta no existe, la gestión de la seguridad de la información se basa en el planteamiento de directrices, procedimientos y criterios que aseguran la evolución eficiente de la seguridad de los sistemas informáticos. (Ochoa Mabel, 2016, pág. 16)

En la siguiente figura se muestra los principios que conlleva a la implementación de un SGSI:

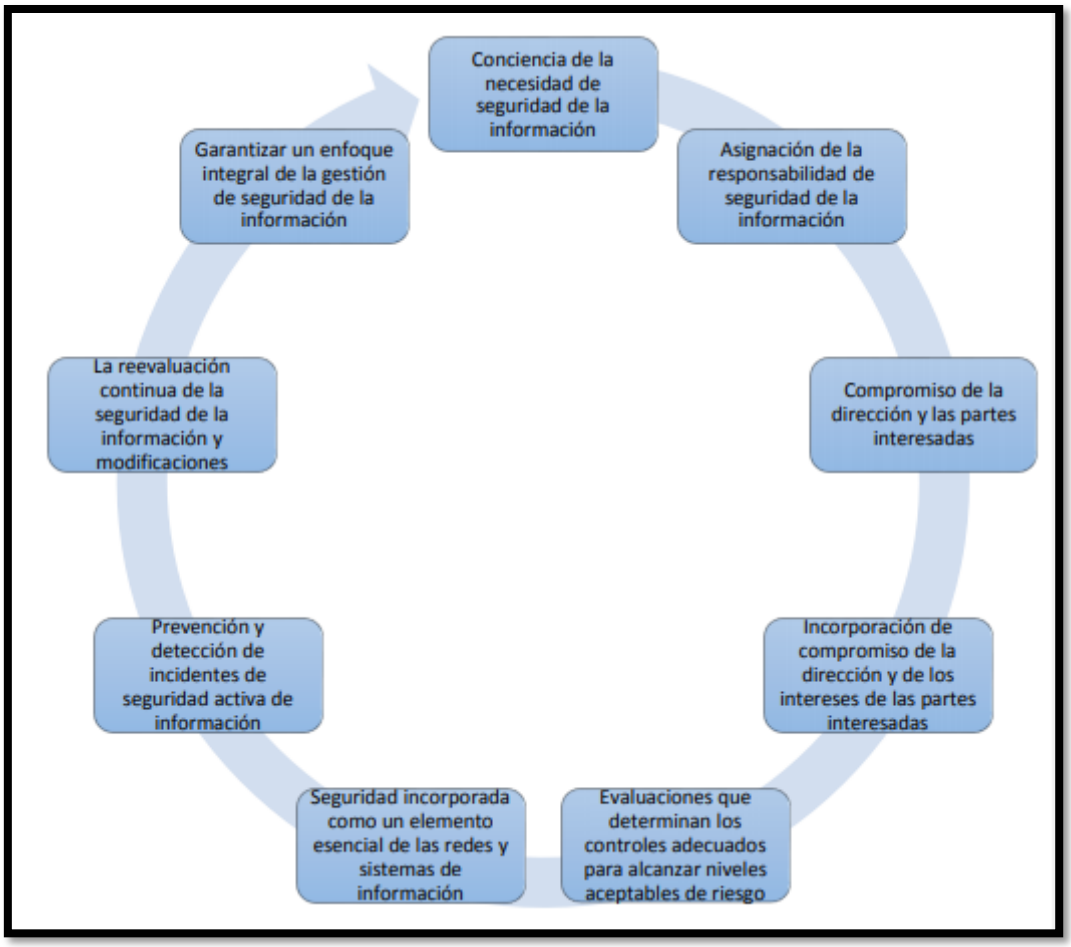


Figura 3: Principios para la implementación de un SGSI
Fuete: (Ochoa Mabel Catherine, 2016, pág. 16)

2.2.3.1. Establecer y monitoreo del SGSI

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)

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)

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)

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)

2.3. Estándares de Seguridad Informática

2.3.1. Norma ISO 27000

La familia de las Normas ISO 27000 es el conjunto de estándares desarrollados por ISO e IEC (International Electrotechnical Commission), que proporciona una gestión en la seguridad de la información que es utilizada por cualquier organización, empresa e institución.

Las más conocidas son:

- ISO/IEC 27000. Proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del proceso PlanDo-Check-Act y términos y definiciones que se emplean en toda la serie 27000.

- ISO/IEC 27001. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican los SGSI's de las organizaciones.

- ISO/IEC 27002. (Antigua ISO 17799:2005). 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.

Tabla 1: Resumen de la Familia ISO

NORMA	CONTENIDO
27000	Visión general de la Serie
27001	Norma principal de la Serie. Requisitos del SGSI. Certificable
27002	Guía de buenas Prácticas: 11 dominios. 39 objetivos de control y 133 controles
27003	Aspectos críticos para el diseño e implementación de un SGSI
27004	Guía para el Desarrollo y utilización de métricas y técnicas de medida de la eficacia de un SGSI y de los controles o grupos de controles
27005	Directrices para la gestión del riesgo
27006	Requisitos para la acreditación de entidades de auditoria y certificación
27007	Guía de auditoría de un SGSI
27008	Guía de auditoría de los controles seleccionados
27013	Guía de implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1
27014	Guía de gobierno corporativo de la seguridad de la información
27031	Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicación
27032	Guía relativa a la ciberseguridad
27033	Guía de seguridad en redes (7 partes)
27034	Guía de seguridad en aplicaciones informáticas
27035	Guía de gestión de incidentes de seguridad de la información
27036	Guía de seguridad de externalización de servicios
27037	Guía de identificación, recopilación y preservación de evidencia digitales

Fuente: (Colegio Oficial de Ingenieros de Telecomunicaciones, s. f.pág. 11)

2.3.1.1. Términos y Definiciones

La norma hace uso de las siguientes definiciones

Tabla 2: Definiciones

Aceptación del Riesgo	**La decisión de aceptar un riesgo**
Activo	Cualquier bien que tiene valor para la empresa o institución
Análisis de Riesgo	Utilización sistemática de la información disponible para identificar los peligros y estimar los riesgos
Confidencialidad	La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
Declaración de aplicabilidad Statement of Applicability (SOA)	Declaración documentada que se describe los objetivos de control y los controles que son relevantes para la SGSI de la organización y aplicables al mismo
Disponibilidad	La prioridad de ser accesible y utilizable por una entidad autorizada
Estimación de Riesgos	El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo
Evaluación de Riesgos	El proceso general de análisis y estimación de riesgos
Evento de seguridad de la información	La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y puede ser relevante para la seguridad.
Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto a los riegos
Incidente de seguridad de la información	Un único evento o serie de eventos de seguridad de la información, inesperados o no deseados, que tiene una probabilidad de significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información
Integridad	La propiedad de salvaguardar la exactitud y completitud de los activos
Riesgos Residuales	Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad
Seguridad de la información	La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad
Sistema de Gestión de la Seguridad de la Información (SGSI) Information Management System (ISMS)	La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.
Tratamiento de Riesgo	El proceso de selección e implementación de medidas encaminadas a modificar los riegos

Fuente: (Colegio Oficial de Ingenieros de Telecomunicaciones, s. f. pág. 11)

2.3.2. Norma ISO/IEC 27001

Esta norma está basada en el modelo Deming, el cual proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de seguridad informática. Este es aplicable a todo tipo de organización, porque es bastante extensa en cuanto a su aplicación y controles operacionales.(Crespo Paul Esteban, s. f. pág. 25-16)

Este estándar se desarrolló para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, este modelo es influenciado por las necesidades y objetivos, requerimientos de seguridad, procesos empleados y el tamaño y estructura de la organización empresarial o institucional. (Villacis Miguel Leopoldo, 2016, pág. 17)

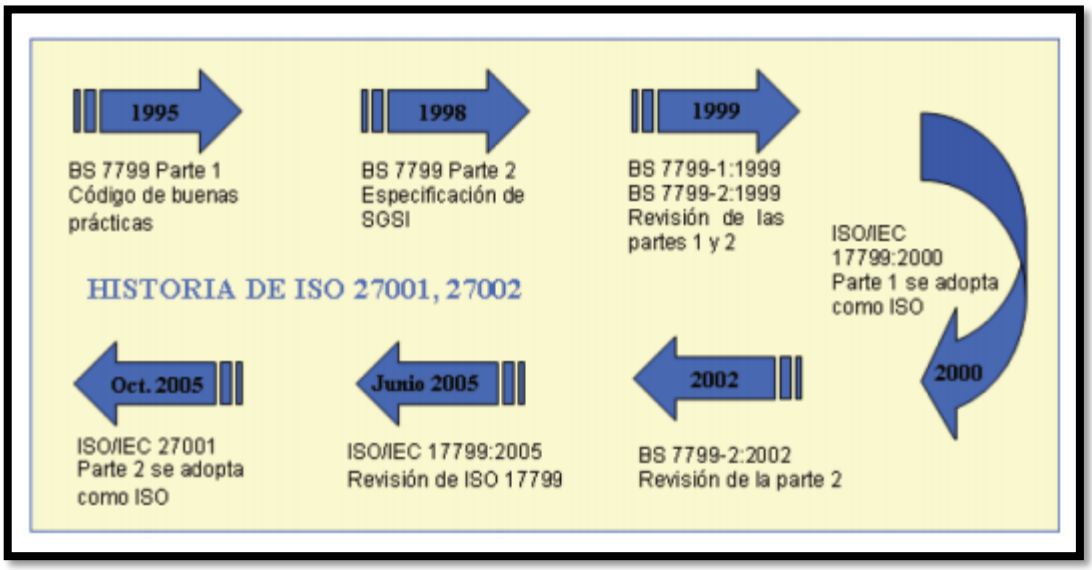


Figura 4: Evolución de la Norma ISO 27001
Fuente: (Villacis Miguel Leopoldo, 2016, pág. 13)

2.3.2.1. Dominio de la Norma ISO 27001

La norma ISO 27001 está constituida por los siguientes dominios:

- Política de Seguridad: su objetivo es garantizar el soporte y gestión para la seguridad, según los requerimientos institucionales y normativas establecidas.
- La organización de la seguridad de la información: tiene como base un marco de referencia para la implementación y control de la seguridad de la información.
- Gestión de Activos: su objetivo es asegurar los activos de la organización.
- Seguridad de los recursos humanos: se fijan medidas para controlar la seguridad de la información, que es maneja por el recurso humano. (Crespo Paul Esteban, s. f. pág. 25-26)

- Seguridad física y del ambiente: busca proteger a las instalaciones de la organización y toda información.
- Gestión de las comunicaciones y operaciones: permite determinar el procedimiento y responsabilidad de las operaciones que se realiza en la organización.
- Control de acceso: permite asegurar la confidencialidad de los sistemas de información de la organización.

Adquisición, desarrollo y mantenimiento de los sistemas informáticos; va dirigido a las organizaciones que desarrollan el software internamente o que tengan contacto con otras organizaciones que están encargadas del desarrollo. (Crespo Paul Esteban, s. f. pág. 25-26)

2.3.2.2. Funcionamiento de la Norma ISO 27001

Esta norma permite la investigación de los problemas que pueden afectar la información para luego establecer los parámetros para evitarlo.

En la figura siguiente se puede observar la filosofía que utiliza la norma para la detección de riegos y luego tratarlos. (Ochoa Mabel Catherine, 2016, pág. 22)

Figura 5: Normas para la Detección de Riesgos
Fuente: (Ochoa Quezada Mabel Catherine, 2016, pág. 22)

2.3.2.3. Políticas de Seguridad de la Norma ISO 27001

La información es el recurso más importante de cualquier empresa o institución que debe ser protegido mediante la creación de políticas de seguridad como la integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad. (Uyaguari María Eliza, 2012, pág. 1)

- Garantizar la confidencialidad de los datos gestionados en los diferentes procesos de la empresa.
- Garantizar la disponibilidad de servicios ofrecidos al cliente y de igual manera a los servicios y procesos internos de la empresa

- Garantizar el funcionamiento de servicios en lapso de tiempos cortos, tras ocurrir situaciones de emergencia. (Uyaguari María Eliza, 2012, pág. 1)
- Prevenir que la información sea modificada sin ninguna autorización.
- Concientizar y brindar formaciones permanentes sobre la seguridad de la información

Las políticas de seguridad de la información están formadas por normas, reglamentos y protocolos que se basan en los objetivos, leyes y requisitos establecidos por la empresa o institución, donde se definen las medidas que se van a proteger la información de amenazas, vulnerabilidades y ataques.(Uyaguari María Eliza, 2012, pág. 1)

Tabla 3: Requerimientos de la Política de Seguridad

Requisitos	Definición	Objetivos
Documento de Política de Seguridad de la Información	Las personas autorizadas son las encargadas de comunicar a todos los empleados sobre las políticas creadas. También se encargan de la redacción del documento sobre la seguridad de la información.	Objetivos de la organización, el alcance y la descripción de la seguridad de la información. Valoración y manejo de los riegos existente, así como detallar los objetivos de control. Descripción de las políticas y normas más importantes para la organización.
Revisión de la Política de Seguridad de la Información	Aquí se indica los cambios más significativos de la evaluación de los riesgos que se presentan en los activos de la empresa. Estas revisiones se deben realizar en tiempos planificados.	

Realizado por: (Verónica Bermeo, 2021)

Fuente: (Uyaguari María Eliza, 2012, pág. 2)

Aspectos organizativos de la seguridad de la Información

Este punto permite la implementación de las guías para administrar y mantener la seguridad de la información, así como las normativas y políticas de seguridad que deben ser aplicadas al personal interno y externo que están involucrados de manera directa e indirecta con la información.

Tabla 4: Aspectos organizativos de la Seguridad de la Información

		Compromiso de la Dirección con la Seguridad de la Información	**Es de vital importancia que la directiva apoye de manera activa la seguridad de la información, esto se debe hacer mediante un comité de dirección involucrando a todas las arias de empresa.**	
Organización Interna	**En primer lugar, se debe hacer una estructura de cómo va iniciar y controlar la implementación de las políticas de seguridad dentro de la organización. Asignar al personal que se**	Asignación de Responsabilidades para la Seguridad de la Información	Se debe definir las responsabilidades para la protección de activos. Las personas encargadas deben verificar correctamente la ejecución de las tareas asignadas.	
		Proceso de Autorización para los Servicios de Procesamiento de Información	Se debe tener en cuenta las siguientes directrices: • Los servicios nuevos deben tener la autorización de la dirección para el usuario apropiado. • Cuando sea necesario el hardware y software deben ser verificados para asegurar la compatibilidad con los demás componentes del sistema. • Se debe implementar controles para las vulnerabilidades	

	va a encargar de manejar la seguridad de la información.		introducidas por equipos personales.	
		Acuerdos sobre Confidencialidad	Definir la información que se va a proteger. Tiempo de duración del acuerdo. Acciones que se van a tomar después de terminar el acuerdo. Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación de la información. Derecho de auditar y monitorear las actividades. Reportar la divulgación no autorizada de la información. términos para la devolución o destrucción de la información confidencial.	
		Contacto con las Autoridades	Las empresas deben contar con procedimientos donde las autoridades deben contar para reportar de manera oportuna los incidentes de le seguridad de la información; esto	

			implica relación con organismos de regulación.	
		Revisión Independiente de la Seguridad de la Información	Esto debe ser realizado por una persona que sea independiente de la empresa, donde se puede conseguir eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la Seguridad de la Información.	
Organización Externa	Se debe realizar normas de seguridad para las personas externas de la empresa que estén involucrados por medio de un contrato, alianza o convenio con el fin de asegurar la integridad, confidencialidad y disponibilidad de la	Identificación de los Riesgos Relacionados con las partes externas	Cuando personal externo quiere acceder a la información de le empresa se debe realizar una evaluación de riesgo, así se puede identificar los controles necesarios.	El tipo de acceso que tendrá la parte externa a la información y servicios. El valor y la sensibilidad de la información involucrada. Controles que deben ser implementadas para que la información no autorizada no esté disponible. La forma que se puede identificar al personal autorizado. Medios y controles que la parte externa tienen para almacenar, procesar, comunicar, compartir información.

	información de la organización.	Abordaje de la Seguridad cuando se trata con Clientes o usuarios	Los siguientes términos deberán ser considerados para abordar la seguridad antes de dar el acceso a los clientes a cualquier activo de la empresa.	Protección de activos. Descripción de producto o servicio que se provee. Política del control de acceso (uso de identificadores, contraseñas, privilegios o revocar derechos). Descripción de cada servicio que va a estar disponible. Derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización. Derecho de prioridad intelectual y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.
Acuerdos con terceras Personas	Se debe garantizar que no existe malos entendidos entre organizaciones y la tercera parte.	Las políticas de seguridad de la información y controles para asegurar la protección del activo. Realizar concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información. Responsabilidades relacionadas con la instalación y mantenimiento del Software y el Hardware. Descripción de cada servicio que va estar disponible los objetivos de cada servicio. Derecho a revocar cualquier actividad relacionada con los activos de la organización.		

		El establecimiento de un proceso de escala para la solución de problemas.		

Realizado por: (Verónica Bermeo, 2021)
Fuente: (Uyaguari María Eliza, 2012, pág. 3-7)

2.3.2.4. Importancia de la Norma ISO 27001

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para ella.
- Implementar y operar controles para reducir los riegos de la seguridad de la información.
- Monitorear y revisar el desempeño y la efectividad del modelo planteado como, por ejemplo: SGSI.
- Proponer un mejoramiento continuo en base a la medición del objetivo. (Villacis Miguel Leopoldo, 2016, pág. 18)
- En la actualidad se está tratando de adoptar el modelo de proceso PDCA (Planear-Hacer-Chequear-Actuar), el mismo que toma como insumos los requerimientos y expectativas de la seguridad de la información de las partes interesadas, generando satisfacción de requerimientos para la seguridad de la información. (Villacis Miguel Leopoldo, 2016, pág. 18)

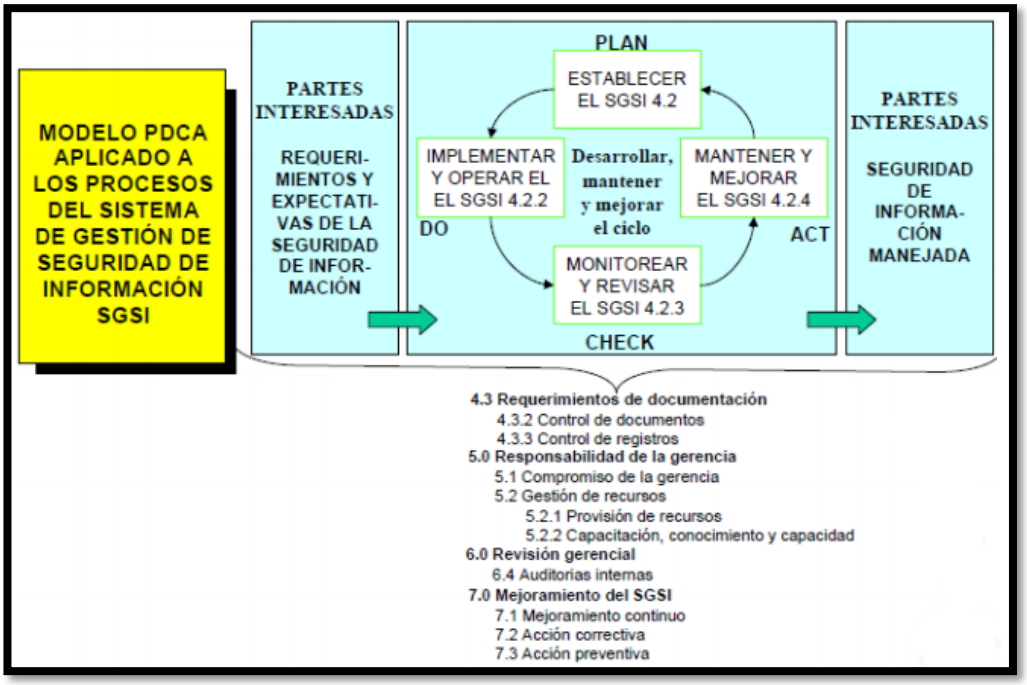


Figura 6: Modelo PDCA (Planear- Hacer-Chequear-Actuar)
Fuente: (Villacis Miguel Leopoldo, 2016, pág. 19)

2.3.2.5. Documentación Obligatoria de la Norma ISO 27001

La norma ISO requiere que se elabore la siguiente documentación:

- Alcance del SGSI
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento de riesgos (Mabel Ochoa, pág. 26)
- Informe de evaluación de riegos
- Definición de roles y responsabilidades de seguridad
- Inventario de Activos
- Uso aceptable de los activos
- Políticas de control de acceso
- Procedimiento operativo para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad de proveedores
- Procedimientos para gestión de incidentes
- Procedimiento para continuidad de la empresa o institución
- Requisitos legales y normativas. (Ochoa Mabel Catherine, 2016, pág. 26)

Registros Obligatorios

- Registro de habilidades, experiencia y calificaciones
- Monitoreo y resultados de la medición
- Programa de auditoría interna (Ochoa Mabel Catherine, 2016, pág. 26)
- Resultados de la auditoría interna
- Resultados de la revisión por parte de la dirección
- Resultados de medidas correctivas.
- Registro de actividades de los usuarios, excepciones y eventos de seguridad

2.4. HIPPA

HIPPA es el conjunto de regulaciones de aplicaciones limitadas a los EEUU fue emitida por el congreso de ese país en 1996, considerándose relativamente antigua, pero se la incluye por relevancia

en el área de la salud. Esta ley tiene la finalidad de regular y asegurar la confidencialidad e integridad sobre la información que involucra a los pacientes, evitando y proviniendo las posibles fugas de datos dentro de las casas de salud. (Quimiz Mauricio Alexander, s. f. pág. 5)

El estudio de la ley HIPPA se enfoca en la Seguridad y Privacidad denominada "Estándares de seguridad para la protección de la información médica electrónica protegida", su principal función es la protección de la información de los pacientes en relación a sus datos clínicos. ((Quimiz Mauricio Alexander, s. f. pág. 5)

Tabla 5: Requerimientos de HIPPA

Requerimientos	ID
Implementar procedimientos para verificar la identidad de la persona que solicite acceso a la información de la salud	HIPPA 1
Exigir a cada persona una contraseña o PIN	
Definir guías de procedimientos que garanticen la confidencialidad, privacidad y seguridad de la información.	HIPPA 2
Exigir algún tipo de dato biométrico como huellas dactilares, patrones de voz, patrones faciales y de iris.	
Implementar mecanismos electrónicos para corroborar que la información de la salud protegida no haya sido alterada o destruida de forma no autorizada.	HIPPA 3
Usar protocolos de comunicación de la red que garanticen que los datos enviados sean los datos recibidos	
Implementar mecanismos para cifrar y descifrar la información protegida de salud electrónica	HIPPA 4
Implementar hardware y software para registrar y examinar la actividad en los sistemas de información que contengan o utilice la información de salud.	HIPPA 5
El recurso humano debe estar acreditado para ofrecer sus servicios según reglamentos vigentes para casa profesión u oficio.	HIPPA 6
Establecer políticas y procesos para actuar frente una emergencia que altere los sistemas que contengan información de salud protegida	
Las instituciones deben certificar que cuentan con personal capacitado pata manejar la tecnología utilizada en los procedimientos de medicina.	HIPPA 7
gestionar el almacenamiento físico de toda la información del sistema	HIPPA 8

Realizado por: (Verónica Bermeo, 2021)

Fuente: (Guillen Edward Paul & Cuesta Edith Paola, 2011, pág 72)

2.4.1. Propósito Principal De La Ley HIPPA

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. (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".

2.4.2. Herramienta de Seguridad para las reglas HIPPA.

El NIST (National Institute of Standards and Technology) 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).

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.

Tabla 6: Comparación de la Norma ISO 27001 con la HIPPA

Criterios	ISO 27001	Ley HIPPA
Confidencialidad	X	X
Integridad	X	X
Disponibilidad	X	
Orientada a la Seguridad de la Información de los Pacientes		X
Sanciones a las entidades de salud por incumplimiento en el aseguramiento de la información de los pacientes		X
Respalda el consentimiento del usuario para uso adecuado de la información.		X

Se aplica a nivel Internacional	X	
Considera el análisis de riegos para mejorar la seguridad de la información	X	X

Realizado por: (Verónica Bermeo, 2021)
Fuente: (Quimiz Moreira Mauricio Alexander, s. f. pág. 6)

2.5. 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).

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 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.).

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1. Tipo y Diseño de la Investigación

3.1.1. Diseño de la Investigación

La investigación es del tipo Cuasi-Experimental ya que se escoge varios métodos, normas y buenas prácticas 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 redes corporativas de salud 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

La presente investigación es de dos tipos: aplicativo y experimental.

- Aplicativo: 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.

- Experimental: ya que se basa en pruebas realizadas en escenarios de laboratorio, en las que se observa los elementos más importantes del objeto de estudio que se investiga para obtener una captación de los fenómenos a primera vista.

3.2. Método de la Investigación

La presente investigación utilizara 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 de la hipótesis

- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis
- Difusión de resultados

3.3. Técnicas de recolección de datos

Las técnicas que serán utilizadas en la presente investigación son:
Búsqueda de información: permite obtener la información necesaria acerca del objeto de estudio de la investigación para su desarrollo, utilizando las fuentes secundarias disponibles.

- Pruebas: permite realizar experimentos en escenarios de laboratorio.
- Observación: permite determinar resultados de las pruebas realizadas en los escenarios de laboratorio.
- Análisis: permite determinar los resultados de la investigación.

3.4. Fuentes de la Información

Las principales fuentes que serán utilizadas en el estudio de investigación serán:
Primaria

- Pruebas
- Observación de resultados

Secundaria

- Tesis realizadas internacionales y nacionales de cuarto nivel
- Trabajos de investigaciones internacionales y nacionales
- Artículos científicos en base de datos de bibliotecas virtuales
- Libros especializados en la biblioteca y electrónicos
- Diccionarios especializados
- Conferencias académicas, congresos, seminarios
- Revistas indexadas y no indexadas publicadas de prestigio
- Revistas electrónicas
- Páginas de internet que brinden información confiable

Plan de Trabajo

Para la planificación del plan de trabajo se va a utilizar la Norma ISO 27001 y la Norma HIPPA que permitirá mejorar la seguridad de la información de las instituciones de Salud.

- Creación del plan de Trabajo
- Definición de las Políticas de Seguridad
- Identificación de los activos de la Información
- Enfoque del Análisis de Riesgo, Amenazas y Vulnerabilidad
- Tratamientos de los Riesgos, Amenazas y Vulnerabilidad
- Definir conjunto de objetivos y métricas
- Asignación y delimitación de responsabilidades
- Formación y Capacitación
- Documento Final

3.5. Personal Involucrado con la Información.

Es importante mencionar que en el grupo de trabajo no todos tienen acceso a la información, tienen acceso total a la información del paciente los médicos y especialistas, mientras que las enfermeras tendrán un acceso parcial a la información, los pacientes pueden tener o no acceso a la información; se debe cifrar la información más importante del paciente para impedir el acceso de personas no autorizadas. En la tabla siguiente se puede observar el acceso a la información del personal:

Tabla 7: Personal que accede a la Información

Personal	Acceso a la base de datos de la información médica	Acceso al Historial de cada Paciente	Agendar Citas Medicas	Permisos para enviar y recibir resultado de exámenes	Información de la Hoja de Vida de cada Profesional
Administrador de RED	X		X		X
Estadística	X	X	X		X
Enfermera		X		X	X

Médico o (Especialista)	X	X		X	X
Paciente			X	X	X
Usuario Externo					X

Realizado por: (Verónica Bermeo, 2021)

- Gerencia
- Director de la Tecnología
- Jefe de talento Humano
- Jefe Financiero
- Jefe de Planificación
- Representante de los Médicos, Especialista
- Represéntate de las Enfermeras

Estas áreas comprenden los procesos críticos de la institución por que se encargan directamente de la recolección, procesamiento, almacenamiento, registro, difusión y respaldo de la información de los pacientes.

La encueta se divide en 14 preguntas que son consideras relevantes e importantes por el estándar ISO 27001 y la Norma HIPPA.

3.6. Identificación y Priorización de Riesgos

3.6.1. Análisis de 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 permiten categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

3.6.2. Nivel y Probabilidad del Riesgo

El nivel de riesgo está dado por la afectación a los activos de la empresa o institución, y la probabilidad de que la amenaza se haga efectiva o no.

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.

Tabla 8: Nivel y Probabilidad del Riesgo

Nivel	Descripción	Ponderación	Probabilidad
4	Se puede generar el riesgo con una probabilidad del 80% y que la amenaza se haga efectiva	Muy Alto	0.75 - 1
3	Se puede generar el riesgo con una probabilidad del 60% y que la amenaza se haga efectiva	Alto	0.50 - 0.74
2	Se puede generar el riesgo con una probabilidad de entre el 20% y 60% y que la amenaza se haga efectiva	Medio	0.25 - 0.49
1	Se puede generar el riesgo con una probabilidad menor al 20 %	Bajo	0 - 0.24

Realizado por: (Verónica Bermeo, 2021)

3.6.3. Nivel e Impacto del Efecto

El efecto es la repercusión de manera negativa sobre el rendimiento de la red y programadores esto se genera por la explotación de las vulnerabilidades a las que están expuestas el sistema de la institución. En la tabla 3-3 puede observar la clasificación del efecto, de acuerdo al nivel de exposición del sistema a las vulnerabilidades.

Tabla 9: Calificación del Efecto

Nivel	Descriptor	Detalle
4	Muy Alto	Se ocasiona pérdida total de la información; copia total de la información por personas no autorizadas. Se debe aplicar normas, políticas o reglas para dar soluciones.
3	Alto	Pérdida irreversible de la información como modificación de la contraseña por personas no autorizadas o inescrupulosas.

2	Medio	Se genera daños reversibles a la información y para dar soluciones se debe aplicar diferentes procesos para recuperar los datos perdidos o modificados, se solita ayuda externa.
1	Bajo	Acceso a la información por personas no autorizadas que no ocasionan perdida menos modificación de la información, y se aplica procedimientos locales para dar soluciones a los problemas.

Realizado por: (Verónica Bermeo, 2021)

3.7. 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 (200).

$\sigma =$ 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 %.

$$n = \frac{200 \cdot 0{,}5^2 \cdot 1{,}645^2}{0{,}1^2(200-1) + 0{,}5^2 \cdot 1{,}645^2}$$

$$n = \frac{135{,}30125}{2{,}6665} = 50{,}741$$

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.

CAPÍTULO IV

4. RESULTADOS Y DISCUCIÓN

4.1. Análisis de la situación actual o Situación Inicial

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:

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

En Tabla se muestra los principales requerimientos de seguridad que demandan la transmisión, recepción y manejo de la información, para cumplir con estos requerimientos. Se clasifica cada requerimiento según el tipo de riesgo que generaría su ausencia en el sistema y el nivel de impacto que causaría una amenaza, si no se cumple con cada requerimiento.

Tabla 10: Respuestas y Probabilidad de ocurrencia de los riesgos identificados

ID	Amenazas	Nivel de Riesgo	Si	No	Probabilidad
1	Existe compromiso de la dirección con la seguridad de la información	2	5	45	0,9
2	Existe Controles o normas de seguridad de la información ya establecidas	4	4	46	0,92
3	Se ha realizado Inventario de los Activos de la Información	3	2	48	0,96
4	Existe un sistema de autenticación de personas que acceden a la información	3	12	38	0,76
5	Se exige contraseña de acceso a cada persona.	4	30	20	0,4
6	Existen límite en los intentos de acceso al sistema	2	0	50	1
7	Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información	2	23	27	0,54

8	Cifrado de la Información antes de ser Enviada	2	0	50	1
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	3	5	45	0,9
10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	3	0	50	1
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	2	3	47	0,94
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	2	6	44	0,88
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	3	2	48	0,96
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	2	5	45	0,9
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare	4	32	18	0,36

Realzado por: (Verónica Bermeo, 2021)

Tabla 11: Ponderación de Ocurrencia de Riesgos

ID	Amenazas	Nivel de Impacto	Probabilidad	Valor Final
1	Existe compromiso de la dirección con la seguridad de la información	4	0,9	3,6
2	Existe Controles o normas de seguridad de la información ya establecidas	3	0,92	2,76
3	Se ha realizado Inventario de los Activos de la Información	3	0,96	2,88
4	Existe un sistema de autenticación de personas que acceden a la información	2	0,76	1,52
5	Se exige contraseña de acceso a cada persona.	2	0,4	0,8
6	Existen límite en los intentos de acceso al sistema	3	1	3
7	Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información	2	0,54	1,08
8	Cifrado de la Información antes de ser Enviada	4	1	4
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	4	0,9	3,6

10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	2	1	2
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	2	0,94	1,88
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	1	0,88	0,88
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	2	0,96	1,92
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	4	0,9	3,6
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare	3	0,36	1,08

Realizado por: (Verónica Bermeo, 2021)

Representación Gráfica del nivel de Riesgo:

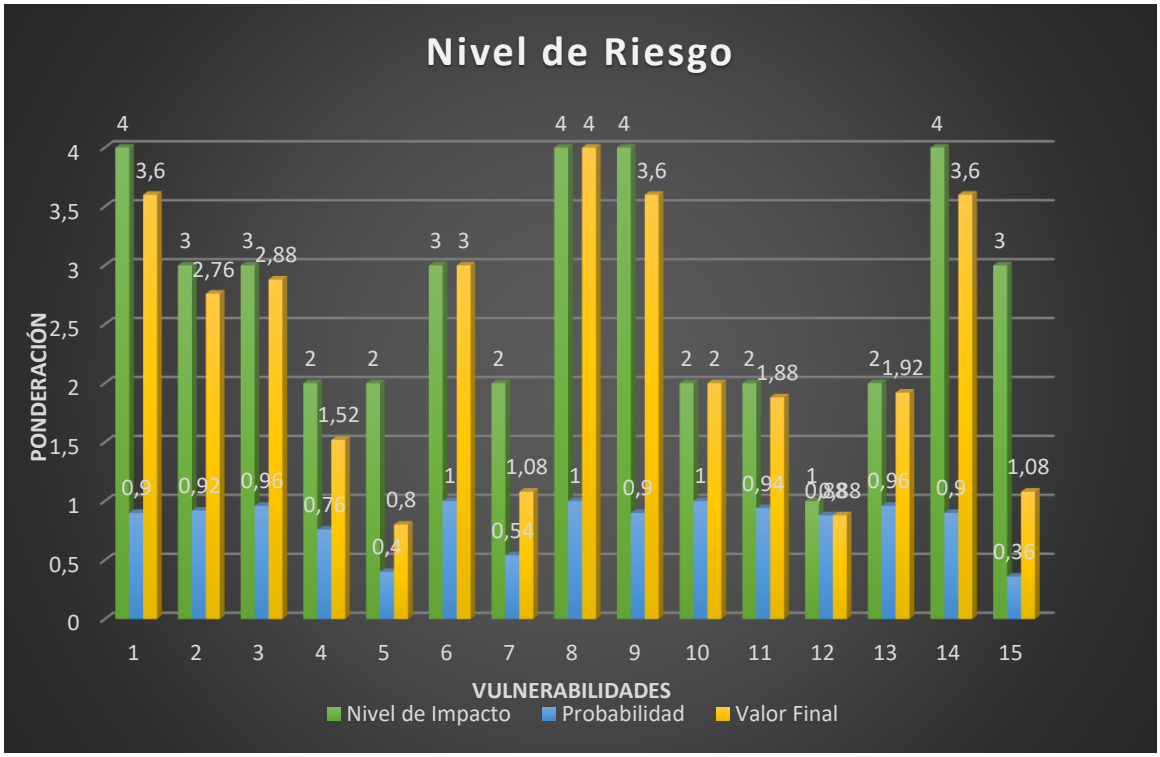


Gráfico 1: Nivel de Riesgo e Impacto de las vulnerabilidades
Realizado por: (Verónica Bermeo, 2021)

El gráfico muestra que el sistema no cumple con alguno de los requerimientos establecidos por las Normas ISO 27001 y HIPPA, y se corre el riesgo de que alguna amenaza o modificación a la

información, pueda generar un impacto negativo en la integridad de la misma. Los riegos con ponderaciones superiores 2.88 son los más críticos y se debe implementar con urgencia una solución para la protección de la información del área médica.

La ecuación permite conocer en qué nivel de riesgo se encuentra un sistema, debido a la falta de implementación de requerimientos establecidos por las Normas ISO 27001 y HIPPA en cuanto a la seguridad de la información.

$$Nivel\ de\ Riesgo = \frac{Personas\ Encuestadas}{Número\ de\ Preguntas}$$

$$Nivel\ de\ Riesgo = \frac{50}{15}$$

$$Nivel\ de\ Riesgo = 3{,}33\ \approx 3$$

Se puede concluir que el sistema no cumple con los requerimientos establecidos en las Normas ISO 27001 y HIPPA y que se encuentra en un nivel de riesgo alto, con una probabilidad entre el 60% y el 100% de que una amenaza se haga efectiva.

Nos podemos dar cuenta que se está afectando directamente 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 12: Situación Post – Implementación

ID	Amenazas	Nivel de Riesgo	Si	No	Probabilidad
1	Existe compromiso de la dirección con la seguridad de la información	1	27	23	0,46
2	Existe Controles o normas de seguridad de la información ya establecidas	2	28	22	0,44
3	Se ha realizado Inventario de los Activos de la Información	1	23	27	0,54
4	Existe un sistema de autenticación de personas que acceden a la información	3	33	17	0,34
5	Se exige contraseña de acceso a cada persona.	2	42	8	0,16
6	Existen límite en los intentos de acceso al sistema	1	29	21	0,42
7	Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información	1	37	13	0,62
8	Cifrado de la Información antes de ser Enviada	1	22	28	0,56
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	2	40	10	0,2
10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	1	36	14	0,28
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	1	37	13	0,26
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	1	39	11	0,22
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	2	29	21	0,42
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	1	33	17	0,34
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare	2	47	3	0,06

Realizado por: (Verónica Bermeo, 2021)

Tabla 13: Ponderación de Ocurrencia de Riesgo

ID	Amenazas	Nivel de Impacto	Probabilidad	Valor Final
1	Existe compromiso de la dirección con la seguridad de la información	2	0,46	0,92
2	Existe Controles o normas de seguridad de la información ya establecidas	2	0,44	0,88
3	Se ha realizado Inventario de los Activos de la Información	1	0,54	0,54
4	Existe un sistema de autenticación de personas que acceden a la información	1	0,34	0,34
5	Se exige contraseña de acceso a cada persona.	1	0,16	0,16
6	Existen límite en los intentos de acceso al sistema	2	0,42	0,84
7	Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información	1	0,62	0,62
8	Cifrado de la Información antes de ser Enviada	3	0,56	1,68
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	3	0,2	0,6
10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	1	0,28	0,28
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	1	0,26	0,26
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	1	0,22	0,22
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	1	0,42	0,42
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	2	0,34	0,68
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare	1	0,06	0,06

Realizado por: (Verónica Bermeo, 2021)

Representación Gráfica del nivel de Riesgo Post - Implementación

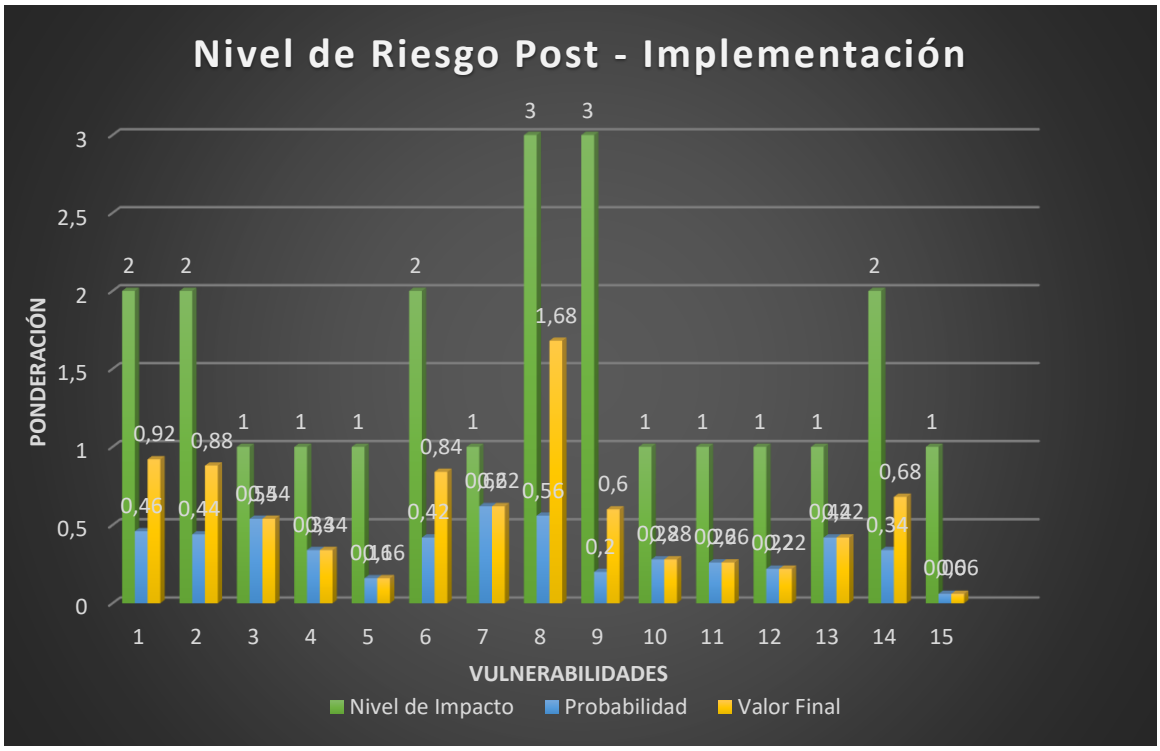


Gráfico 2: Nivel de Riesgo Impacto de las vulnerabilidades
Realizado por: (Verónica Bermeo, 2021)

El gráfico muestra que el sistema cumple con la mayoría de los requerimientos establecidos por las Normas ISO 27001 y HIPPA, y no se corre el riesgo de que alguna amenaza o modificación a la información, pueda generar un impacto negativo en la integridad de la misma. La protección en la información en el área médica ha sido implementada de acuerdo a las Normas ISO 27001 y HIPPA obteniendo una disminución de los riegos con valores menores a 1,68.

Se puede concluir que el sistema actualmente cumple con los requerimientos establecidos en las Normas ISO 27001 y HIPPA y que se encuentra en un nivel de riesgo bajo, con una probabilidad entre el 60% y el 80% de que una amenaza no se haga efectiva.

Se puede observar que la información sensible del usuario y personal del centro de Salud cuenta con medidas correctivas ante vulnerabilidades que se pueden presentar y se garantiza su Confidencialidad, Privacidad, Integridad de dicha información.

En base a este análisis se puede establecer que los riesgos de ponderación superior a los 2.88 que se establecieron en el estudio inicial han disminuido notablemente como se puede observar en la siguiente tabla:

Tabla 14: Comparación de los Riesgos en Situación Inicial con la Post – Implementación

ID	Amenazas	Situación Inicial	Post Implementación
1	Existe compromiso de la dirección con la seguridad de la información	3,6	0,92
2	Existe Controles o normas de seguridad de la información ya establecidas	2,76	0,88
3	Se ha realizado Inventario de los Activos de la Información	2,88	0,54
4	Existe un sistema de autenticación de personas que acceden a la información	1,52	0,34
5	Se exige contraseña de acceso a cada persona.	0,8	0,16
6	Existen límite en los intentos de acceso al sistema	3	0,84
7	Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información	1,08	0,62
8	Cifrado de la Información antes de ser Enviada	4	1,68
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	3,6	0,6
10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	2	0,28
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	1,88	0,26
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	0,88	0,22
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	1,92	0,42
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	3,6	0,68
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare	1,08	0,06

Realizado por: (Verónica Bermeo, 2021)

Representación gráfica de la comparación de ponderaciones Inicial vs Post – Implementación

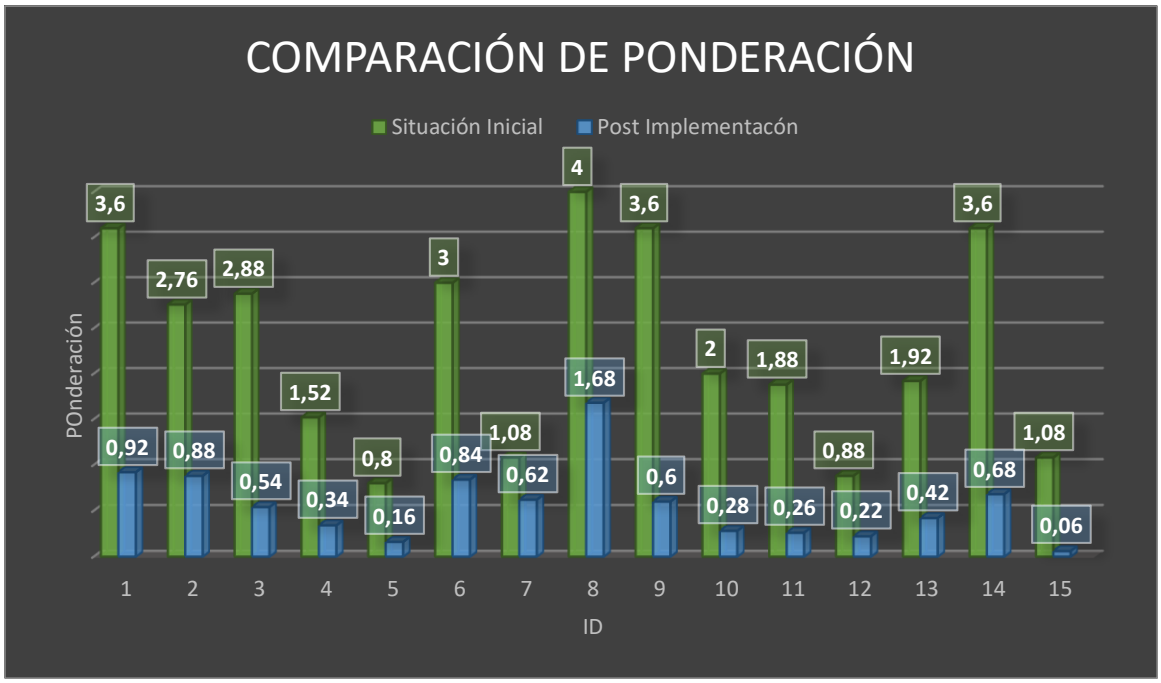


Gráfico 3: Comparación de Ponderación situación Inicial y Post – Implementación
Realizado por: (Verónica Bermeo, 2021)

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 15: Porcentaje de Reducción de Riesgos Inicial vs Post - Implementación

ID	Amenazas	Porcentaje de Situación Inicial	Porcentaje Post Implementación	Porcentaje de Reducción del Riesgo
1	Existe compromiso de la dirección con la seguridad de la información	90%	23%	67%
2	Existe Controles o normas de seguridad de la información ya establecidas	69%	22%	47%
3	Se ha realizado Inventario de los Activos de la Información	72%	13,5%	58,5%
4	Existe un sistema de autenticación de personas que acceden a la información	38%	8,5%	29,5%
5	Se exige contraseña de acceso a cada persona.	20%	4%	16%
6	Existen límite en los intentos de acceso al sistema	75%	21%	54%
	Existe normas, políticas, protocolos y guías para garantizar la			

7	confidencialidad, privacidad y seguridad de la información	27%	15,5%	11,5%
8	Cifrado de la Información antes de ser Enviada	100%	42%	58%
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	90%	15%	75%
10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	50%	7%	43%
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	47%	6,5%	40,5%
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	22%	5,5%	16,5%
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	48%	10,5%	37,5%
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	90%	17%	73%
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare	27%	1,5%	25,5%

Realizado por: (Verónica Bermeo, 2021)

Representación gráfica de los porcentajes de Reducción de Riesgos: Inicial vs Post – Implementación

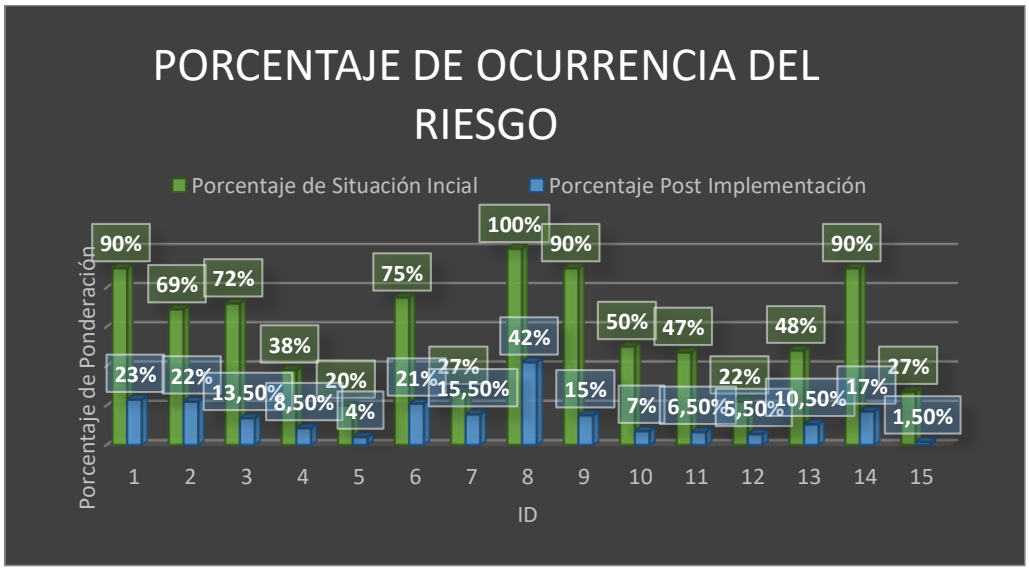


Gráfico 4: Comparación de ponderación de riesgos Iniciales Vs Post – Implementación

Realizado por: (Verónica Bermeo, 2021)

Representación gráfica de los porcentajes de Reducción de Riesgos

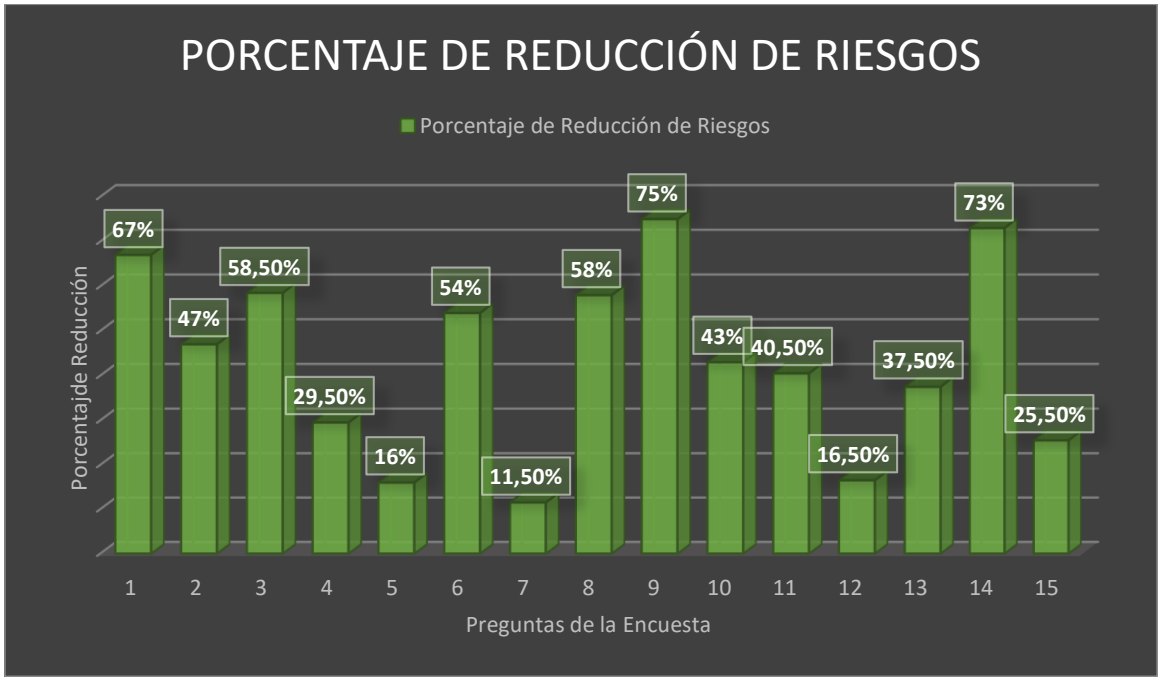


Gráfico 5: Porcentaje de reducción de Riesgos
Realizad por: (Verónica Bermeo, 2021)

Como se puede observar en el gráfico el porcentaje de reducción de riesgos es de manera significativa, las puntuaciones de mayor prevalencia en el análisis inicial tuvieron una disminución después de haberse aplicado el modelo en base a las Normas ISO 27001 y HIPPA en Seguridad de la Información se ha reducido sustancialmente la ponderación de la probabilidad de que los riesgos de un 90 a un 75 por ciento.

4.3. Comprobación de la Hipótesis

Para demostrar la hipótesis esta es sometida a diferentes pruebas que permiten determinar si es verdadera, falsa o nula, de acuerdo a los resultados obtenidos.

La prueba que se va a utilizar es la T de Student que perite determinar algunos de los parámetros de confianza con una distribución T de Student esta 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.

Hipótesis de investigación (Hi)

La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos de seguridad en redes de Corporativas de Salud.

Hipótesis de Nula (H0):

La Adaptación de las Normas ISO 27001 e HIPAA no permitirá la reducción de riesgos de seguridad en redes de Corporativas de Salud.

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

Hipótesis Alternativa (H1):

La Adaptación de las Normas ISO 27001 e HIPAA permitirá la reducción de riesgos de seguridad en redes de Corporativas de Salud.

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

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

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.

$$\alpha = 0.05$$

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.

4.3.1. Regla de decisión

Caso 1.

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

Caso 2.

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

Análisis

Los datos obtenidos en la investigación fueron evaluados en el software SPSS que permite de forma automática ejecutar las fórmulas 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 16: Datos de respuestas Probabilidad de ocurrencia de riesgos identificados Post-Implementación

ID	Amenazas	Situación Inicial	Post Implementación
1	Existe compromiso de la dirección con la seguridad de la información	3,6	0,92
2	Existe Controles o normas de seguridad de la información ya establecidas	2,76	0,88
3	Se ha realizado Inventario de los Activos de la Información	2,88	0,54
4	Existe un sistema de autenticación de personas que acceden a la información	1,52	0,34
5	Se exige contraseña de acceso a cada persona.	0,8	0,16
6	Existen límite en los intentos de acceso al sistema	3	0,84
7	Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información	1,08	0,62
8	Cifrado de la Información antes de ser Enviada	4	1,68
9	Existe protocolos o estándares de red que garantice que los datos enviados sean los recibidos	3,6	0,6
10	Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuestas a cambios ambientales u operacionales que afecten la seguridad de la información.	2	0,28
11	Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra lo sistemas	1,88	0,26
12	El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente	0,88	0,22
13	Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no puedan acceder a la información	1,92	0,42
14	El personal del hospital revisa de manera periódica la políticas y procedimientos de seguridad de la información (manual)	3,6	0,68
15	Se tiene conocimiento del procedimiento que se debe tomar cuando el sistema tiene Malvare o virus	1,08	0,06

Realizado por: (Verónica Bermeo, 2021)

Al analizar los datos obtenidos en la tabla 6-4 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

Figura 7: Tabla de Descriptivos de la Normalidad
Realizado por: (Verónica Bermeo, 2021)

En promedio de los riesgos de amenazas inicial es 2.31 mayor que los riesgos de amenaza post implementación igual 0.57; además las amenazas de riesgo inicial presentan 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.

Figura 8: Normalidad distribución de Kolmorogov-Smirnov y Shapiro-Wilk
Realizado por: (Verónica Bermeo, 2021)

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

Figura 9: Estadísticas de muestras emparejadas
Realizado por: (Verónica Bermeo, 2021)

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

Figura 10: Pruebas de muestras emparejadas
Realizado por: (Verónica Bermeo, 2021)

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 en redes de Corporativas de Salud., puesto que se obtuvieron resultados favorables.

CAPÍTULO V

5. Modelo de adaptación de las Normas ISO 27001 e HIPPA

Para el desarrollo del plan de seguridad de la información se cuenta con varias estrategias como son: 1) el estudio de la situación actual y de la definición de requerimientos, 2) se realiza la producción y ejecución de las estrategias, 3) monitoreo de estas estrategias. El monitoreo de las estrategias permite identificar las vulnerabilidades del sistema; cada proceso se realimenta con los otros como se puede observar en la figura siguiente:

Figura 71: Ciclo de planeación de estrategias del sistema
Realizado por: (Verónica Bermeo, 2021)

Tabla 17: Fases de Implementación del Modelo de adaptación de Seguridad de Información y la relación con los numerales de la Norma ISO 27001

Fases	Etapas	Numerales de la Norma ISO 27001
Fase 1. **Obtener la aprobación del director del Centro de Salud.**	Determinar las prioridades o activos importantes de la organización para el proyecto. Definir el alcance del proyecto. Creación del Plan de trabajo y personal encargado.	1. Conocimiento de las instalaciones de la institución y su contexto. 2. Ver las necesidades y expectativas del personal involucrado con el usuario. 3. Compromisos y Liderazgos del Personal. 4. Recursos con los que se cuenta para el desarrollo del proyecto.
Fase 2. **Definir el alcance, límites y políticas del proyecto.**	Definir el alcance y límites de las Tecnologías de Información y su medio de comunicación. Definir alcances y límites de manera física. Definir cada alcance y límite con el proyecto a ser ejecutado. Desarrollo de las políticas Administrar roles y responsabilidades del proyecto.	5. Determinación del alcance del proyecto de seguridad de la información. 6. Compromisos y liderazgos por el personal encargado. 7. Objetivos y cumplimiento de la seguridad de la información. 8. Roles y responsabilidades por parte de las autoridades de la institución. Personal Competente.
Fase 3. **Hacer el análisis de los requisitos de seguridad de la información**	Definir los requisitos para la seguridad de la información y correcta elaboración del proyecto. Identificar los activos más importantes del Instituto de Seguridad Social IESS de Guaranda. Realizar una evaluación de la seguridad de la información en el del Instituto de Seguridad Social IESS de Guaranda.	9. La institución debe garantizar la seguridad de la información de todos los usuarios. 10. Valorar los Riesgos de la Seguridad de la Información.
	Realizar la valoración de los riesgos.	11. Valorar o Ponderar los riesgos que afecta la seguridad de la información.

Fase 4. **Realizar la valoración de los riesgos y planificar el tratamiento de los mismos**	Seleccionar los objetivos de controles. Obtener la autorización del director del centro de Salud para el proyecto.	12. Procesamiento de Riesgos de la seguridad de la información. Planes y objetivos para la seguridad de la información. 13. Compromisos y Liderazgos.
Fase 5. **Diseño del plan de la Seguridad de la Información.**	Diseño de seguridad de la información de la institución. Diseño especifico de las soluciones para los riesgos. Producir el proyecto de Plan específico.	14. Planificación y control operacional. Comunicación e información documentada. 15. Valoración de los riesgos de seguridad de la información. Procesamiento de riesgos de la seguridad de la información. 16. Seguimiento, medición y evaluación del plan de proyecto. Comunicación dl sistema implementado para la reducción de riesgos dentro de la institución.

Realizado por: (Verónica Bermeo, 2021)

La implementación está formada por cinco fases secuenciales, a continuación, se detalla cada una de ellas.

Fase 1: Obtener la aprobación del director del Instituto de Seguridad Social IESS de Guaranda.

Se debe tener en cuenta que el proyecto no constituye un propósito exclusivo del área Informática, sino que representa un proyecto institucional de tal maneara se debe tener la aprobación de la dirección y del área administrativa para continuar con su implementación.

Se debe conocer a ciencia cierta las prioridades que tiene la institución para llevar a cabo la implementación de un plan de seguridad de la información, para lo cual se recomienda tomar en cuenta los siguientes elementos:

1) objetivos estratégicos de la institución.

2) requisitos normativos relacionados con la seguridad de la información.

3) sistemas de gestión existentes.

En primer lugar, se debe conocer que recursos se desea proteger y con base a ello, se puede determinar de forma preliminar el alcance, este debe incluir un resumen de los requerimientos establecidos por la administración y las obligaciones impuestas de manera externa a la institución. El primer paso para promover su diseño e implementación es delimitar con precisión los tiempos, recursos y personal requerido, para ello, es necesario utilizar herramientas de gestión de proyectos existentes en el mercado.

Fase 2: Definir el alcance, límites y política del proyecto

Para el alcance se debe fundamentar y delimitar el proceso de gestión de riesgos, y para la implementación de un Sistema de Gestión de Seguridad de la Información se debe tener en claro los recursos o activos que se van a proteger.

Las políticas y objetivos van a reflejar lo que la institución desea hacer con relación a la seguridad de la información, en base a requisitos legales y reglamentos, además hay que tomar en consideración el compromiso de la parte administrativa para lograr conseguirlo. Una de las maneras de demostrar el apoyo de la Administración es la aprobación tanto de los objetivos como de las políticas del proyecto dentro del alcance definido.

Fase 3: Hacer el análisis de los requisitos de seguridad de la información

Para la seguridad de la información necesariamente hay que tomar en consideración los siguientes elementos:

1) identificar los activos de la Institución

2) identificar la visión de la institución

3) identificar las formas actuales de procesamiento de información

4) identificar los requisitos legales

5) identificar el nivel de conocimientos sobre el tema seguridad de la información

La institución posee un sinnúmero y variedad de activos tecnológicos, y tratar de establecer y clasificar estos activos puede ser una tarea difícil, los activos que se toman en cuenta son: datos electrónicos, documentos físicos y miles de dispositivos y usuarios. La norma en estudio establece activos de dos tipos: primarios y de soporte. Los primeros constituyen los procesos de negocio y la información, mientras que los últimos constituyen aquellos de los cuales dependen los activos primarios y pueden clasificarse de la siguiente manera: software, hardware, personal, redes, estructura, instalación y ubicación de la institución.

Fase 4: Realizar la valoración de los riesgos y planificar el tratamiento de los mismos.

Esta fase es el eje fundamental del proyecto y es necesario tener en cuenta los siguientes aspectos:

- Establecimiento de contexto: Es el proceso de preparación de riesgos con alcance, objetivos, políticas y parámetros de evaluación.

- Parámetros de probabilidad: Para los parámetros de probabilidad es necesario realizar una tabla de frecuencias de la posible ocurrencia de las amenazas, con los niveles requeridos en relación a las diferentes necesidades de la institución.

- Parámetros de impacto: Estos parámetros son definidos en función de las consecuencias que podrían tener cualquier amenaza sobre la información o los activos en lo referente a la integridad, confidencialidad y disponibilidad.

- Determinación de la vulnerabilidad: Es la materialización de una amenaza sobre la información; por lo tanto, en términos generales la vulnerabilidad es medible en términos porcentuales, además en función de los parámetros definidos anteriormente (probabilidad e impacto).
  La valoración del riesgo contempla tres fases: identificación del riesgo, estimación del riesgo y evaluación del riesgo.

    - La identificación de riesgos es determinar qué va a suceder, cómo, dónde y por qué podría ocurrir esta pérdida.

    - Para estimar el riesgo, se puede llevar a cabo: análisis cualitativo, semi cuantitativo o cuantitativo, o bien, una combinación de los tres.

- La evaluación del riesgo consiste en realizar una comparación de las vulnerabilidades resultantes de cada riesgo y confrontarlas contra el nivel de aceptación de riesgo.

- Los resultados obtenidos de la evaluación de riesgos permitirán diseñar informes de vulnerabilidad por cada criterio de seguridad de la información y diversos indicadores que ayudan a monitorear el nivel de avance en la gestión del riesgo.

- El tratamiento de riesgos establece acciones a desarrollar, mediante los controles propuestos, para llevar el riesgo detectado a un nivel aceptable dentro de la institución.

Fase 5: Diseño del plan de Seguridad de la Información

El diseño del Proyecto se encuentra conformado por tres componentes:

- la documentación que debe tener el sistema,
- la implementación de los controles previstos en el plan de tratamiento de riesgos
- el monitoreo constante de la seguridad de la información.

La información que debe tener el sistema posee requisitos de la Norma ISO 27001 y HIPPA, las mismas que tienen su origen a partir de la implementación de sus diferentes fases.

La implementación del plan de tratamiento de riesgos aprobado por la Administración y el mantenimiento de los controles existentes, es lo que permite garantizar niveles aceptables de seguridad de la información.

La evaluación del desempeño del sistema de seguridad de la información se realiza mediante la supervisión, medición, análisis y evaluación del sistema.

Figura 82: Resumen de los Pasos a Seguir para la Implantación del Sistema
Realizado por: (Verónica Bermeo, 2021)

5.1. Organización de la Seguridad de la Información

En los centros de Salud se debe formar los comités que permitan la coordinación de la seguridad de la información de manera periódica llevando un registro documentado de:

- Hacer una Acta de compromiso del director del del Instituto de Seguridad Social IESS de Guaranda con la seguridad de la información.
- Delegar responsabilidades de la Coordinación de la Gestión de la Seguridad de la Información.
- Delegar responsabilidades para la seguridad de la información.
- Autorizar nuevos servicios de procesamiento de la información.
- Redactar acuerdos de Confidencialidad.
- Revisión independiente de la seguridad de la información

- Identificación de los riesgos

5.2. Seguridad de los Recursos Humanos

Todas las personas que tienen contacto con la información deben documentar claramente sus funciones, responsabilidades, términos, condiciones laborales, terminaciones de contrato, devolución de activos. Esta información se la debe hacer en formularios generados por el Director de Talento Humano.

5.3. Control de Acceso

Las Políticas de control de acceso se la deben realizar mediante perfiles y contraseñas como principal activo del Instituto de Seguridad Social IESS de Guaranda, tomando como política:

- Uso de contraseñas.
- Bloqueo de pantalla.
- 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.

5.4. Incidentes de la Seguridad de la Información

Se debe elaborar Reportes sobre los eventos de seguridad de la información emitiendo Reportes sobre:

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

5.5. Políticas y Sanciones

5.5.1. Políticas relacionadas al uso de Tecnologías.

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

Ámbito. - Las Políticas de Tecnología de la Información serán aplicadas de manera obligatoria por los funcionarios, servidores y trabajadores del centro de salud que utilicen el hardware, software para el cumplimiento de sus actividades diarias.

Recursos Tecnológicos. - Las Políticas de Tecnología de la Información regularán el uso de los recursos informáticos en el centro de salud y pone a disposición de todo el personal para desarrollar sus actividades.

5.5.2. Políticas para la Contraseña

Los usuarios (servidores, trabajadores y funcionarios) deben cumplir con todas las políticas establecidas para el uso correcto de las contraseñas, y que el acceso a la información solo sea por el personal autorizado; todos los equipos, sistemas deben tener un mecanismo de contraseñas como por ejemplo al inicio de sesión se debe pedir la contraseña para que pueda acceder al sistema.

- Todas las contraseñas son personales y no se pueden trasferir.
- Las contraseñas se deben cambiar por lo menos unas 3 veces al año.
- Las contraseñas deben cumplir con algunos requerimientos como: tener letras mayúsculas, letras minúsculas, números y caracteres especiales con un mínimo de 8 dígitos.
- Las contraseñas no deben tener secuencia de números, fechas, nombres de personas ha llegadas.
- Cuando el personal se desvincule de la institución o cambie de rol dentro de la misma se debe informar al personal encargado para suspender los usuarios.

5.5.3. Políticas para el uso del Correo Electrónico

Los funcionarios, servidores y usuarios deben hacer el uso correcto del correo electrónico porque es una herramienta de comunicación dentro de la institución.

- La comunicación entre el personal de la institución solo se lo hará por el correo institucional para evitar perdida de información.
- El responsable de esta área podrá modificar, bloquear o habilitar los servicios de correo electrónico cunado lo crea pertinente sea por razones administrativas, de mantenimiento o por otras causas.
- En cualquier momento el responsable de esta área podrá cancelar o inhabilitar la cuenta de cualquier usuario sin previo aviso e incluso eliminar ésta por falta de uso, o si considera que el usuario ha transgredido las reglas establecidas.
- Las direcciones electrónicas estarán formadas por el apellido, inicial del nombre y la inicial del segundo apellido.
- Los servicios de correo electrónico serán administrados por el Área de Informática los que serán responsable de velar por el correcto funcionamiento y operación de dichos servicios.
- No se deberá utilizar el correo electrónico para actividades comerciales ajenas a la institución.
- No se deberá utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad del emisor del correo electrónico para actos inapropiados.
- Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.

5.5.3.1. Tipo de cuentas

Existen tres tipos de cuentas dentro de una institución:

- **Cuentas Personales:** El personal de centro de salud contará con una cuenta de correo en el servidor de la Institución cuya dirección electrónica estará formada por la inicial del nombre, el apellido y la inicial del segundo apellido.
- **Cuentas Temporales:** Estas cuentas se crearán bajo un propósito específico y con un tiempo de validez para después ser borrado una vez que ya no se la necesite.
- **Cuentas Departamentales:** Estas cuentas serán creadas, con el objetivo de comunicación a todos los miembros de una determinada dirección o lista de usuarios específica.

5.5.4. Políticas de Seguridad de la Información

Los usuarios deberán cumplirán las siguientes recomendaciones:

- Bloquear el equipo de trabajo cuando se esté utilizando para evitar la pérdida de información.
- 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.
- Una de las normativas prohíbe la instalación de aplicaciones, programas que no estén debidamente notificadas al área técnica de información.
- El usuario deberá sacar respaldos de la información en discos extraíbles, o a su vez subirlos a la nube para evitar perdida de la información y que a su vez esté disponible en cualquier momento.
- Los trabajadores, funcionarios y servidores de la institución deben firmar hojas de compromiso que garantice la confidencialidad y no divulgación de la información.
- Los responsables de la seguridad de la información deben clasificar, manejar, trasmitir, comunicar y almacenar de manera correcta los datos generados dentro de la institución.
- Los custodios de la información deben respaldar y almacenar la información que poseen a su cargo, en general son los que están a cargo de la base de datos
  También se encargan de la integridad, disponibilidad, acceso y permisos para acceder a la información.
- 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.

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

1. Clasificación de la Información:

a) Valor: Es el principal criterio de clasificación, está basada en el valor del activo desde el punto de vista del negocio.
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:

a) PUBLICA: Es la información visible o divulgada por el personal de la organización, clientes o el público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad de la organización.

b) SENSIBLE: Solo para uso interno y exclusivo por parte de los empleados de la organización su divulgación y visibilidad es dentro de la institución de manera segura; cuando la divulgación es fuera de la institución puede tener un impacto leve en la privacidad del personal o causar un daño leve a la imagen de la organización.

c) RESTRINGIDA: La información es de uso exclusivo de la organización, se puede acceder y visualizar solo por el personal de la organización que cuente con la autorización del jefe de área informática. La divulgación o visualización no autorizada dentro de la organización o fuera de ella podría violar la privacidad de personas, causar un daño significativo a la institución

d) CONFIDENCIAL: Es la información sensible y está destinada a uso solamente interno y por parte del personal que poseen permisos y autorización, si no posee autorización causaría una violación a la privacidad de las personas y produciría ocasionar un daño grave o irreparable a la imagen de la organización.

5.6. Guía de buenas prácticas de seguridad de la información para el personal

En la siguiente tabla se puede observar la guía de buenas prácticas de la seguridad de la información obtenida de las recomendaciones, normas y estándares revisados y está orientada al personal. 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 que se encuentras en el ANEXO A de normas y recomendaciones de seguridad para el ámbito de los centros de salud.

Tabla 18: Guía de buenas prácticas de seguridad de la información para el personal

ID	Detalle	Estándares y Normas
Contraseñas	La contraseña se debe cambiar en un tiempo determinado. La contraseña debe tener por lo menos 8 dígitos. Debe estar compuesta por letras mayúsculas, minúsculas, números y caracteres especiales. La contraseña no debe ser compartida con nadie y menos guardada en el navegador.	11, 16 4, 11,15,16 1,4,11,15,16 1, 4, 11, 15, 16, 22
Correo Electrónico	No se debe consultar cuentas personales desde el lugar de trabajo. No se debe utilizar el correo electrónico de trabajo para fines personales. Se debe encriptar los correos electrónicos que tengan datos del personal del centro de salud.	1, 22 1, 9, 22 1, 2, 5
Uso de dispositivos y medios extraíbles	Se debe pedir permiso para sacar información personal en un medio extraíble. Se debe codificar la información personal que sale del centro de salud en un medio extraíble. Se debe tener precaución con los medios extraíbles para evitar el contagio de virus dentro de la institución.	1, 6, 16, 19, 22 2, 10, 16, 19, 22 1, 16, 19, 22
Uso de equipos	Se debe cerrar la sesión, bloquear o apagar la pantalla cuando se vaya a ausentar. La información sensible no debe ser guardada en ordenadores compartidos con otros trabajadores. Borrar la memoria de impresoras y fotocopiadoras la información que tenga información personal de los usuarios.	1, 2, 7, 16, 22 1, 22 1, 22
Instalación de Software	No se debe instalar software que no estén relacionados con las funciones del puesto de trabajo. Se debe tener precaución con el software que se va instalar esté libre de virus.	7, 16 1, 16
Seguridad	Se debe tener conocimiento sobre los protocolos para detección de amenazas. Se debe dar a conocer sobre cualquier anomalía en el funcionamiento de la computadora al encargado de esa área.	1, 16 1, 16

Realizado por: (Verónica Bermeo, 2021)

CONCLUSIONES

- La conclusión más importante que se puede obtener es la reducción de riesgos presentes en el sistema, esto se da por la implementación del modelo de seguridad de la información en el centro de Salud, el porcentaje de reducción de riesgo es del 43,5 % frente a la situación inicial que es del 50%, esto se lo realizo en dos fases inicial y post implementación, generando una mejoría en la seguridad de la información basadas en confidencialidad y privacidad.
- Se puede concluir que las normas ISO 27001 e HIPPA poseen requerimientos en común para políticas de seguridad de la información como respaldos, contraseñas, designación de responsabilidades, análisis de riesgos, sanciones, tratamiento de riesgos y todo está enfocado al sector de la Salud.
- El estudio de esta propuesta concluye que la presente es alcanzable, medible, coherente y que genera cambios positivos y sostenibles en el manejo seguro de la información de la institución, dado el rol clave que cumple la información en cada proceso hospitalario, y minimizar riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada.
- El principal problema que se encontró para el desarrollo del presente proyecto son los escasos estudios desarrollados en materia de la Normativa ISO/IEC 27001 y la Norma HIPPA aplicada al sector de la salud en el Ecuador, lo cual provoco varios inconvenientes para el desarrollo del mismo.
- Luego de analizar los principales requerimientos establecidos por las normas ISO 27001 y HIPPA para la seguridad de la información, se evaluó el nivel de riesgo e impacto que puede generar la no implementación de estos requerimientos y poner en peligro la confidencialidad de la información. Luego de la evaluación, se hace evidente que evadir requerimientos como: implementar protocolos de comunicación, mantener un respaldo de la información, limitar acceso de personal y definir políticas de acceso a la información, se genera riesgo muy alto que afecta la integridad de la información dentro de la institución.

RECOMENDACIONES

- Se recomienda implementar esta propuesta de seguridad de la Información basado en las Normas ISO 27001 e HIPAA para la reducción de riesgos de la información en los centros de salud a nivel nacional, puesto que se obtuvieron resultados favorables.

- El Estado deben implementar políticas para proteger la información de todos sus usuarios, estos mecanismos están definidos por regulaciones internacionales diseñadas específicamente para manipular la información en el sector de la salud; estos mecanismos permiten mejorar la calidad de servicio y brindar mayor seguridad.

- En futuras investigaciones se propone adaptar la metodología propuesta en diferentes instituciones que no necesariamente estén inmersos dentro del sector de la salud, sino que esté disponible para organizaciones que necesiten manejar un Sistema de Gestión de la Seguridad de Información con la finalidad de salvaguardar la información existente.

- El nivel de seguridad que se puede alcanzar ante la implementación de este modelo de la seguridad de la información basado en las normas debe ser administrado por una persona con basto conocimiento de Seguridad de la Información, y debe ser incorporado a la plantilla de personal de cada centro de salud.

BIBLIOGRAFIA

Benítez, 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. https://doi.org/10.1136/jamia.2009.000026

Colegio Oficial de Ingenieros de Telecomunicaciones. (s. f.). *Implantación de Sistema de Gestión de la Seguridad de la Información SGSI según la Norma ISO 27001* (Guía de Iniciación a Actividad Profesional). Colegio Oficial Ingeniero de Telecomunicaciones. https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Crespo Martínez Paul Esteban. (s. f.). *Metodologia de la Seguridad de la Información para la Gestion de Riesgo Informatico aplicable a MMYPES* [Universidad de Cuenca]. http://dspace.ucuenca.edu.ec/bitstream/123456789/26105/1/Tesis.pdf

Castillo Peñaherrera Cristian & SECRETARIA NACIONAL DE LA ADMINISTRACION PUBLICA. (2013). *Acuerdo Ministerial 166*. Registro Oficial Suplemento 88.

Guillen Pinto Edward Paul, R**amírez López Leonardo Juan. & Estupiñán Cuesta Edith Paola**. (2011). *Análisis de Seguridad para el Manejo de la Información Médica en Telemedicina*. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-81702011000200004

ISO 27001—Information security management. (s. f.). Recuperado 17 de febrero de 2015, de http://www.iso.org/iso/es/home/standards/management-standards/iso27001.htm

ISO IEC. (2005). *ESTÁNDAR INTERNACIONAL ISO/IEC 27001*. ISO/IEC. https://www.iso.org

LA PROTECCIÓN DE DATOS PERSONALES - Derecho Ecuador. (s. f.). Recuperado 21 de febrero de 2015, de http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2011/02/07/la-proteccion-de-datos-personales

Mazorra Olmedo Erik Ramiro. (2019). *Metodología para la Implementación de un Sistema de Gestión de Seguridad de la Información ISO/IEC 2700. Para Soporte de Áreas de Admisión y Atención de un Hospital Público. M*aestría en Auditoria de Tecnologías de la Información.

[Universidad Espíritu Santo]. http://repositorio.uees.edu.ec/bitstream/123456789/2925/1/MAZORRA%20OLMEDO%20ERIK%20RAMIRO.pdf

National Institute of Standards and Technology. (2008). *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). *HIPAA Security Rule Toolkit User Guide*. National Institute of Standards and Technology.

Ochoa Quezada Mabel Catherine. (2016). *Implementación de la Norma ISO/IEC 27001 para la Seguridad de Data Center del GAD Municipal del Cantón Cuenca. Facultad de Ciencias Tecnológicas. Escuela de Ingeniería Electrónica.* [Universidad del Azuay]. http://dspace.uazuay.edu.ec/bitstream/datos/5733/1/12053.pdf

Quimiz Moreira Mauricio Alexander. (s. f.). *Estudio de la Seguridad de la Información de los Pacientes en los Hospitales Públicos Tipo II de Ecuador*. Maestría en Auditoria de Tecnologías de la Información. [Universidad Espiritu Santo]. http://repositorio.uees.edu.ec/bitstream/123456789/3060/1/QUIMIZ%20MOREIRA%20MAURICIO.pdf

S**ánchez, L. E., Olmo, A. S., Álvarez, 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. https://doi.org/10.1109/TLA.2012.6222590

Segada de Araujo Luiz, Geraldo Silva Coelho Flavia Estelia & Bezerra Edson Kowask. (s. f.). *Gestión de la Seguridad de la Información*. REDCEDIA. https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf

Tigse Moposita Jorge Luis. (2020). *Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la Empresa Plasticaucho S.A. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera se*

Ingeniería en Sistemas Computacionales e Informáticos. [Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec/bitstream/123456789/30696/1/Tesis_t1663si.PDF

Uyaguari Guartatanga María Eliza, Avilés Armijos Jessica Maricela (2012). *Diseño de una Política de Seguridad para la Empresa de Telecomunicaciones Puntonet en la Ciudad de Cuenca, en base a las Normas de Seguridad ISO 27001 y 27011 como línea de base para las buenas prácticas de tratamiento y Seguridad de la Información*. Facultad de Ingeniería. Escuela de Ingeniería en Sistemas. [Universidad Politécnica Salesiana Sede Cuenca]. https://dspace.ups.edu.ec/bitstream/123456789/2158/14/UPS-CT002406.pdf

Villacis Espinosa Miguel Leopoldo. (2016). *Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) Basado en la Norma ISO 27001:2013 para la Red Corporativa de la Empresa Ecuatronix. Ingeniería Electrónica*. [Universidad Salesiana Sede Quito]. https://dspace.ups.edu.ec/bitstream/123456789/12406/1/UPS%20-%20ST002224.pdf

ANEXOS

ANEXO A: 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 u 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.

ANEXO B: MODELO DE LA ENCUESTA APLICADA

	Instituto Ecuatoriano de Seguro Social IESS		
	ENCUESTA		
El Centro de Salud está realizando una evaluación para saber los parámetros en la Seguridad de la Información que existe actualmente en la Institución. Para lo cual pedimos se conteste con toda sinceridad las siguientes preguntas.			
Preguntas		**SI**	**NO**

Existe compromiso de la dirección con la seguridad de la información		
Existe Controles o normas de seguridad de la información ya establecidas		
Se ha realizado Inventario de los Activos de la Información		
Se ha realizado Inventarios de los Activos de la Información		
Existe un sistema de autenticación de personas que accede a la información		
Se exige contraseñas de acceso a cada persona		
Existen límites en los intentos de accesos al sistema		
Existe normas, políticas, protocolos y guías para garantizar la confidencialidad, privacidad y seguridad de la información		
Cifrado de la Información antes de ser enviada		
Existen protocolos o estándares de red que garantice que los datos enviados sean los recibidos		
Se realiza evaluaciones periódicas basadas en la aplicación de normas y respuesta a cambios ambientales u operacionales que afecten la seguridad de la información.		
Se realiza copias de seguridad de la información y se guarda en sitios diferentes al sitio donde se encuentra los sistemas		
El recurso humano está capacitado para ofrecer sus servicios según el reglamento vigente		
Existen políticas y procedimientos que garantizan que quienes no tienen acceso, no pueden acceder a la información		

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE
UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *05 / 08 / 2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *Verónica Vanessa Bermeo Jiménez*
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magister en Seguridad Telemática*
f. Analista de Biblioteca responsable: *Lic. Luis Caminos Vargas Mgs.*

LUIS ALBERTO CAMINOS VARGAS

0047-DBRAI-UPT-IPEC-2021

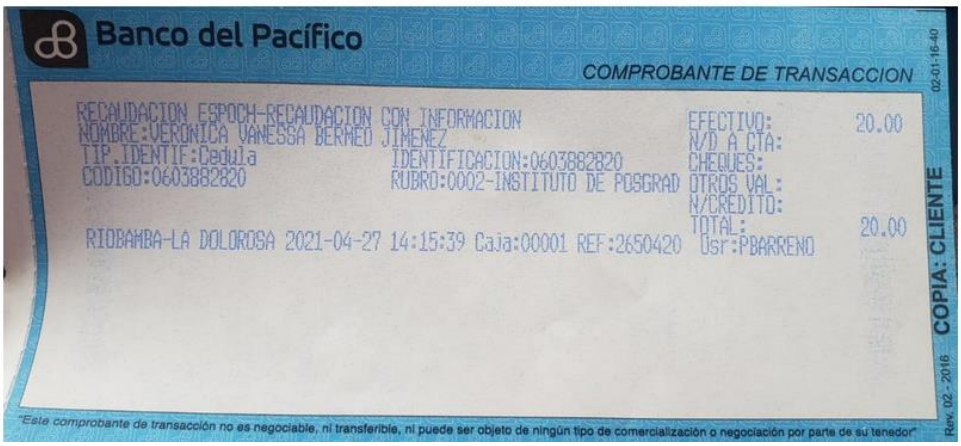
JOSE GABRIEL CARPIO SALAS <jgcarpio@espoch.edu.ec>
Para: Vanessa Bermeo

mar., 27 abr. a las 8:33 p. m.

BUENAS NOCHES NO ME HA ENVIADO EL RESUMEN

De: Vanessa Bermeo <vvanessabj@yahoo.es>
Enviado: martes, 27 de abril de 2021 15:04
Para: Washington Gustavo Mancero Orozco <washington.mancero@espoch.edu.ec>
Cc: JOSE GABRIEL CARPIO SALAS <jgcarpio@espoch.edu.ec>
Asunto: SOLICITUD DE TRADUCCION DE INGLES

Saludos cordiales por favor me podria ayuar con la traduccion
Nombres: Veronica Vanessa Bermeo Jimenez
Numero de Cedula:0603882820
programa de maestria: Maestria de Seguridad Telematica
Cohorte: 2
año: 2018


Banco del Pacífico

COMPROBANTE DE TRANSACCION

02-01-16-40

RECAUDACION ESPOCH-RECAUDACION CON INFORMACION
NOMBRE:VERONICA VANESSA BERMEO JIMENEZ
TIP.IDENTIF:Cedula IDENTIFICACION:0603882820
CODIGO:0603882820 RUBRO:0002-INSTITUTO DE POSGRAD

EFECTIVO: 20.00
N/D A CTA:
CHEQUES:
OTROS VAL:
N/CREDITO:
TOTAL: 20.00

RIOBAMBA-LA DOLOROSA 2021-04-27 14:15:39 Caja:00001 REF:2650420 Usr:PBARRENO

COPIA: CLIENTE

"Este comprobante de transacción no es negociable, ni transferible, ni puede ser objeto de ningún tipo de comercialización o negociación por parte de su tenedor"

Rev. 02 - 2016

ENVIO TRADUCCION

Yahoo/Buzón

JOSE GABRIEL CARPIO SALAS <jgcarpio@espoch.edu.ec>
Para: Centro de Idiomas, Washington Gustavo Mancero Orozco, Vanessa Bermeo

mié., 28 abr. a las 12:12 p. m.

ENVIO TRADUCCION

tra VANESS... .docx
16.7kB