DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN AJUSTADO A LAS NECESIDADES DE LA CORPORACIÓN MÉDICA CLÍNICA VIDA DE QUIBDÓ.

FERNEY GUARDIA PALACIOS

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN AJUSTADO A LAS NECESIDADES DE LA CORPORACIÓN MÉDICA CLÍNICA VIDA DE QUIBDÓ.

FERNEY GUARDIA PALACIOS

Trabajo de grado para optar al título de Magister

Asesor

JOAQUÍN YEPEZ MEJÍA

Ingeniero Electrónico

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2017

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) _____

Medellín mayo de 2017

AGRADECIMIENTOS

Principalmente a Dios por las bendiciones que me ha brindado, a mi madre Luz Enith Palacios Chaverra que me dio la vida y realizo muchos sacrificios para mi proceso de formación, a mi hija Enith Carolina Guardia Moreno quien es un motivo personal de esfuerzo y superación, a la Universidad Pontificia Bolivariana y a cada uno de sus docentes que aportaron para que este proceso de formación fuera posible, a mi director de Tesis Joaquín Yépez por su dedicación, compromiso y por poner a mi alcance sus conocimientos y experiencia, a mis compañeros durante cada uno de los módulos de la carrera.

CONTENIDO

TABLA DE TABLAS

TABLA DE ILUSTRACIONES

Glosario

Activo de Información: Un activo de la información es cualquier sitio o conjunto de información, almacenada dentro de algún lugar de la organización, definido y dirigido como una unidad sola de modo que nosotros podamos entenderlo, compartir y protegerlo con eficacia y sacar el máximo partido el valor de ello. Es algo que no podemos sustituir gratis, el tiempo, la habilidad y recursos.

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

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

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

Política de Seguridad: Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Riesgo: Es la combinación de la probabilidad de un evento y su ocurrencia.

RESUMEN

Este proyecto tiene como fin determinar el estado actual de seguridad de la información en la corporación médica Clínica Vida de la ciudad de Quibdó, detectar posibles debilidades y vulnerabilidades relacionadas con la seguridad de la información. Luego de tener un análisis detallado del estado de dicha corporación, diseñar un Sistema de seguridad de la información que se ajuste a las necesidades específicas de la clínica, el cual será revisado por un experto. El proyecto será presentado a la junta directiva de la Corporación Médica, quien analizará su posibilidad de implementación en un futuro.

PALABRAS CLAVE: Sistema de gestión de la seguridad de la información, Activos de Información, Riesgo, Integridad, autenticidad, confidencialidad y disponibilidad de la información, Políticas de seguridad.

ABSTRACT

This project aims to determine the current state of information security in medical corporation Clinic Vida of the city of Quibdó, detect potential weaknesses and / or related to information security vulnerabilities. After having a detailed status of such corporation analysis, design a Management System information security that meets the specific needs of the clinic, which will be reviewed by an expert. The project will be presented to the board of the medical corporation, who will discuss the possibility of implementation in the future.

KEY WORDS: Information, Management, Technology, Security.

1. INTRODUCCIÓN

En el presente trabajo, se analiza el estado actual en materia de seguridad de la información para una Corporación Médica en la ciudad de Quibdó, para mejorar la forma como esta gestiona sus activos de información, buscando un avance representativo en la confianza de sus clientes para con ellos, sabiendo que cuando una empresa obtiene una certificación o la ejecución de la misma, crea una imagen de prestigio entre las demás.

Se decidió la aplicación de la Gestión de Seguridad de Información en la Corporación medica Clínica Vida debido a la importancia que representa, teniendo en cuenta las falencias que tiene la ciudad en el sector salud y que esta corporación recibe pacientes de todo el departamento del Chocó, brindando servicios como urgencias, maternidad, pediatría, cuidados intensivos, entre otros mejorando la calidad de vida de sus habitantes y prolongando sus expectativas de vida.

Dicha corporación fundada en 1994 producto del desempeño de un grupo de profesionales de la salud Chocoanos por ayudar a mejorar la situación de la salud en el departamento, con acciones del sector privado.

Al inicio de este proyecto, la Corporación Medica Clínica vida carecía de una metodología o modelo para avalar la seguridad e integridad de sus activos físicos y lógicos ajustada a los procesos en sus distintas dependencias, exponiéndola a riesgos como perdida de información crítica e incumplimiento de aspectos legales. Por esta razón se trazó como objetivo diseñar un Sistema de Gestión de Seguridad de la Información ajustado a las necesidades de la Corporación que permitiera tener un mejor control del riesgo de afectación de su información en términos de la disponibilidad, integridad y autenticidad de su información.

Para lograr el objetivo antes mencionado, se Identificó el estado actual de la Corporación Médica en materia de Gestión de Seguridad de la Información, permitiendo tener un inventario actualizado de sus activos y los riesgos a los cuales estaban expuestos. Posteriormente se diseñó un modelo del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ajustado al estado actual de la Corporación, los controles, procesos y políticas de seguridad basados en las debilidades y amenazas detectadas en al análisis inicial y en las recomendaciones que hace la norma ISO 27001:2013 y sus anexos.

Además, se establecen las responsabilidades y compromisos en materia de seguridad de la información, tanto de la alta Gerencia, como también de los funcionarios directos e indirectos y proveedores de la corporación, Posteriormente se realiza una serie de recomendaciones y se presenta finalmente a la dirección de la clínica, el diseño del modelo de Gestión de Seguridad para su revisión y posible futura implementación.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 Problema

Actualmente, el surgimiento de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a su vez han aumentado los riesgos para las empresas que se exponen a nuevas amenazas. Desafortunadamente, es relativamente fácil tener acceso a muchas herramientas que permiten a personas no autorizadas llegar hasta la información protegida, sin necesidad de esforzarse mucho y con pocos conocimientos, causando graves perjuicios para la empresa. la mayor parte de la información reside en equipos computadores, soportes de almacenamiento y redes de datos, englobados dentro de lo que se conoce como Sistemas de Información. Estos Sistemas de Información están sujetos a riesgos y amenazas que pueden generarse desde el interior de la propia organización o desde afuera.

La información es un activo muy valioso para las organizaciones, ya que de ella depende el buen funcionamiento de la misma. Conservar su integridad, confidencialidad y disponibilidad es indispensable para lograr los objetivos de negocio, razón por la cual, algunas organizaciones han puesto medios para evitar el robo y manipulación de sus datos confidenciales, en algunos casos no han sido suficiente o idóneas para tal fin, pues han sido víctima de personas mal intencionadas. (SILVA, 2015)

Los activos de una organización, requieren junto a sus procesos y sistemas que la manejan, ser protegidos convenientemente a partir de un análisis de riesgos, frente a amenazas que puedan poner en peligro su integridad para alcanzar los objetivos. la seguridad de la Información no es un problema sólo de las grandes empresas sino de todo el mundo.

Los ataques informáticos se han convertido en una industria global que ha afectado muchos países. Los delitos informáticos influyen en la información personal e institucional, las personas que realizan este tipo de ataques están preparados para detectar vulnerabilidades en los sistemas de información, en los procesos y en las personas. Los ataques se van complejizando cada vez más, proteger toda la información de una empresa parece ser una tarea ardua y compleja, encontrar personal capacitado y dispuesto a combatir los ataques es cada vez más difícil de hallar, proteger a los usuarios y a las empresas, requiere la combinación de la tecnología, la gestión y la educación para estar protegidos. (ESET, 2016)

En la actualidad los ataques a los que son victima las organizaciones con mayor frecuencia son: Ingeniería social, Infección de Malware, Phishing, Fraude interno o externo, Explotación de vulnerabilidades, DDOS, suplantación de identidad, Fuga de información, Obtención de contraseñas o credenciales, SPAM, ataques a dispositivos móviles, fraudes, secuestro de información, ingeniería social entre otras. (ESET, 2016)

Existen riesgos físicos como inundaciones, incendios o terremotos que pueden afectar la disponibilidad de nuestra información y recursos, haciendo poco probable la continuidad de nuestro negocio si no estamos preparados para afrontarlos, también se encuentran los riesgos lógicos asociados con la propia tecnología. Estos riesgos pueden acabar con la confianza de los clientes y la imagen de una empresa en el mercado. la Corporación Médica Clínica Vida de la ciudad de Quibdó no está exenta de dichos riesgos, por tal razón es importante tomar medidas o políticas que apunten a la preservación integral de la información que se maneja en las distintas dependencias tanto de usuarios internos como externos puesto que es delicada y relevante, ya que en cierta medida la vida e intimidad de algunos usuarios depende de ella. Además, no cuenta con un Sistema de Gestión de Seguridad de la Información proporcional a sus necesidades.

Hasta el momento, la clínica vida no cuenta con ninguna certificación en materia de sistema de gestión de la seguridad de la información, por otra parte, carece de una metodología o modelo para garantizar la seguridad e integridad de sus activos físicos y lógicos ajustada a los procesos de la corporación en sus distintas dependencias o departamentos. Además, la gran mayoría de los funcionarios no tienen conciencia de la importancia de garantizar la seguridad de la información al interior de la organización, lo cual los expone aún más a amenazas como ingeniería social, suplantación, fraudes, ataques informáticos entre otros, y a la toma inadecuada de decisiones en situaciones como incendios, inundaciones, terremotos o ante la ausencia del encargado de un proceso.

2.2 Justificación

Para proteger a nuestras organizaciones de las amenazas a las que están expuestas en materia de seguridad de la información, es necesario definir procedimientos adecuados e implementar controles de seguridad basados en la evaluación de riesgos y una medición de la eficacia de los controles

actuales.

Desde su fundación, la corporación medica Clínica Vida se ha esforzado por el fortalecimiento del sistema de información mediante la implementación de aplicativos que funcionan de manera integral permitiendo la disminución de los tiempos de procesamiento, mejorar el control y flujo de la información y por consiguiente aumentar el porcentaje de satisfacción de los usuarios internos y externos. Unido a esto, se ha trabajado en el robustecimiento de la plataforma tecnológica mediante la adquisición gradual de servidores de red, equipos de cómputo, equipos activos y de soporte eléctrico.

La información que se maneja en las distintas dependencias de la Corporación Médica es crítica, y está expuesta a amenazas tanto internas como externas que pueden ser Naturales como incendios, inundaciones, terremotos; Intencionales como fraudes, vandalismos, sabotaje, espionaje, invasiones, robo de información, suplantación, entre otras; pero también pueden ser involuntarias causadas por las acciones de los usuarios como virus, revelación de contraseñas, ingeniería social entre otras muchas veces generadas por la falta de conocimientos. Estas distintas amenazas originan en la Clínica Vida la necesitad de pensar en alternativas de mitigación, por tal razón la alta gerencia está dispuesta y comprometida con el establecimiento de un Sistema de Gestión de Seguridad de la Información que evolucione.

Un Sistema de Gestión de Seguridad de la Información, permite establecer políticas, procedimientos y controles con el objeto de disminuir los riesgos de la organización. Además, genera grandes ventajas para la organización ya que reduce los riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello se logra reducir las amenazas hasta alcanzar un nivel asumible por la organización. de este modo, si se produce una incidencia, los daños se minimizan y se respalda la continuidad del negocio.

De nuevo, la seguridad se convierte en una actividad de gestión, deja de ser un conjunto de actividades y se transforma en un ciclo, en el que participa toda la organización, avalando el cumplimiento de la legislación vigente como la Ley 18331 de protección de datos personales y acción de habeas data, el Decreto 452/009 de protección de historias clínicas, la Ley 1581 de 2012 cuyo objeto es desarrollar el derecho constitucional de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas entre otras, evitando riesgos y costos innecesarios como demandas por perdida o mal uso de la información de los pacientes o sus

historias clínicas, aplicación de medicamentos o procedimientos médicos a pacientes de que no corresponden, permitiendo racionalizar recursos, la organización se asegura de cumplir con el marco legal que protege a la empresa de aspectos que posiblemente no se habían tenido en cuenta anteriormente, generando a su vez un mejor posicionamiento en la región y el buen nombre de la Corporación Médica.

Para el caso específico de la Corporación médica Clínica Vida, se plantea el diseño de un Sistema de Gestión de Seguridad de la Información considerando el conjunto de sus bienes a partir de su importancia y el papel que representa para el cumplimiento de sus actividades, haciendo mayor énfasis en aquellos que son críticos en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo al cual están expuestos. la seguridad de la información se convierte en algo fundamental para la corporación médica, ya que la afectación de información como historias clínicas, información financiera, la suplantación de pacientes, la alteración de tratamientos, alteración de inventarios o alteración de nóminas, podrían afectar de manera directa no solo la continuidad del negocio y el buen nombre de la clínica sino que además pondría en peligro la vida de los usuarios e incluso violaciones normativas como la Resolución 1995 de 1999 del Ministerio de Salud que reglamenta lo relacionado con las historias clínicas. (SALUD, 1999).

Se proyecta la planificación de un sistema de gestión de la información que oriente a la corporación médica Clínica Vida sobre cómo tratar los aspectos de seguridad y los controles necesarios para resguardar la disponibilidad, integridad y confidencialidad de su información tanto física como lógica, a partir de un análisis de riesgos, diseño de políticas de aceptación o mitigación de los mismos, el establecimiento de las políticas aceptación o mitigación, objetivos, procesos y procedimientos del Sistema de Gestión de Seguridad de la Información pertinentes a la gestión de riesgos y mejora de la seguridad de la información, basado en los objetivos de la Corporación Clínica Vida, que consienta aceptarlos, mitigarlos o transferirlos.

3. OBJETIVOS

3.1. Objetivo General.

Diseñar un Sistema de Gestión de Seguridad de la Información ajustado a las necesidades de la Corporación médica Clínica Vida de Quibdó para tener un mejor control del riesgo de afectación de la información en términos de la disponibilidad, integridad y autenticidad de su información.

3.2. Objetivos Específicos

- Identificar el estado actual de la Corporación Médica clínica Vida en materia de Gestión de Seguridad de la Información.
- Diseñar una propuesta de implementación del Sistema de Gestión de Seguridad de la Información ajustada a las vulnerabilidades detectadas en el diagnóstico previamente realizado.
- Presentar y validar la propuesta del sistema de gestión de seguridad de la información.

4. MARCO REFERENCIAL

4.1. Marco Contextual

El departamento del Chocó es uno de los treinta y dos departamentos de Colombia, localizado en el noroeste de Colombia, en la región del Pacífico Colombiano, comprende las selvas del Darién y las cuencas de los ríos Atrato y San Juan. Su capital es la ciudad de Quibdó. Este de departamento limita por el Norte con la República de Panamá y el mar Caribe, por el Este con los departamentos de Antioquia, Risaralda y Valle del Cauca, por el Sur con el departamento del Valle de Cauca, y por el Oeste con el océano Pacífico y tiene una extensión total de 46.530 km2, sus principales actividades económicas son la agricultura y la explotación minera, la explotación forestal, agricultura y ganadería, además ofrece innumerables atractivos turísticos desde el punto de vista natural, cultural y científico. Entre los principales lugares de interés turístico sobresalen los parques nacionales naturales Los Katíos, Utría y Tatamá. Selvas y playas vírgenes ofrecen a sus

visitantes la flora y la fauna más exóticas del trópico. (Gobernacon del Chocó, 2012)

la Clínica Vida es un proyecto de la Sociedad Médica Vida SOMEVI S.A., empresa fundada en 1994 producto del desempeño de un grupo de profesionales de la salud Chocoanos por ayudar a mejorar la situación de la salud en el departamento, con acciones del sector privado, utilizando las herramientas de la seguridad y compromiso que ejemplifican las sociedades anónimas. Está ubicada en el departamento del Chocó, en la ciudad de Quibdó, en la Carrera 4 A # 29-64 en un edificio de cuatro pisos. Tiene como misión ofrecer los servicios de salud con calidad, humildad y actualidad, mediante una permanente evaluación del desempeño en las atenciones realizadas, para retroalimentar y renovar los procesos programáticos con educación continua, inyección de tecnología y administración líder. (Vida, 2011)

de igual manera, la Corporación Médica Vida presta los servicios de consulta médica general, consulta y cirugía de medicina especializada, servicio de apoyo clínico, urgencias, cuidados intensivos, entre otros a diferentes IPS, EPS y de forma particular atendiendo usuarios de la ciudad de Quibdó y municipios cercanos.

Contar con un Sistema de Gestión de Seguridad de la Información en la Corporación es significativo para una evaluación constante del desempeño de las atenciones realizadas, permitiendo ser consecuente con la visión de ofrecer servicios de salud con calidad, humildad y actualidad además de la renovación de los procesos con educación continua.

4.2. Marco Conceptual

Se presentan algunas definiciones importantes relacionadas al diseño de Sistema de Gestión de la Seguridad de la Información que se busca realizar en la Corporación Médica Clínica Vida de Quibdó.

Sistema de Gestión de Seguridad de la Información: 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. Puede ayudar a las pequeñas, medianas y grandes empresas en cualquier sector mantener los activos de información segura (ISO / IEC 27001, 2013), un Sistema de Gestión de Seguridad de la Información en general, abarca una estructura,

unos recursos, unos procesos y unos procedimientos que tienden a poner en práctica los objetivos y políticas de una organización (Bartolin, 2008).

Según (Álvarez, 2012) el Sistema de Gestión de Seguridad de la Información es una 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. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore.

Por otra parte, al establecer un Sistema de Gestión de Seguridad de la Información en una compañía es de gran utilidad al proporcionar una metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de su negocio que tengan que ver con la información, el Sistema de Gestión de Seguridad de la Información diseñado ha de ser dinámico y fácilmente adaptable a los cambios y las mejoras a introducir en la compañía, la aplicación del modelo P.H.V.A. es fundamental, basado en el concepto de mejora continua, si se decide obtener la certificación ISO/IEC 27001 del sistema, mejora la imagen del organismo y se contribuye a generar confianza entre los usuarios y la empresa.

Finalmente argumentan que es fundamental la concreción de los controles de seguridad para supervisar el seguimiento de los planes de acción, los controles incluidos, concretos y medibles en el tiempo permiten evaluar la efectividad de los planes de acción. (OHANNA CAROLINA BUITRAGO, 2012)

Activo de Información: Un activo de la información es cualquier sitio o conjunto de información, almacenada dentro de algún lugar de la organización, definido y dirigido como una unidad sola de modo que nosotros podamos entenderlo, compartir y protegerlo con eficacia y sacar el máximo partido el valor de ello. Es algo que no podemos sustituir gratis, el tiempo, la habilidad y recursos. (know, 2010)

Se entiende por cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. Otra buena definición de Activo es todo aquello que tiene valor para su empresa. la ISO 27001:2013 pide que todos los activos relevantes sean identificados e inventariados. Existe un poco de confusión porque se acostumbra a asociar la expresión “inventario de activos” al usual inventario de hardware y software.

Seguridad de la Información: Según la norma ISO 27001:2013, la seguridad de la información es la preservación de la confidencialidad, integridad y

disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas. la gestión de la seguridad de la información engloba todas las actividades relacionadas con la dirección y control de la seguridad de activos de información de una organización. Estas actividades consisten en la valoración de las amenazas y del astado actual en que se encuentra la seguridad de la información en esta organización. (Bartolin, 2008)

Confidencialidad Integridad y Disponibilidad: la información no se pone a disposición ni se revela a individuos o entidades no autorizados, con el objetivo de mantener la exactitud, completitud y métodos de proceso de la misma, garantizando el acceso y utilización de la información y los sistemas de tratamiento cuando lo requieran. (ISO 27001)

Glosario

Políticas de Seguridad: Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del Sistema de Gestión de Seguridad de la Información.

Organización de la Seguridad de la Información: Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

Gestión de Activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.

Activo de Información: Un activo de la información es cualquier sitio o conjunto de información, almacenada dentro de algún lugar de la organización, definido y dirigido como una unidad sola de modo que nosotros podamos entenderlo, compartir y protegerlo con eficacia y sacar el máximo partido el valor de ello. Es algo que no podemos sustituir gratis, el tiempo, la habilidad y recursos. (know, 2010)

Se entiende por cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. Otra buena definición de Activo es todo aquello que tiene valor para su empresa. la ISO 27001:2013 pide que todos los activos relevantes sean identificados e inventariados. Existe un poco de confusión porque se acostumbra a asociar la expresión “inventario de activos” al usual inventario de hardware y software.

Seguridad de Los Recursos Humanos: Orientado a reducir el error humano, ya que, en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información. Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

Control de Accesos: El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. de igual forma, detecta actividades no autorizadas.

Sistemas de Información, Adquisición, Desarrollo y Mantenimiento: Busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

Gestión de Incidentes de Seguridad de la Información: Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de administración de incidentes, que es básicamente definir de forma clara pasos, acciones, responsabilidades,

Gestión de Continuidad del Negocio: Lo que considera este control es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

Administración de Riesgos: Se llama así al proceso de identificación, análisis y evaluación de riesgos. (ISO 27001)

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Control: El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los ajustes o correcciones necesarias en caso se detecten eventos que escapan a la naturaleza del proceso. Es una etapa primordial en la administración, pues, por más que una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, no se podrá verificar la situación real de la organización si no existe un mecanismo que verifique e informe si los hechos van de acuerdo con los objetivos.

Declaración de Aplicabilidad: la declaración de aplicabilidad o SOA, del inglés Statement of Applicability, Es un documento que se referencia en la

cláusula 4.2.1 del estándar ISO/IEC 27001 y describe los objetivos de control y controles relevantes y aplicables al alcance del Sistema de Gestión de Seguridad de la Información de la empresa, en función de la política y conclusiones del proceso de evaluación y tratamiento del riesgo. En el documento básicamente van 2 campos: uno donde va el control específico y una columna donde va la aplicabilidad, donde se justifica la decisión tomada sobre si el control es aplicable o no.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

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

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

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

4.3. Marco Legal

Ley 1266 DE 2008: la presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y los demás derechos libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Políticas así como el derecho a la información establecido en el artículo 20 de la Constitución Política¡ particularmente en relación con la información financiera y crediticia, comercial¡ de servicios y la proveniente de terceros países.

Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa. (Super Intendencia de Industria y Comercio, 2008)

Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. (Senado Republica de Colombia, 1999)

Articulo 1o. Ámbito de Aplicación. la presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Articulo 2o. Definiciones**.** Para los efectos de la presente ley se entenderá por:

a) Mensaje de datos. la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y

estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

e) Intercambio Electrónico de Datos (EDI). la transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

f) Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. (Senado Republica de Colombia, 1999)

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Mintic, 2015)

Ley 1341 de 2009: Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Artículos 12 y 68 reglamentados por el Decreto 2044 del 19 de septiembre de 2013. Ley reglamentada por el Decreto 2693 del 21 de diciembre de 2012. Parágrafo 2° del artículo 57 modificado por el artículo 59 de la Ley 1450 de 2011, Inciso 1°y 3° y el parágrafo 1°y 2° del artículo 69 derogado por el artículo 276 de la Ley 1450 de 2011.numerales 6 y 7 del artículo 18, el numeral 11, del artículo 28 y el artículo 29 de la Ley 1341 de 2009 derogados por el Decreto 4169 del 2011. (Alcaldia Bogotá, 2009)

Ley 18331: Protección de datos personales y acción de habeas data Esta ley establece que se deberán registrar todas las bases de datos que contenga información de personas físicas y jurídicas. Según cita la ley: “Artículo 2º. Ámbito subjetivo. - El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda. Artículo 3º. Ámbito objetivo. El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado. (Datos L. q., 2013)

No será de aplicación a las siguientes bases de datos:

a. A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b. Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

c. A las bases de datos creadas y reguladas por leyes especiales.

Ley 18381:

Acceso a la información pública: Esta ley establece que toda información producida por el organismo deberá ser pública, salvo que entre en las categorías de confidencia, reservada o secreta. Según cita la ley:

Artículo 1º. (Objeto de la ley). - la presente ley tiene por objeto promover la transparencia de la función administrativa de todo organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública.

Artículo 2º. (Alcance). - Se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales.

Artículo 3º. (Derecho de acceso a la información pública). - El acceso a la información pública es un derecho de todas las personas, sin discriminación por razón de nacionalidad o carácter del solicitante, y que se ejerce sin necesidad de justificar las razones por las que se solicita la información. (Datos L. d., 2013)

Ley 1581 de 2012: Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Los principios y disposiciones contenidas en esta ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. Además, aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en

virtud de normas y tratados internacionales. (Colombia, Senado Republica de, 2012)

Decreto 452/009

Este decreto establece que todas las unidades ejecutoras deben adoptar una política de seguridad de la información, tomando como base la propuesta en dicho decreto. Además, exhorta a los gobiernos departamentales, entes autónomos, servicios descentralizados y demás órganos del estado a adoptar las disposiciones establecidas por el decreto. Que se debe disponer medidas para garantizar la confianza y seguridad de los sistemas y de la información en poder de los organismos públicos con el fin de proteger los activos de información y minimizar el impacto en los servicios causados por vulnerabilidades o incidentes de seguridad se debe proveer una efectiva gestión de la seguridad. (AGESIC, 2009)

Resolución Numero 1995 DE 1999: la Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

Artículo 12.- Obligatoriedad del Archivo. Todos los prestadores de servicios de salud, deben tener un archivo único de historias clínicas en las etapas de archivo de gestión, central e histórico, el cual será organizado y prestará los servicios pertinentes guardando los principios generales establecidos en el Acuerdo 07 de 1994, referente al Reglamento General de Archivos, expedido por el Archivo General de la Nación y demás normas que lo modifiquen o adicionen.

Artículo 13 Custodia de la Historia Clínica. la custodia de la historia clínica estará a cargo del prestador de servicios de salud que la generó en el curso de la atención, cumpliendo los procedimientos de archivo señalados en la presente resolución, sin perjuicio de los señalados en otras normas legales vigentes. El prestador podrá entregar copia de la historia clínica al usuario o a su representante legal cuando este lo solicite, para los efectos previstos en las disposiciones legales vigentes. (SALUD, 1999)

4.4. Estado del Arte

En el estado del arte presentado en este trabajo se resalta la postura a nivel normativo en Colombia en cuanto a la seguridad de la información, diferentes enfoques de algunos investigadores para abordar el diseño, implementación de un Sistema de Gestión de Seguridad de la Información, algunas experiencias documentadas sobre la implementación de un sistema de Gestión de Seguridad de Información para el sector salud en los últimos 10 años a nivel nacional e internacional.

A nivel nacional mediante el documento COMPES 3854 del Consejo Nacional de Política Económica y Social de la República de Colombia, en su Departamento Nacional de Planeación plantea la política nacional de seguridad digital, ha cambiado el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital, cuyo objetivo principal es fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Además, en esta política se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación. Para lograrlo, se implementarán acciones en torno a cinco ejes de trabajo.

1. Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
4. Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
5. Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional

Para poner en marcha esta política, se ha construido un plan de acción que se ejecutará durante los años 2016 a 2019 con una inversión total de 85.070

millones de pesos. Las principales entidades ejecutoras de esta política son el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. (Consejo Nacional de Política Económica y Social, 2016)

En Colombia, JOHANNA CAROLINA BUITRAGO, DIEGO HERNANDO BONILLA, CAROL ESTEFANIE MURILLO (Colombia 2012) en su trabajo de tesis Diseño de Una Metodología Para la Implementación del Sistema de Gestión de Seguridad de la Información- Sistema de Gestión de Seguridad de la Información, En El Sector de Laboratorios de Análisis Microbiológicos, Basado En ISO 27001:2013. Abordan las amenazas que constituyen un riesgo sobre uno de los activos más críticos y vulnerables de las organizaciones como la información, asegurar la disponibilidad, la confidencialidad y la conservación de los datos y garantizar el nivel de seguridad en el sector de laboratorios de análisis microbiológicos

En la tesis se utilizó una metodología que consiste en reunir un grupo interdisciplinar que esté involucrado en el proceso, evaluar cada una de las variables que pueden llegar a afectar el resultado de la operación en que se detectó el problema. Propone implementar herramientas como cartas de control, planes de verificación del Sistema de Gestión de Seguridad de la Información, balanced scorecard o cuadro de mando integral y el programa de auditorías internas.

Los autores concluyeron que para garantizar la seguridad de los activos de la información se debe desarrollar una gestión orientada a mitigar el impacto de los riesgos para lo cual se ha de diseñar un método de evaluación de riesgos completo que ha de permitir conocerlos y afrontarlos de forma coordinada, como lo hace el método de evaluación incluido en el trabajo. Y, seguidamente, definir unos planes bien de acción o bien de seguimiento con unos controles de seguridad que permitan verificar el rendimiento de cada plan.

Por otra parte (AURA LUCIA CASADIEGOS, 2014) desarrollo en el departamento del Cesar, más exactamente en el Municipio de Rio de Oro un proyecto llamado Sistema de Gestión de Seguridad de la Información para el área de contabilidad de la E.S.E. hospital local de Rio de Oro Cesar, el cual tiene como objetivo realizar un diagnóstico del área de contabilidad de la E.S.E. Hospital Local identificando los elementos que conforman Sistema de Gestión de Seguridad de la Información para el Área de Contabilidad de la

E.S.E. para Elaborar un documento formal para la gestión de la seguridad de la información del Área de contabilidad que incorpore la política de la seguridad de la información.

En el marco académico de América Latina, un artículo llamado Seguridad de la Información, clave en la protección de datos sanitarios, realizado por Karina Ingrid Medinaceli Díaz y Eugenio Gil en la Paz Bolivia en el mes de junio de 2015, exponen la importancia de implementar medidas de seguridad para el control de accesos y del uso de la información que se encuentra en los ordenadores, tratando de preservar así la intimidad de los pacientes. Plantean algunas medidas y procedimientos para mejorar la seguridad en el acceso a las historias clínicas de los pacientes entre los que están la implementación de firmas electrónicas, auditorias informáticas y la implementación de Sistemas de Gestión de Seguridad de la Información.

En este artículo, los autores concluyeron que para garantizar la seguridad y confidencialidad de la información clínica se debe resolver la visibilidad de la historia clínica electrónica, para lo cual se establecerán protocolos y guías de actuación, además un sistema de gestión de la información permitirá que los accesos a las historias clínicas queden registrados en los logs y mediante firmas digitales establecer quien lo hizo. También consideran la historia clínica electrónica más segura y confidencial que la historia clínica en papel. (Gil, 2015)

El objetivo principal de este estudio es la construcción de un mecanismo para la gestión de la información en materia de seguridad que se aplica a las organizaciones médicas. Este mecanismo se basa en los once elementos de control y ciento treinta y tres objetivos de control de la norma ISO 27001:2013 de Gestión de Seguridad de la Información. Este estudio analiza e identifica los eventos más comunes relacionados con la seguridad de la información en las organizaciones médicas y clasifica estos eventos como de alto riesgo, de riesgo transferibles, y el riesgo controlado para facilitar la gestión de dicho riesgo.

También (Vasco, 2015) en su tesis de grado en la ciudad de lima Perú diseñó un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013 el cual tiene por propósito generar una solución específica para una organización del sector público y específicamente del rubro salud, debido a que se tomarán los procesos institucionales de una empresa de este tipo como campo de

estudio para aplicar las metodologías y herramientas anteriormente mencionadas. El proyecto se centra en los procesos institucionales referentes al área de admisión de pacientes, limitando el alcance que se utilice para la creación de la documentación a dos de estos procesos críticos para la operación del área indicada.

Al final el autor concluye que existe una brecha importante en cuanto a seguridad de la información en la institución sobre la que se ha realizado el presente proyecto, se debe involucrar a la dirección en las acciones del plan que se debe definir con motivo de la implementación del Sistema de Gestión de Seguridad de la Información institucional, el cual debería ser gestionado como un proyecto institucional, de manera que se cuente con el apoyo de las distintas direcciones y áreas del INMP. También es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del Sistema de Gestión de Seguridad de la Información y que deberá contar con el apoyo de la Dirección General de modo que se facilite el acceso a la información de todas las áreas pertinentes.

5. METODOLOGÍA

Para el desarrollo del proyecto diseño de un Sistema de Gestión de Seguridad de la Información ajustado a las necesidades de la corporación médica clínica vida de Quibdó, se tomó como base los requisitos que establece la norma NTC-ISO/IEC 27001:2013, para el establecimiento de un Sistema de Gestión de Seguridad, los cuales se describen a continuación y son desarrollados en el capítulo 6:

a) Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.

b) Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología.

c) Definir el enfoque organizacional para la valoración del riesgo.

d) Identificar los riesgos.

e) Analizar y evaluar los riesgos.

f) Identificar y evaluar las opciones para el tratamiento de los riesgos.

g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

h) Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.

i) Obtener autorización de la dirección para implementar y operar el SGSI.

j) Elaborar una declaración de aplicabilidad.

La metodología de este proyecto fue desarrollada tomando como referencia el marco de Cyber Seguridad de la NIST que propone 5 funciones relacionadas con la gestión de riesgos de seguridad de la información que son de uso muy válido a nivel mundial. Además, se plantea una metodología híbrida entre cualitativa y cuantitativa, en las que se realizó algunas entrevistas y observaciones para el levantamiento de información y obtención de evidencias y se desarrolló algunas etapas del modelo P.H.V.A. En la figura 1, se presentan las 4 fases sugeridas para este proyecto:

Figura 1. Metodología del Sistema de Gestión de Seguridad de la Información.

5.1 Diagnostico del Estado Actual: En esta primera fase del proyecto, se realizará un diagnóstico del estado actual de la corporación médica Clínica Vida en materia de Sistema de Gestión de Seguridad de la Información y se empleará la metodología de entrevistas, revisión de documentación y visita en sitio.

Diagnóstico de la situación de seguridad de la información de la Corporación Médica Clínica Vida de la ciudad de Quibdó, haciendo énfasis en identificar adecuadamente los activos de información vinculados a los procesos financiero, asignación de citas médicas, historia clínica y/o urgencias así como las posibles vulnerabilidades y los riesgos asociados a dichos activos.

5.1.2 Inventario de Activos de Información: Identificación de los activos de información del de la corporación médica Clínica Vida, enfatizando primeramente los procesos fundamentales de negocio, los activos de información específicos que involucra, y sus diversos tipos y formatos. Se realizará entrevista al administrador de sistemas y al encargado de almacén.

5.1.3 Análisis de Riesgos: Identificación los activos de información, se identificará los riesgos y amenazas a los que están expuestos dichos activos,

cuantificando el nivel de severidad de riesgo y el tratamiento sugerido. Dichos riesgos serán listados y caracterizados.

5.2. Diseño de la Situación Deseada: Para la segunda etapa del proyecto, se diseñará una propuesta de Sistema de Gestión de Seguridad de la Información. En esta fase se tomará como base la norma ISO 27001:2013 e ISO 27002 y se diseñaran los controles, políticas y procesos de seguridad de la información que plantea la norma, el anexo A y el anexo SL.

Creación del Plan de Seguridad de la Información: Una vez realizada la fase de Diagnóstico y habiendo obtenido el inventario de activos con su correspondiente análisis de riesgo, se propondrán los productos y controles necesarios para mitigar los riesgos potenciales.

5.3 Planificación de la Transición

Metodología. Establecer un plan de trabajo de alto nivel con un cronograma de actividades, en el que se establezcan las actividades con sus responsables y los tiempos de ejecución, para el cierre de las brechas de acuerdo con las capacidades y recursos de la clínica.

En esta etapa, se trazará una ruta que organice el trabajo, que incluya elementos de planificación de tareas y funciones y se establecerá un Plan de Seguridad de la Información, en el cual se tendrán en cuenta los siguientes elementos:

- Política de seguridad de la información.
- Objetivos estratégicos para la seguridad de la información.
- Resultado de la fase de Diagnóstico: análisis de riesgos.

5.4 Presentación y Socialización de Recomendaciones. Se presentará y socializará el diseño del Sistema de Gestión de Seguridad de la Informaciónpara la Corporación Médica Clínica Vida de la ciudad de Quibdó, se establecerán posibles recomendaciones de mejora, Se comunicara a la Junta Directiva de dicha Corporacion la propuesta final del Sistema de Gestión de Seguridad de la Informacion para su análisis y posble implementacion.

6. ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se desarrollan los elementos requeridos por la norma NTC-ISO/IEC 27001:2013 para el establecimiento del Sistema de Gestión de Seguridad de la Información de la Clínica vida de la ciudad de Quibdó.

6.1 Definición del alcance y límites del Sistema de Gestión de Seguridad de la Información.

Este proyecto, cubre los elementos de la gestión de riesgos de Seguridad de la Información para en el uso de las plataformas tecnológicas de la clínica Vida. El limite se circunscribe a la información que se gestiona en las plataformas tecnológicas de la clínica, en esta primera etapa se quiere controlar la información que está en las plataformas de TI de la clínica, pero queda a discreción de la gerencia la ampliación de este proyecto, a las áreas en las que determinen su aplicación.

6.2 Definición de política del Sistema de Gestión de Seguridad de la Información.

En este ítem se instaló la creación del comité de seguridad de la información, el comité de gestión de incidentes y se establecieron los parámetros para la declaración y notificación e incidentes. Además, se presenta un resumen de la política del Sistema de Gestión de Seguridad para la clínica Vida, en el ANEXO 15 Gobierno del Sistema de Gestión, Se describe en detalle como está conformado el gobierno de gestión de seguridad, con sus respectivas funciones.

6.2.1 Comité de Seguridad de la Información.

Se estableció el comité de Seguridad de la Información para la Corporación Médica Clínica Vida de la ciudad de Quibdó, el cual tiene como objetivo asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en la

Corporación, así como de la formulación y mantenimiento de una política y controles de seguridad de la información a través de todo el organismo.

El Comité de Seguridad de la Información está conformado de la siguiente manera:

- Oficial de Seguridad de la información
- Director General Administrativo
- Responsable de Talento Humano
- Responsable del Área de infraestructura
- Responsable de Auditoria Interna
- Responsable de Jurídico
- Responsable de Seguridad

6.2.2 Comité de Gestión de Incidentes.

Se creó el comité de gestión de incidentes, el cual está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la Clínica. En el ANEXO 15 Gobierno del Sistema de Gestión, se especifican las funciones y responsabilidades de este comité.

6.2.3 Declaración y notificación e incidentes.

Se edificaron los parámetros para la declaración y notificación e incidentes con el fin de responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información, la interrupción de los servicios, el proceso de tratamiento de incidentes y manejar correctamente los aspectos legales que pudieran surgir durante este proceso. Los detalles de estas directrices, donde se estipula que hacer durante y después de un incidente de seguridad, se encuentran en el ANEXO 15. Gobierno del Sistema de Gestión.

6.2.4 Políticas de Seguridad

Se desarrollaron las Políticas de Seguridad para la Corporación Medica Clínica Vida de la ciudad de Quibdó. Se tomó como base los lineamientos que brinda la norma ISO 27001, el ANEXO A de la norma ISO/IEC 27001:2013 Dominios, Objetivos de Control y Controles y las recomendaciones para las Políticas de Seguridad que plantea el Framework de Ciberseguridad de la NIST (National Institute of Standards and Technology)

Objetivo

Exhibir en forma clara las políticas de seguridad que deben conocer y cumplir todos los directivos sin importar su cargo, funcionarios contratistas o empleados y terceros naturales o jurídicos que presten sus servicios o tengan algún tipo de relación con la Sociedad Médica Clínica Vida de la ciudad de Quibdó.

Alcance

Las políticas que aquí se documentan, son de cumplimiento obligatoria para todos los funcionarios de la Corporación Médica Clínica Vida, que hagan uso directa o indirectamente de tecnologías de información y comunicaciones o de los activos de la misma.

Lineamientos de Políticas

Toda información que se utilice en los equipos de cómputo y por supuesto, bajo el uso de los sistemas operativos y de información de la Corporación Medica serán de carácter confidencial, por lo que ningún funcionario podrá hacer uso de ella con fines personales, tampoco podrá facilitarla a personal externo en cualquier forma de transmisión.

Los equipos designados a cada funcionario serán de su uso exclusivo y con fines laborales, siendo responsable de los daños realizados al mismo o al sistema operativo. Será un agravante si el uso indebido se realiza con fines lucrativos.

La tabla 1 resume las políticas desarrollas con sus respectivos objetivos, en el ANEXO 12. Políticas de Seguridad, se describen en detalle las políticas diseñadas para las Clínica Vida.

TABLA 1. Resumen de las Políticas de Seguridad.

POLITICA	OBJETIVO
Políticas de seguridad ligada a los recursos humanos	Asegurar que los empleados y contratistas comprendan sus responsabilidades, tomen conciencia de sus responsabilidades en materia de seguridad de la información, las cumplan y son los idóneos en los roles para los que se consideran, Proteger los intereses de la corporación medica durante el proceso de vinculación o desvinculación de empleados o contratistas
Políticas de seguridad en gestión de activos	Identificar los activos organizacionales de la corporación Medica Clínica vida, y definir las responsabilidades de protección apropiadas, así como prevenir la divulgación, modificación, el retiro o la destrucción de información almacenada en medios de soporte.
Políticas de seguridad en controles de acceso	Velar porque la información solo sea accedida por personal autorizado y solo para el desempeño de su función, limitar el acceso a información e instalaciones de procesamiento de información, haciendo que los usuarios rindan cuentas por la custodia de su información de autenticación.
Políticas de seguridad física y ambiental	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y las instalaciones de procesamiento de información de la Corporación Médica Clínica Vida y prevenir la perdida, daño, robo o compromiso de activos de la misma.
Políticas de seguridad operativa	Asegurar las operaciones correctas y seguras de las operaciones, protegiéndolas contra la perdida de datos, asegurando la integridad de los sistemas

	operacionales y minimizar el aprovechamiento de vulnerabilidades técnicas.
Políticas de seguridad en las telecomunicaciones	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte y mantener la seguridad de la información transferida dentro de la Corporación Médica o con cualquier entidad externa.
Políticas de seguridad para adquisición, desarrollo y mantenimiento de los sistemas de información.	Permitir que la adquisición o desarrollo de software para la corporación se realice con los controles adecuados, cumpla con las normas de licenciamiento y haya sido autorizado por el área de Sistemas. además, garantizar que la instalación de software en los equipos de la Corporación sea realizada por personal idóneo y autorizado para esta actividad.
Políticas de seguridad en relación con suministradores.	Asegurar la protección de los activos de información de la Corporación que sean accesibles a los proveedores, manteniendo el nivel de seguridad y la correcta prestación de servicio por parte de los proveedores.
Políticas de seguridad para la gestión de incidentes en la seguridad de la información.	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación y los responsables de atender los eventos o debilidades en materia de seguridad.
Políticas de seguridad en aspectos de seguridad de la información en la gestión de la continuidad del negocio.	Asegurar la disponibilidad de las instalaciones de procesamiento de información y la inclusión de la seguridad en los sistemas de gestión de continuidad de negocio en la Corporación Médica.
Políticas de cumplimiento.	Evitar violaciones de obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de requisitos de seguridad por parte de la Corporación Médica.

6.3 Definición del enfoque organizacional para la valoración del riesgo.

Luego de realizar visitas a la corporación sociedad médica Clínica Vida y de realizar entrevistas a los funcionarios, labores de observación y revisión de documentación de las dependencias de Sistemas, Facturación, Ambiental, Cartera, Jurídica, Control Interno, Almacén, Estadística, Revisión Fiscal, Pagaduría, Contabilidad, Archivo y Admisión, se obtuvo el un cuadro con el inventario de activos de información, el cual se encuentra en el ANEXO 11. Inventario de Activos de Información.

6.4 Identificación de los Riesgos.

Para la identificación de los riesgos en materia de Seguridad de la Información para la Clínica Vida, tomamos como referencia el modelo de madurez de COBIT adaptado a la realidad de la clínica vida.

Luego de realizar visitas a las distintas dependencias de la Corporación Médica Clínica Vida, realizar entrevistas a los funcionarios de distintas dependencias y labores de observación a los distintos procesos al interior de la misma, con el objetivo de determinar el estado actual en materia de seguridad de la información de los activos de información relacionados en el ANEXO 11, Inventario de Activos, se detectaron los siguientes hallazgos o amenazas en materia de Seguridad de la Información al igual que los controles recomendados por el ANEXO A de la norma ISO 27001:2013, su valoración está basada en el ANEXO 4, Escalas de Valoración. A continuación, se señalan algunos hallazgos relevantes, en el ANEXO 14. Tabla de Riesgos, se explican con más detalle dichos hallazgos.

- No se evidencia un conjunto de políticas para la seguridad de la información.
- No cuenta con asignación de responsabilidades para la seguridad de la información
- No se evidencia políticas de uso para dispositivos móviles ni para jornadas de teletrabajo.
- No se realizan jornadas de concienciación, educación y capacitación en seguridad de la información al personal.
- No cuenta con un inventario detallado de activos.

- No evidencia gestión de soportes extraíbles, eliminación de soportes, soportes físicos en transito ni control de unidades extraíbles en las estaciones de trabajo.
- Presenta deficiencias en las políticas de control de acceso.
- Se detecto falencias en los procedimientos de inicio de sesión seguros
- Se detecta deficiencias en la seguridad física.
- Presenta deficiencias en los controles contra códigos maliciosos.
- Carece de políticas y procedimientos de intercambio de información.
- No se han definido responsabilidades y procedimientos para la gestión de incidentes.
- no cuenta con revisiones independientes en materia de seguridad de la información.

6.5 Análisis y Evaluación de los Riesgos.

El análisis y evaluación de los riesgos en materia de Seguridad de la Información para la Clínica Vida, fue elaborado tomando como referencia el marco de Cyber seguridad de la NIST (National Institute of Standards and Technology). Por otra parte, en el ANEXO 10, diagnóstico del estado actual se presenta un resumen de los elementos tenidos en cuenta para la evaluación, así como su respectiva valoración. la evaluación completa y las valoraciones de la evaluación se encuentra en el ANEXO 8, en un documento ANEXO llamado ¨Evaluación en materia de Seguridad de la Información de la Clínica Vida¨.

6.6 Identificar y evaluar las opciones para el tratamiento de los riesgos.

Con la clínica se diseñó un plan de acción para convenir la manera en que serán tratados los riesgos cuyo nivel de madurez es muy bajo, en el que se traza responsabilidades y actividades para su tratamiento, las cuales se muestran a continuación:

6.6.1 Responsabilidades de la Alta Gerencia.

La implicación de la alta gerencia de la Corporación es uno de los principales componentes un Sistema de Gestión de Seguridad de la según la norma ISO 27001:2013.

La alta gerencia de la Corporación debe asumir que el Sistema de Gestión de Seguridad de la Información afecta a la gestión del negocio y requiere que todas las acciones futuras y las decisiones que se tomen solo las puedan desarrollar la alta dirección de la organización. No puede considerar que el Sistema de Gestión de Seguridad de la Información sea una cuestión meramente tecnológica o técnica de los niveles inferiores de la empresa sino todo lo contrario, la Gerencia debe tener la responsabilidad de gestionar los riesgos y los impactos del negocio.

Desde el punto de vista del alcance del Sistema de Gestión de Seguridad de la Información, el término dirección de la organización debe estar contemplado siempre las tareas fundamentales del Sistema de Gestión de Seguridad de la Información que ISO 27001:2013 asignan a la Dirección en los que se detallan los siguientes elementos: (ISO 27001)

La alta dirección de la Corporación debe comprometerse con la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información. Para ello, debe llevar a cabo las siguientes iniciativas:

- Desarrollar una política de Seguridad de la Información.
- Garantizar el cumplimiento de planes y objetivos de Sistema de Gestión de Seguridad de la Información.
- Constituir roles y responsabilidades de Seguridad de la Información.
- Informar la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad.
- Designar todos los recursos necesarios para llevar a cabo el Sistema de Gestión de Seguridad de la Información.
- Determinar todos los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asignar los recursos suficientes para todas las fases del Sistema de Gestión de Seguridad de la Información.
- Garantizar que se realizan todas las auditorías internas.
- Llevar a cabo revisiones periódicas del Sistema de Gestión de Seguridad de la Información.

6.6.2 Asignación de Recursos.

Para que se realicen todas las actividades vinculadas con el Sistema de Gestión de la Seguridad de la Información, es fundamental designar los recursos necesarios. Es tarea de la alta dirección la de garantizar que cuentan con los suficientes medios para:

- Operar, establecer, implementar, monitorizar, revisar y mantener el Sistema de Gestión de Seguridad de la Información.
- Poder asegurar que todos los procedimientos de seguridad de la información apoyan a los requerimientos de negocio.
- Detallar todos los requerimientos necesarios para cumplir con la legislación vigente.
- Suministrar todos los controles implementados de una forma correcta.
- Desarrollar todas las revisiones cuando sea necesario.
- Mejorar la eficiencia del Sistema de Gestión de Seguridad de la Información.

6.6.3. Formación y Concienciación.

Para conseguir el éxito del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013 es fundamental contar con dos elementos muy básicos como son la formación y la concienciación en Seguridad de la Información. Por ello, la Alta Gerencia de la Corporación debe garantizar que todos los empleados tengan sus responsabilidades asignadas y definidas en el Sistema de Gestión de Seguridad de la Información. Por lo que se deberá:

- Decidir las competencias necesarias que debe tener cada trabajador de la empresa en función de las tareas que vaya a desempeñar.
- Complacer las necesidades mediante planes de formación.
- Analizar y evaluar la eficiencia de las acciones que ha desarrollado.
- Conservar todos los registros de estudios, formación, habilidades, experiencia y cualificación.

La alta dirección deberá garantizar que todos los empleados relevantes se involucren y se conciencien de la importancia de las actividades relacionadas con la seguridad de la información y el grado de contribución a la consecución de los objetivos del Sistema de Gestión de Seguridad de la Información.

6.6.4. Revisión de Sistema de Gestión de Seguridad de la Información.

La tarea de la alta dirección de la Corporación es que, al menos una vez al año, revise el Sistema de Gestión de Seguridad de la Información, para poder garantizar que continúa siendo eficaz, eficiente y adecuado. Para ello, la Gerencia debe recibir una serie de información para ayudarle en esa toma de decisiones y entre ellas se destacan las siguientes:

- Amenazas o vulnerabilidades que no se ha trasladadas adecuadamente en evaluaciones de riesgos anteriores.
- Los resultados de las mediciones de eficacia.
- Resultados de las auditorías y revisiones del Sistema de Gestión de Seguridad de la Información.
- Controlar todas las partes interesadas.
- Productos, técnicas o procedimientos que puedan ser útiles para mejorar el rendimiento y eficiencia del Sistema de Gestión de Seguridad de la Información.
- Comunicar el estado de las distintas acciones preventivas y correctivas.
- El estado de las acciones iniciadas a raíz de las diversas revisiones anteriores de la Dirección de la Corporación.
- Cualquier cambio que puede afectar al Sistema de Gestión de Seguridad de la Información.
- Obtener recomendaciones de mejora.

Por otra parte, la Gerencia debe revisar el Sistema de Gestión de Seguridad de la Información y tomar las decisiones relativas y oportunas a:

- Enriquecer y desarrollar la eficiencia del Sistema de Gestión de Seguridad de la Información.

- Actualización del Plan de Tratamiento de Riesgos y de la evaluación de riesgos.
- Cambiar los Controles y procedimientos que afecten a la seguridad de la información. de esta forma, obtendremos como respuesta cambios internos o externos en los requisitos de los negocios.
- Mejorar la forma de medir la eficacia de los Controles de Seguridad.

6.6.5. Compromisos del Comité de Seguridad de la Información

Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. Desarrollar el plan de formación y sensibilización de la Corporación incorporando el componente de seguridad de la información en diferentes áreas.

6.7 Selección de los objetivos de control y los controles para el tratamiento de los riesgos.

Se siguió la metodología del Sistema de Gestión realizando un recorrido por los 14 dominios, 35 objetivos de control y 114 controles que plantea la norma ISO 27001:2013, para determinar control por control cuales aplican o no, y se definió la aplicabilidad de cada uno de ellos. En el ANEXO 9, Control de aplicabilidad se relacionan cada uno de ellos y su adaptación a los procesos de la clínica. También se diseñaron las Políticas de Seguridad y los Controles de Seguridad para la clínica, se busca Dejarlas documentadas, contribuir en la mitigación de los hallazgos relacionados en el diagnóstico de estado actual de la Clínica Vida, definir los procedimientos que se deben seguir en materia de Seguridad de la Información, así como los responsables de llevarlo a cabo.

Una vez que se han determinado los riesgos y su implicación a la seguridad de la información de la Corporación Medica Clínica Vida, se debe buscar la manera de tratarlos. El riesgo puede ser mitigado, transferido o asumido. Para que este proceso se lleve a efecto, es necesario que todos los elementos de la organización, es decir, personas, equipos, instalaciones,

procesos, tareas, documentos, y más componentes de la misma, se encuentren alineadas a directrices claras y documentadas que establezcan lo que debe hacerse, la manera de hacerlo y las responsabilidades por su incumplimiento. de aquí se deriva la urgente necesidad de contar con Controles de Seguridad para la organización, como un factor fundamental y básico para enfocar la actividad de la seguridad de la información de manera efectiva.

6.7.1 Controles de Seguridad

Fueron elaborados los controles de seguridad para la clínica, con base en la Tabla A.1. Objetivos de control y controles del ANEXO A de la norma técnica colombiana NTC-ISO/IEC 27001:2013. A continuación, se describe su objetivo, su alcance y un resumen de los controles diseñados para la Cínica Vida. En el ANEXO 13. Controles de Seguridad, se evidencian completamente y en detalle todos los controles diseñados para la Clínica Vida.

Objetivo

Brindar instrucciones para todo aquel que tenga relación directa o indirecta con la Clínica Vida, dando orientación de estricto cumplimiento, concientizándolos sobre el correcto uso de los activos de información, equipos, sistemas operativos y sistemas de información y la sensibilidad de los datos manejados por los mismos.

Alcance

Los controles que aquí se documentan, son de cumplimiento obligatoria para todos los funcionarios de la Corporación Médica Clínica Vida, que hagan uso directa o indirectamente de tecnologías de información y comunicaciones o de los activos de la misma. El comité se Seguridad de la Información será el encargado de verificar cumplimiento y revisión periódica de los controles de seguridad, con el fin de realizar los ajustes necesarios que resulten por crecimiento de la Corporación o la aparición de nuevas amenazas.

La tabla 2 presenta un resumen de los controles y el objetivo de cada uno de los controles diseñados para la Clínica Vida.

TABLA 2. Resumen de Controles

CONTROLES	OBJETIVOS
Controles de políticas de seguridad.	Brindar apoyo y orientación a la dirección de la Corporación Medica con respecto a la seguridad de la información, y los reglamentos y leyes pertinentes.
Controles para la organización de la seguridad de la información.	Gestionar y mantener la seguridad de la información y los servicios de procesamiento dentro de la organización.
Controles de gestión de activos	Lograr y mantener la protección adecuada de los activos de la Corporación, además, mantener actualizados los registros de inventario.
Controles de los recursos humanos.	Asegurar que los empleados, contratistas y usuarios por tercera parte entiendan sus responsabilidades y son adecuados para los roles para los que se les considera, reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones, y que estén conscientes de las amenazas y preocupaciones de seguridad de la información, sus responsabilidades y sus deberes y que estén equipados para apoyar las políticas de seguridad durante el desarrollo de sus funciones.
Controles de seguridad física del entorno.	Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información, y evitar perdida, daño o puesta en peligro los activos y la interrupción de las actividades de la Corporación Médica.
Controles de gestión de comunicaciones y operaciones.	Asegurar la operación correcta y segura de los servicios de procesamiento de información manteniendo la integridad y disponibilidad de la información, mantener un grado de seguridad en

	la prestación de los servicios y minimizar el riesgo de fallas de los sistemas, asegurar la protección de la información en las redes y las infraestructuras de soporte y evitar la divulgación, modificación, retiro o destrucción de activos no autorizada en la Corporación Médica.
Controles de acceso	Controlar el acceso no autorizado a la información de los servicios de procesamiento de información, servicios en red, sistemas operativos y sistemas de información de la Corporación.
Controles de adquisición, desarrollo y mantenimiento de sistemas de información.	Garantizar que la seguridad es parte integral de los sistemas de información, protegiendo la confidencialidad, autenticidad o integridad de la información de la Clínica por medios criptográficos, manteniendo la seguridad del software y de la información del sistema de aplicaciones y reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.
Controles de gestión de incidentes de la seguridad de la información.	Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente, y se aplique un enfoque consistente y eficaz.
Controles de gestión de la continuidad del negocio.	Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.
Controles de cumplimiento.	Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

6.8 Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.

Falta la implementación de los planes de acción para mitigar los riesgos encontrados y someter a aprobación los riesgos residuales posteriores a la implementación de los planes de acción.

6.9 Obtener autorización de la dirección para implementar y operar el Sistema de Gestión de Seguridad de la Información.

Al momento del cierre de este proyecto, la junta directiva de la clínica vida se encuentra evaluando la posible implementación del Diseño del Sistema de Gestión y la y las posibles formas de financiación.

6.10 Elaboración de declaración de aplicabilidad.

Declaración de Aplicabilidad

La declaración de aplicabilidad diseñada para la Corporación Medica con base en los 14 dominios, 35 objetivos de control y 114 controles que plantea la norma ISO 27001:2013, se encuentra adjunta en los anexos del proyecto, ANEXO 9. Control de Aplicabilidad.

7. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

En este capítulo se recapitulan las soluciones planteadas para el diseño del Sistema de Gestión de Seguridad de la Información de la Clínica Vida, resumiendo los avances logrados en cada una de las etapas del proyecto.

Con el diseño del Sistema de Gestión para la Clínica Vida, se logró identificar e inventariar los activos de información, conocer el estado actual de la Clínica en materia de Gestión de Seguridad de la Información, identificar los riesgos asociados a estos activos y diseñar herramientas para minimizarlos. Finalmente se entregó una propuesta para su futura implementación.

7.1. Identificación e Inventario de Activos:

Se identificaron y relacionaron los principales activos de información de la clínica, principalmente aquellos que utilizan las plataformas de tecnologías de la información de la Clínica, los responsables de estos activos. Este inventario de activos es importante porque permitió conocer con que cuenta la clínica y que es lo que se debe proteger. En el ANEXO 11 expone completamente los activos identificados.

7.2. Diagnóstico del Estado Actual:

El diagnóstico del estado actual permitió conocer la forma como la Clínica Vida está protegiendo los activos relacionados en el inventario de activos, estipulando si los controles o medidas que se están aplicando son débiles, necesitan mejora o son suficientes. En el ANEXO 10. Se explican los criterios tenidos en cuenta para la obtención del diagnóstico y el ANEXO 8. Se muestra la evaluación completa.

7.3. Identificación y Análisis de Riesgos:

La identificación y el análisis de los riesgos, permitió conocer las debilidades que tiene la Clínica Vida en Gestión de Seguridad, con los hallazgos relacionados en el ANEXO 14, y el apoyo de anexo A de la norma ISO 27001:2013, se pudo diseñar los controles y políticas de seguridad para la

clínica, los cuales se encuentran relacionados en los ANEXOS 12 y 13 del proyecto.

7.4. Diseño de Controles y Políticas de Seguridad:

Se diseñaron los controles y las políticas de seguridad, estableciendo un control de aplicabilidad encauzado a la naturaleza del negocio de la Clínica Vida, aprobando de acuerdo a esta naturaleza en cada uno de los dominios y sub dominios del anexo A de la norma ISO 27001:2013 son aplicables o excluibles, lo cual se puede validar en el ANEXO 9 control de aplicabilidad. También se diseñaron los controles de seguridad con el propósito de reducir los riesgos identificados en el ANEXO 14. Tabla de Riesgos. Además, se diseñaron las políticas de seguridad en el ANEXO12. Políticas de Seguridad de la Información, con la voluntad de definir las responsabilidades de todos los actores directos o indirectos de la Clínica correspondiente a la seguridad de la información.

7.5. Presentación de Propuesta del Sistema de Gestión

Se presenta una propuesta del Sistema de Gestión de Seguridad de la Información para la Clínica Vida, la cual se le entrega a la Alta gerencia quien analiza las posibilidades de implementación en una segunda etapa.

8. CONCLUSIONES

Al terminar este proyecto, se concluye que el Sistema de Gestión de Seguridad de la Información diseñado de acuerdo a las necesidades de la Clínica Vida de Quibdó permite tener un mejor control sobre los riesgos de afectación de la información en términos de la disponibilidad, integridad y autenticidad de su información.

Con el desarrollo de este proyecto, se logró Identificar el estado actual de la Clínica Vida en materia de Gestión de Seguridad de la Información, permitiendo diseñar una propuesta de implementación del Sistema de Gestión de Seguridad de la Información ajustada a los hallazgos detectadas en el diagnóstico previamente realizado, obteniendo todos los pormenores necesarios del área de infraestructura de la Clínica para ubicar y valorar los riesgos y vulnerabilidades, construyendo un modelo basado en las necesidades reales de la Clínica.

El modelo de Seguridad de la Información diseñado en este trabajo necesita actualización y retroalimentación constante, de lo contrario no se acoplará de forma correcta a riesgos futuros institución, ya que no evolucionará de la mano del crecimiento que tenga la Clínica. El éxito en la posible implementación de este modelo diseñado depende del apoyo de la Alta Gerencia y las autoridades de la Clínica Vida ya que serán las encargadas de su difusión y acatamiento.

9. TRABAJOS FUTUROS

Se espera que en un futuro se desarrollen otros proyectos basados en el que aquí se presenta, que consientan implementar y mantener el ciclo de vida de un Sistema de Gestión de Seguridad de la Información para la Corporación Medica Clínica Vida de la ciudad de Quibdó, permitiendo detectar amenazas o debilidades generadas por el crecimiento de la corporación o por los avances tecnológicos.

10. REFERENCIAS

Bibliografía

SILVA, C. A. (2015). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO . Colombia.

ESET. (2016). *Tendencias 2016 Insecurity Everywhere.* Año tras año, desde los Laboratorios de ESET a nivel mundial hacemos un repaso de los sucesos más importantes del año y de su impacto tanto en el mundo corporativo como en la información de los usuarios hogareños. Al conversar, debatir y evaluar qué es lo que sucedió en el mundo de la tecnología, es difícil resumir todo en una sola frase. la velocidad con la que aparecen nuevas tecnologías, los reportes de ataques, nuevas familias de malware o fallas de seguridad de impacto global, hacen de la seguridad un desafío cada vez más importante para los negocios, las empresas, los gobiernos y los usuarios alrededor del mundo., Laboratorios, Buenos Aires.

ESET. (2016). *Eset Security Report Latinoamérica .* Equipo de Investigacion Eset Latinoamerica, Buenos Aires.

Gobernacon del Chocó. (14 de 12 de 2012). (http://www.choco.gov.co/informacion_general.shtml, Productor) Recuperado el 5 de 6 de 2016, de http://www.choco.gov.co/: http://www.choco.gov.co/informacion_general.shtml

Vida, C. (2011). *Quienes Somos*. Recuperado el 20 de 11 de 2015, de clinicavidachoco: http://www.clinicavidachoco.com.co/?mod=pag&id=4

ISO / IEC 27001. (2013). *Gestión de seguridad de la información*. Obtenido de http://www.iso.org/: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Bartolin, J. A. (2008). *Seguridad de la Informacion Redes, Informatica y Sistemas de Informacion .* (M. J. Razo, Ed.) España: Paraninfo Cengage Learning.

Álvarez, L. G. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. *Asociación Española de Normalización y Certificación , 2*, 13-19.

OHANNA CAROLINA BUITRAGO, D. H. (2012). Diseño de Una Metodología Para la Implementación del Sistema de Gestión de Seguridad de la Información- SGSI, En El Sector de Laboratorios de Análisis Microbiológicos, Basado En ISO 27001. *Diseño de Una Metodología Para la Implementación del Sistema de Gestión de Seguridad de la Información- SGSI, En El Sector de Laboratorios de Análisis Microbiológicos, Basado En ISO 27001* . Bogota , Cundinamarca, Colombia.

know, w. d. (2010). *Information asset definition*. Recuperado el 10 de 4 de 2016, de www.whatdotheyknow.com: https://www.whatdotheyknow.com/request/216130/response/539410/attach/3/Information%20asset%20definition%20page%20v1.3.pdf

ISO 27001. (s.f.). *ISO2700.ES*. (A. L. Spohr, Productor) Recuperado el 10 de 05 de 2015, de so27000.es: http://www.iso27000.es/

Super Intendencia de Industria y Comercio. (31 de 12 de 2008). Recuperado el 10 de 4 de 2016, de www.sic.gov.co: http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf

Senado Republica de Colombia. (21 de 08 de 1999). *Secretaría de Senado*. Recuperado el 10 de 04 de 2016, de www.secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Mintic. (30 de 06 de 2015). *Ley 1273 de 2009*. Recuperado el 20 de 11 de 2015, de Mintic: http://www.mintic.gov.co/portal/604/w3-article-3705.html

Alcaldia Bogotá. (30 de 7 de 2009). *Ley 1341 de 2009 Nivel Nacional*. Recuperado el 10 de 2016, de http://www.alcaldiabogota.gov.co/: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

Datos, L. q. (05 de 08 de 2013). *Lo que tiene que saber sobre la nueva ley de Protección de Datos.* Recuperado el 20 de 11 de 2015, de www.elpais.com.co: http://www.elpais.com.co/elpais/colombia/noticias/tiene-saber-sobre-nueva-ley-proteccion-datos

Datos, L. d. (30 de 07 de 2013). *Ley de Protección de Datos.* Recuperado el 20 de 11 de 2015, de www.mincit.gov.co: http://www.mincit.gov.co/publicaciones.php?id=7456

Colombia, Senado Republica de. (18 de 10 de 2012). *secretariasenado*. Recuperado el 10 de 4 de 2016, de www.secretariasenado.gov.co: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

AGESIC. (8 de 10 de 2009). *Decreto N° 452/009, de 28 de setiembre de 2009*. Recuperado el 10 de 2016, de http://www.agesic.gub.uy: http://www.agesic.gub.uy/innovaportal/v/299/1/agesic/decreto-n%C2%B0-452_009-de-28-de-setiembre-de-2009.html

SALUD, M. D. (08 de 07 de 1999). *RESOLUCION NUMERO 1995 DE 1999.* Recuperado el 2016 de 04 de 20, de www.minsalud.gov.co: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

Consejo Nacional de Política Económica y Social. (2016). *https://cc-csirt.policia.gov.co/Publicaciones/conpes_3854*. Recuperado el 12 de 05 de 2016, de https://cc-csirt.policia.gov.co/: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

AURA LUCIA CASADIEGOS, M. Q. (14 de 04 de 2014). SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN(SGSI) PARA EL ÁREA DE CONTABILIDAD DE LA E.S.E. HOSPITAL LOCAL DE RIO DE ORO CESAR. 144. Ocaña, Santander, colombia.

Gil, K. I. (2015). la seguridad de la información, clave en la protección de datos sanitarios. *Asamblea Legislativa Plurinacional , 9* (38), 56-64.

Vasco, R. T. (05 de 2015). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓNPARA UNA ENTIDAD ESTATAL DE SALUD DE ACUERDO A LA ISO/IEC 27001:2013 . *Tesis de Grado* , 90. Lima, Perú.

MinTic. (s.f.). *Gestion_Incidentes*. Recuperado el 06 de 2017, de http://www.mintic.gov.co/: http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

11. ANEXOS

ANEXO 1. FORMATO DE INVENTARIO DE ACTIVOS DE INFORMACIÓN.
ANEXO. 2. FORMATO DE ASIGNACIÓN DE ACTIVOS.
ANEXO. 3. CUADRO DE INCIDENTES DE SEGURIDAD.
ANEXO. 4. ESCALAS DE VALORACIÓN.
ANEXO. 5. FAMILIA DE LA NORMA ISO 27000.
ANEXO. 6. ANEXO A. DE LA NORMA ISO 27001:2013.
ANEXO. 7. NORMA ISO 27001:2013.
ANEXO. 8. EVALUACIÓN ESTADO EN MATERIA DE SEGURIDAD CLÍNICA VIDA.
ANEXO. 9. CONTROL DE APLICABILIDAD.
ANEXO. 10. DIAGNOSTICO DEL ESTADO ACTUAL.
ANEXO. 11. INVENTARIO DE ACTIVOS DE INFORMACIÓN.
ANEXO. 12. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPORACIÓN MÉDICA CLÍNICA VIDA DE LA CIUDAD DE QUIBDÓ..
ANEXO. 13. CONTROLES DE SEGURIDAD.
ANEXO. 14. TABLA DE RIESGOS.
ANEXO. 15. GOBIERNO DEL SISTEMA DE GESTION

ANEXO 5.

FAMILIA DE LA NORMA ISO 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

ISO 27000:
En fase de desarrollo; su fecha prevista de publicación es noviembre de 2008. Contiene términos y definiciones que se emplean en toda la serie 27000. la aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está prevista que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.

ISO 27001:
Publicada el 15 de octubre de 2005. 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 por auditores externos los SGSI de las organizaciones.

Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su ANEXO A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO 27002:
Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. 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. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. Desde 2006, sí está traducida en Colombia (como ISO 17799.

ISO 27003:
En fase de desarrollo; su fecha prevista de publicación es mayo de 2009. Consistirá en una guía de implementación de SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004:
Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PHVA.

ISO 27005:
Publicada el 4 de junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

ISO 27006:
Publicada el 13 de febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específico relacionados con ISO 27001 y los SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican

a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

ISO 27007:
En fase de desarrollo; su fecha prevista de publicación es mayo de 2010. Consiste en una guía de auditoría de un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

ISO 27011:
Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031:
Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032:
Consiste en una guía de gestión de seguridad de la información relativa a la ciberseguridad.

ISO 27033:
Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provee la revisión, ampliación y re-numeración de ISO 18028.

ISO 27034:
Consiste en una guía de gestión de seguridad de la información relativa a la seguridad en aplicaciones.

ISO 27799:
Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones

sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud.

ISO 27799:2008

Se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

ANEXO 12.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPORACIÓN MÉDICA CLÍNICA VIDA DE LA CIUDAD DE QUIBDÓ.

A continuación, se desarrollan las Políticas de Seguridad para la Corporación Medica Clínica Vida de la ciudad de Quibdó. Se tomó como base los lineamientos que brinda la noema ISO 27001, el ANEXO A de la norma ISO/IEC 27001:2013 Dominios Objetivos de Control y Controles y las recomendaciones para las Políticas de Seguridad que plantea el Framework de Ciberseguridad de la NIST (National Institute of Standards and Technology)

Objetivos

Exhibir en forma clara las políticas de seguridad que deben conocer y cumplir todos los directivos sin importar su cargo, funcionarios contratistas o empleados y terceros naturales o jurídicos que presten sus servicios o tengan algún tipo de relación con la Sociedad Médica Clínica Vida de la ciudad de Quibdó.

El presente documento sirve de instrumento para todo aquel que tenga relación directa o indirecta con la Corporación, dando lineamientos de estricto cumplimiento, concientizándolos sobre el correcto uso de los activos de información, equipos, sistemas operativos y sistemas de información y la sensibilidad de los datos manejados por los mismos.

Alcance

Las políticas que aquí se documentan, son de cumplimiento obligatoria para todos los funcionarios de la Corporación Médica Clínica Vida, que hagan uso directa o indirectamente de tecnologías de información y comunicaciones o de los activos de la misma.

Compromisos Por Parte de la Dirección

Como una muestra del compromiso de la Gerencia de Corporación Médica Clínica Vida con el diseño e implementación de las políticas de seguridad de la información en la entidad, aprueba las políticas contenidas en este documento, así como también su apoyo en:

El fomento de manera activa para la creación de una cultura de seguridad dentro de la entidad.

Divulgación de estas políticas a cada uno de los funcionarios de la entidad.

Verificación de que las políticas del presente manual sean cumplidas a cabalidad por parte de los funcionarios, proveedores o quien tenga relación directa con la corporación.

Revisión y actualización periódica de estas políticas a cada uno de los funcionarios de la entidad y personas naturales o jurídicas que tengan relación directa o indirecta con la Corporación.

El Área de Sistemas será la encargada de difundir, capacitar y sensibilizar al resto de la Corporación las Políticas de Seguridad, asimismo se creará el comité de Gestión de Seguridad de la información, el mismo se encargará de reunirse periódicamente para evaluar o actualizar este modelo. El comité estará conformado por:

- Oficial de Seguridad de la información
- Director General Administrativo
- Responsable de Talento Humano
- Responsable del Área de infraestructura
- Responsable de Auditoria Interna
- Responsable de Jurídico

El oficial de Seguridad de la información no pertenecerá a tecnología, pero debe tener los conocimientos necesarios en cuanto a los procesos que se gestionan en la Dirección de Tecnología y Comunicaciones además de conocimientos esenciales sobre tecnología en el caso de servidores su definición, función e importancia.

Lineamientos de Políticas

Toda información que se utilice en los equipos de cómputo y por supuesto, bajo el uso de los sistemas operativos y de información de la Corporación

Medica serán de carácter confidencial, por lo que ningún funcionario podrá hacer uso de ella con fines personales, tampoco podrá facilitarla a personal externo en cualquier forma de transmisión.

Los equipos designados a cada funcionario serán de su uso exclusivo y con fines laborales, siendo responsable de los daños realizados al mismo o al sistema operativo. Será un agravante si el uso indebido se realiza con fines lucrativos.

Políticas de Seguridad Ligada a los recursos Humanos

Objetivos.

Asegurarse que los empleados y contratistas comprendan sus responsabilidades, tomen conciencia de sus responsabilidades en materia de seguridad de la información, las cumplan y son los idóneos en los roles para los que se consideran,

Proteger los intereses de la corporación medica durante el proceso de vinculación o desvinculación de empleados o contratistas

El factor humano es muy importante en el mantenimiento de la seguridad de la información de la entidad, por lo que se debe contar con el personal mejor calificado para cada uno de los cargos.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe asegurar antes de la realización de una contratación las responsabilidades de seguridad, describiendo de forma clara y precisa el cargo, asíí como los términos y condiciones del contrato, el cual debe incluir una cláusula de confiabilidad y cumplimiento de las políticas de seguridad del presente documento.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe validar que la información suministrada por los aspirantes a algún cargo disponible sea verás, antes de que su vinculación definitiva. Además, deberá verificar los antecedentes del personal aspirante al cargo.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe asegurar que los funcionarios, contratistas y demás colaboradores de la Corporación Médica Clínica Vida, entiendan sus

responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe desarrollar un programa de concientización sobre protección de la información para todo el personal. Todo el personal deberá asistir a los cursos que se impartan dentro del programa de concientización, aplicando los conocimientos adquiridos en sus puestos de trabajo.

Al presentarse algún cambio en los puestos de trabajo o funciones, se revisará nuevamente los perfiles y permisos de los funcionarios para validar que quede con los privilegios idóneos para su nuevo cargo.

Cuando se dé por finalizado un contrato, el personal saliente debe firmar un acuerdo de confidencialidad para evitar la fuga de información sensible o clasificada como reservada.

Políticas de Seguridad En Gestión de Activos

Objetivo

Identificar los activos organizacionales de la corporación Medica Clínica vida, y definir las responsabilidades de protección apropiadas, así como prevenir la divulgación, modificación, el retiro o la destrucción de información almacenada en medios de soporte.

La Corporación Medica Clínica Vida mantendrá un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el Área de Tecnología o Sistemas.

La Corporación Medica Clínica Vida es propietaria de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la Corporación que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

Los activos de información pertenecen a la Corporación Medica Clínica Vida y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

Los usuarios deben utilizar únicamente los programas y equipos autorizados por el Área de Tecnología o Sistemas.

La Corporación Medica Clínica Vida proporcionará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Corporación, los funcionarios solo podrán realizar Backup de sus archivos personales o de información pública.

Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la Corporación Medica Clínica Vida; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

Periódicamente, el Área de Tecnología o Sistemas efectuará la revisión de los programas utilizados en cada dependencia. la descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información de la Corporación.

Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la mesa de ayuda del Área de Tecnología o Sistemas con su correspondiente justificación para su respectiva viabilidad.

Estarán bajo custodia del Área de Tecnología o Sistemas los medios magnéticos/electrónicos (CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los *passwords* de administración de los equipos informáticos, sistemas de información o aplicativos.

En caso de ser necesario y previa autorización del Comité de Seguridad Informática y de Sistemas de la Corporación Medica Clínica Vida, los funcionarios del Corporación podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o

reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.

Los recursos informáticos de la Corporación Medica Clínica Vida no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos.

Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Tecnología y Sistemas de Información:

Modificar, revisar, transformar o adaptar cualquier software propiedad la Corporación.

Descompilar o realizar ingeniería inversa en cualquier software de propiedad la Corporación.

Copiar o distribuir cualquier software de propiedad la Corporación.

El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento.

El usuario será responsable de todas las transacciones o acciones efectuadas con su cuenta de usuario.

Ningún usuario deberá acceder a la red o a los servicios TIC la Corporación, utilizando una cuenta de usuario o clave de otro usuario.

Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la seguridad de los recursos informáticos de la Corporación. El Área de Tecnología o de la Corporación, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus antes de ser instalados en la infraestructura TIC de la Corporación.

Todos los archivos provenientes de equipos externos a la Corporación, deben ser revisados para detección de virus antes de su utilización dentro de la red de la Corporación.

Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios del Área de Tecnología o Sistemas de la Corporación.

La información la Corporación Medica Clínica Vida debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información esta segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

de ser necesario, se asignará a cada funcionario una estación de trabajo y de los activos necesarios para apoyar al cumplimiento de sus labores.

Cada usuario es responsable del equipo y los activos que se le asigne o facilite, por lo que debe procurar su cuidado.

No se permite el traslado de los equipos de cómputo, sus partes o de activos a un área distinta a la que fue asignado. Para poder realizarlo se debe solicitar por escrito al jefe del área de Sistemas.

No es permitido el uso de dispositivos de almacenamiento extraíbles como memorias USB o discos externos.

Evitar la exposición directa al sol o al polvo.

No está permitido fumar así como tampoco el consumo de alimentos y/o bebidas en los puestos de trabajo.

Informar de forma oportuna cualquier incidente que impida el buen funcionamiento del equipo y/o del sistema operativo al Área de Sistemas (Formato Reporte de Incidente).

Las solicitudes de instalación o cambio, ya sea del equipo completo o alguna de sus partes, deben ser aprobadas por los jefes del área solicitante y del Área de Sistemas.

Políticas de Seguridad En Controles de Acceso

Objetivo

Velar porque la información solo sea accedida por personal autorizado y solo para el desempeño de su función, limitar el acceso a información e instalaciones de procesamiento de información, haciendo que los usuarios rindan cuentas por la custodia de su información de autenticación.

La Corporación Médica Clínica Vida suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

Todo trabajo que utilice los servidores de la Corporación Médica Clínica Vida con información de la entidad, sus funcionarios o contratistas, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación de la Corporación.

La conexión remota a la red de área local de la Corporación Médica Clínica Vida debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

La corporación asignará a cada usuario una cuenta para el ingreso a la red de datos, con la cual podrán acceder a una carpeta personal así como otra para compartir archivos con los demás usuarios.

Deben ser utilizados exclusivamente por personal de la entidad con autorización para ello.

Los directorios asignados deben utilizarse solo para fines institucionales, evitando guardar archivos personales además de fotos, música, videos o material innecesario.

Evitar acceder, modificar o borrar información privada de otros usuarios ajenos a su propiedad.

Los archivos y carpetas almacenados en la red son propiedad de la entidad, sin que exista un derecho particular sobre ellos.

Cada funcionario debe estar identificado para acceder al sistema operativo y al sistema de información mediante una cuenta de usuario, la cual tendrá ciertos permisos o privilegios dependiendo del rol asignado. Para este ítem se aplicarán las siguientes políticas:

Toda solicitud de creación de cuenta o modificación de la misma debe realizarse por escrito (jefe del Área Administrativa o quien realice las funciones de Gestión Humana), debidamente autorizada por los jefes del área solicitante y del Área de Sistemas (Formato Creación/Modificación de usuarios).

Solo el jefe del Área de Sistemas podrá eliminar una cuenta de usuario, No se creará cuentas de Invitado, tampoco a personal externo.

El jefe del Área Administrativa o quien realice las funciones de Gestión Humana, deberá informar de manera oportuna situaciones que impliquen creación, modificación y/o borrado de cuentas de usuario, tales como rotación de personal, despidos o renuncias, etc., con el fin de mantener la base de datos de usuarios actualizada (Formato Creación/Modificación de usuarios).

Se verifica que el usuario que intenta ingresar al sistema sea quien dice ser, mediante un mecanismo de autenticación, compuesto por la combinación de usuario y contraseña.

El usuario y la contraseña deben ser de uso personal, siendo el dueño responsable de todas las acciones realizadas, y esta se debe mantener de forma confidencial, ya que solo el dueño debe conocerla. El usuario y su contraseña, son personales e intransferibles.

Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Corporación.

Los usuarios deben tener en cuenta los siguientes aspectos de seguridad:

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.

Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.

Las claves o contraseñas deben:

- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, nombre de mascotas, etc.
- Tener mínimo diez caracteres alfanuméricos (Mayúsculas, Minúsculas, Números y Caracteres especiales).
- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Cambiarse obligatoriamente cada 30 días, o cuando lo establezca el Área de Tecnología o de Sistemas.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- No ser reveladas a ninguna persona, incluyendo al personal del Área de Tecnología o de Sistemas.
- No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado por el Área de Tecnología o de Sistemas.

Políticas de Seguridad Física y Ambiental

Objetivo

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y las instalaciones de procesamiento de información de la Corporación Médica Clínica Vida y prevenir la perdida, daño, robo o compromiso de activos de la misma.

La instalación de software en los computadores suministrados por la Corporación Médica Clínica Vida, es una función exclusiva del Área de Tecnología y Sistemas de Información o por personal autorizado por dicha dependencia. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.

Solo el personal del Área de Sistemas está facultado para abrir, desarmar, cambiar o instalar piezas del equipo de cómputo, así como formatear, instalar, reinstalar o modificar el sistema operativo o cualquier otro programa en la estación de trabajo.

El préstamo de equipos de cómputo, computadores portátiles y video proyectores se debe tramitar a través del área de Sistemas con anticipación y se proveerá de acuerdo a la disponibilidad.

Los equipos que ingresan temporalmente a la Corporación Medica Clínica Vida que son de propiedad de terceros: deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización, la corporación Médica Clínica Vida no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

El Área de Sistemas no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la Corporación Médica Clínica Vida.

Los usuarios no deben mantener almacenados en los discos duros, de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.

A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el área Administrativa.

Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

Deben existir planos que describan las conexiones del cableado. El acceso a los centros de cableado (Racks), debe estar protegido.

Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.

Para que los equipos puedan salir fuera de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la Corporación Médica Clínica Vida.

Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la Corporación Médica Clínica Vida (consultores, pasantes, visitantes, etc.) será registrado y controlado en las porterías de ingreso o salida de la Corporación. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información.

El traslado entre dependencias de la Corporación de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

El personal de la Corporación Médica Clínica Vida, debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada,

copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

El personal de la Corporación Médica Clínica Vida debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Todos los funcionarios de la corporación deben apagar completamente los equipos al finalizar su jornada laboral con el fin de ahorrar energía eléctrica y prevenir daños en los equipos.

Políticas de Seguridad Operativa

Objetivo

Asegurar las operaciones correctas y seguras de las operaciones, protegiéndolas contra la perdida de datos, asegurando la integridad de los sistemas operacionales y minimizar el aprovechamiento de vulnerabilidades técnicas.

La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como Discos externos, Memorias USB, CD, DVD, etc.

Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (Cifrado) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos o Back UP periódicos.

Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes o por requerimiento legal.

Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.

Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la Corporación Medica Clínica Vida.

Semanalmente los administradores de infraestructura de Corporación Medica Clínica Vida, verificarán la correcta ejecución de los procesos de Backup,

El Área de Tecnología o Sistemas debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la Corporación Medica Clínica Vida.

Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega la Corporación Medica Clínica Vida a los usuarios.

Políticas de Seguridad en las Telecomunicaciones

Objetivo

Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte y mantener la seguridad de la información transferida dentro de la Corporación Médica o con cualquier entidad externa.

Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, ser· motivo de verificación y tendrá como resultado directo la realización de una auditoria de seguridad.

El departamento de Sistemas deberá emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Los accesos a la red interna o local desde una red externa de la Corporación o extranet, se harán mediante un mecanismo de autenticación seguro y el tráfico entre ambas redes o sistemas ser cifrado.

Se registrará todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la Corporación o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la Corporación.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet.

El área de los servidores, debe permanecer con acceso restringido, sólo el personal autorizado tiene permitido el ingreso.

Cualquier persona externa que ingrese a la Oficina de Sistemas, debe registrarse en la bitácora de ingreso, proporcionando su nombre, firma y motivo de ingreso.

Queda prohibida la manipulación de los equipos del área de servidores por personal no autorizado para ello.

Todos los equipos deben estar conectados a un sistema de alimentación ininterrumpida de corriente eléctrica.

El cuarto de servidores debe estar en la temperatura adecuada, manteniendo un segundo aire acondicionado de respaldo.

El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en

cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Corporación Medica Clínica Vida, que sea creado a nombre personal, como redes sociales, *twitter*®, *facebook*, *youtube* likedink o *blogs,* se considera fuera del alcance del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no son de propiedad de la Corporación Medica Clínica Vida, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Área de Tecnología o Sistemas de la Corporación.

La instalación, activación y gestión de los puntos de red es responsabilidad del Área de Tecnología o Sistemas.

Se permite a los usuarios de la Corporación Medica Clínica Vida, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.

Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la corporación.

Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la Corporación Medica Clínica Vida se consideran bajo el control de la entidad.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el la Corporación y no debe utilizarse para ningún otro fin.

El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.

Los usuarios deben ser precavidos al abrir mensajes de personas desconocidas, evitando abrir archivos adjuntos que puedan afectar el software instalado en el equipo.

No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la Corporación, su cuenta de correo será desactivada.

Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo, el área de Recursos Humanos es la responsable de solicitar la modificación o cancelación de las cuentas electrónicas a la Oficina de sistemas del de la Corporación.

Las cuentas de correo electrónico son propiedad de la Corporación Médica Clínica Vida, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Corporación y no debe utilizarse para ningún otro fin.

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.

No facilitar el usuario y la contraseña a terceras personas.
Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Corporación.

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos.

Políticas de Seguridad Para Adquisición, Desarrollo y Mantenimiento de Los Sistemas de Información.

Objetivo

Permitir que la adquisición o desarrollo de software para la corporación se realice con los controles adecuados, cumpla con las normas de licenciamiento y haya sido autorizado por el área de Sistemas. además, garantizar que la instalación de software en los equipos de la Corporación sea realizada por personal idóneo y autorizado para esta actividad.

El Área de Sistemas será la encargada de determinar de acuerdo con las necesidades particulares de los funcionarios cual es el software a instalar en los equipos de cómputo.

Solo el Área de Sistemas puede realizar instalaciones, modificaciones de software y de las configuraciones del mismo en los equipos de cómputo.

Solo se tendrá instalado software que este licenciado y que sea de carácter legal.

Se podrá instalar software tipo Free, GNU, Shareware, Demos partiendo de un análisis de licenciamiento, seguridad y de una necesidad particular solicitada expresamente por el usuario o cualquier persona autorizada mediante carta dirigida al jefe del Área de Sistemas y que lo considere necesario para el desarrollo de sus funciones administrativas.

Se deberá mantener cifrada la información reservada o restringida durante su almacenamiento y/o transmisión por cualquier medio con el fin de mantener la confiabilidad e integridad de la misma.

El Área de Sistemas debe establecer un procedimiento para la verificación que los programas o aplicativos que requieran la transmisión de información clasificada como reservada o restringida cuenten con algún método adecuado de cifrado de datos.

Durante el desarrollo de aplicaciones propias o en la contratación con terceros para este fin, se debe asegurar que los sistemas construidos cumplan con el cifrado de la información establecido en la Corporación.

Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de seguridad de la información.

En caso de desarrollos propios de la entidad se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la Corporación.

Todo nuevo hardware o software que se vaya a adquirir y conectar a la plataforma tecnológica de la Corporación Medica Clínica Vida, por cualquier dependencia o proyecto de la Corporación, deberá ser gestionado por el Área de Tecnología o Sistemas para su correcto funcionamiento.

La compra de una licencia de un programa permitirá a la Corporación realizar una copia de seguridad, para ser utilizada en caso de que el medio se averíe.

Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

El Área de Tecnología o Sistemas será la única dependencia autorizada para realizar copia de seguridad del software original.

La instalación del software en las máquinas de la Corporación, se realizará únicamente a través del Área de Tecnología o Sistemas

Los programas de software proporcionados por la Corporación Medica Clínica Vida no puede ser copiado o suministrado a terceros.

Para la adquisición y actualización de software, es necesario efectuar la solicitud al Área de Tecnología o con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.

El software que se adquiera a través de los proyectos o programas, debe quedar a nombre de la Corporación Medica Clínica Vida.

Se encuentra prohibido el uso e instalación de juegos en los computadores de la Corporación Medica Clínica Vida.

La información producto de las pruebas de software, será protegida igual que los demás activo de información de la Corporación.

Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.

Políticas de Seguridad En Relación Con Suministradores.

Objetivo.

Asegurar la protección de los activos de información de la Corporación que sean accesibles a los proveedores, manteniendo el nivel de seguridad y la correcta prestación de servicio por parte de los proveedores.

Se deben establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Corporación Medica Clínica Vida. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de Seguridad Informática y de Sistemas antes de firmar el contrato de outsourcing.

Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.

Si la información intercambiada lo amerita, se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el outsourcing de acuerdo al objetivo y al alcance del contrato; el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos de la entidad.

El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.

Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatará las responsabilidades que devengan de la utilización del mismo.

Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de la Corporación, además de los requisitos expuestos en su contrato/convenio con la Corporación.

Políticas de Seguridad para la Gestión de incidentes en la seguridad de la información.

Objetivo.

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación y los responsables de atender los eventos o debilidades en materia de seguridad.

Los eventos e incidentes de seguridad que se presenten serán responsabilidad del Área de Sistemas, quienes deberán atenderlos, recopilar evidencias y documentar los mismos.

El Área de Sistemas debe asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas.

El Área de Sistemas tendrá la responsabilidad, de priorizar una situación de la otra en cuanto a incidentes de seguridad o problemas en las estaciones de trabajo.

Semanalmente los administradores o Área de Sistemas, verificarán la correcta ejecución de los procesos de Backup, suministrarán las copias de seguridad requeridas para cada trabajo y controlarán la vida útil de cada copia de seguridad o medio empleado.

La Corporación debe contar con respaldos de la información ante cualquier incidente, estos respaldos de información deberán ser almacenados en un sitio aislado y libre de cualquier daño o posible extracción por terceros dentro de la Corporación y se utilizarán únicamente en casos especiales ya que su contenido es de suma importancia para la Corporación.

Se prioriza la información de mayor importancia para la Corporación y se evacuará la información o activo basándose en los niveles confidenciales de la Corporación.

El Área de Sistemas tendrá la responsabilidad de llevar un registro manual de todos los incidentes de seguridad que se presenten en la corporación y las actividades sospechosas de los empleados.

Políticas de Seguridad En Aspectos de seguridad de la información en la Gestión de la continuidad del negocio.

Objetivo.

Asegurar la disponibilidad de las instalaciones de procesamiento de información y la inclusión de la seguridad en los sistemas de gestión de continuidad de negocio en la Corporación Médica.

La Corporación Medica Clínica Vida deberá contar con un conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la Corporación, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo ante una contingencia.

La Corporación Medica Clínica Vida deberá prevenir interrupciones en las actividades de la plataforma informática del Corporación que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de la Corporación podrán ser restaurados dentro de escalas de tiempo razonables.

La Corporación Medica Clínica Vida deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta la Identificación y asignación de prioridades a los procesos críticos de TI de la Corporación de acuerdo con su impacto en el cumplimiento de la misión de la misma.

Se documentarán las estrategias de continuidad del negocio, un plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente y un plan de pruebas de la estrategia de continuidad del negocio.

La alta dirección de la Corporación Medica Clínica Vida será la responsable de velar por la implantación de las medidas relativas a ésta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

La alta dirección de la Corporación Medica Clínica Vida, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

Se revisará por lo menos una vez cada seis (6) meses revisión de todas las políticas en materia de seguridad de la información para actualizar y/o agregar nuevas políticas que permitan el adecuado uso de las tecnologías de información y los sistemas en la Corporación Médica Clínica Vida.

Políticas de Cumplimiento.

Objetivo.

Evitar violaciones de obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de requisitos de seguridad por parte de la Corporación Médica.

Todo el personal de la entidad queda sujeto al cumplimiento de las normas aquí expuestas, so pena de ser sancionado disciplinaria y/o legalmente, si hubiera lugar a ellas. Las sanciones van desde un llamado de atención hasta la suspensión del cargo, dependiendo de la gravedad de la falta cometida, además de la malicia o perversidad con que se cometa.

La Ley 1273 establece los atentados contra los sistemas de información, afectando la confidencialidad, integridad y disponibilidad de los datos, para lo cual se regirá de acuerdo a esta, o las leyes que la modifiquen para efectos de sanciones legales.

ANEXO 13.

CONTROLES DE SEGURIDAD

Los controles que a continuación se relacionan, fueron elaborados con base en la Tabla A.1. Objetivos de control y controles del ANEXO A de la norma técnica colombiana NTC-ISO/IEC 27001.

Objetivo

Brindar instrucciones para todo aquel que tenga relación directa o indirecta con la Clínica Vida, dando orientaciones de estricto cumplimiento, concientizándolos sobre el correcto uso de los activos de información, equipos, sistemas operativos y sistemas de información y la sensibilidad de los datos manejados por los mismos.

Alcance

Los controles que aquí se documentan, son de cumplimiento obligatoria para todos los funcionarios de la Corporación Médica Clínica Vida, que hagan uso directa o indirectamente de tecnologías de información y comunicaciones o de los activos de la misma. El comité se Seguridad de la Información será el encargado de verificar cumplimiento y revisión periódica de los controles de seguridad, con el fin de realizar los ajustes necesarios que resulten por crecimiento de la Corporación o la aparición de nuevas amenazas.

Controles de Políticas de Seguridad

Objetivo

Brindar apoyo y orientación a la dirección de la Corporación Medica con respecto a la seguridad de la información, y los reglamentos y leyes pertinentes.

Controles

Las políticas de seguridad diseñadas para la corporación Medica Clínica Vida serán publicadas en la intranet de la institución y comunicadas a todos y cada uno de los empleados de la misma, a su vez serán dadas a conocer a todos los actores externos a la clínica en el momento de su vinculación.

El área de Sistemas Se encargará de la publicación de las políticas de seguridad en la intranet de la corporación, de su revisión periódica cada 6 meses y de su modificación o actualización en caso de ser necesario.

Para que los usuarios puedan colaborar con la gestión de la seguridad, se les debe concienciar e informar a fin de que cumplan con las medidas establecidas por la organización en el desempeño habitual de sus funciones.

Es preciso instruir al personal de forma apropiada sobre seguridad y el uso correcto de los sistemas de información y sus recursos, así como sobre la importancia de la seguridad en el tratamiento de los datos en la organización.

Se debe informar a todo el personal de la corporación que vaya a tratar datos del sistema de información sobre las normas de utilización y medidas de seguridad que debe contemplar dicho tratamiento.

El área de recursos humanos validara la revisión periódica de las políticas diseñadas para la corporación y el cumplimiento de las mismas por el personal o empresa contratista que tenga relación con la Corporación Médica.

Controles Para la Organización de la Seguridad de la Información

Objetivo

Gestionar y mantener la seguridad de la información y los servicios de procesamiento dentro de la organización.

Controles

Las actividades de la seguridad de la información deben ser coordinadas por los representantes o directores de todas las dependencias de la Corporación, con los roles y funciones laborales pertinentes.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe validar que la información suministrada por los aspirantes a algún cargo disponible sea verás, antes de que su vinculación definitiva. Además, deberá verificar los antecedentes del personal aspirante al cargo. Antes de la realización de una contratación se explicarán las responsabilidades de seguridad, describiendo de forma clara y precisa el cargo, asíf como los términos y condiciones del contrato, cumplimiento de las

políticas de seguridad del presente documento y can consecuencias que acarrea el incumplimiento de las mismas.

El Departamento legal, en conjunto con Recursos Humanos y la Dirección del Clínica redactarán un documento de confidencialidad; en el que se obliga al empleado a la no divulgación, ni exposición de toda información que incluya datos de uso exclusivo de la organización. Este documento deberá ser firmado por cada uno de los empleados en el momento de la contratación, este documento será archivado junto con su hoja de vida.

Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del organismo. El documento de confidencialidad tendrá vigencia de doce meses adicionales una vez concluida la relación laboral Empleado-Clínica.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la Corporación por parte de cada una de las dependencias, en los procesos que involucre partes externas a la clínica, su acceso deberá ser autorizado por los directores de cada dependencia y el área de sistemas se encargara de la aplicación de los controles adecuados.

El usuario del sistema de información debe ser informado de forma clara y precisa acerca de sus funciones y obligaciones en el tratamiento de los datos.

Se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores.

Cada proceso debe identificar a un propietario, un depositario y a los usuarios que participarán en el mismo. de esta forma se evitarán malentendidos acerca de las responsabilidades sobre los elementos del sistema de información.

Todas las funciones y responsabilidades deben comunicarse a los usuarios involucrados en su ejecución, de una forma clara y asegurando su recepción y entendimiento. Dichas funciones y obligaciones de cada una de las personas estarán claramente definidas y documentadas.

Las funciones de seguridad y las responsabilidades de los empleados, contratistas y usuarios terceros, deben estar definidas y documentadas conforme a la política de seguridad de la información de la organización.

Además de la información de qué datos tratar y de qué forma, todo usuario debe recibir información acerca de la obligación de mantener secreto profesional sobre los datos que conozca en el desarrollo de sus funciones, aún después de finalizar la relación laboral que le une a la organización.

Cuando un empleado cese sus funciones o cambie de funciones dentro de la organización, está obligado a cumplir con el acuerdo de confidencialidad; es decir a la no divulgación de la información.

Se deben definir exigencias de confidencialidad y no divulgación de datos para todo el personal que dispone de acceso al sistema de información para el desarrollo de sus funciones, tanto para el personal contratado como para el personal externo. Estas exigencias se definirán formalmente en acuerdos de confidencialidad, que todo el personal deberá firmar como prueba de su recepción.

Controles de Gestión de Activos

Objetivo

Lograr y mantener la protección adecuada de los activos de la Corporación, además, mantener actualizados los registros de inventario.

Controles

El Área de Almacén deberá implementar el proceso de etiquetado y clasificación de los activos de la Corporación, permitiendo su clara identificación, además de mantener actualizado, protegido y disponible el inventario de los activos de la Clínica siempre que la Dirección de la Corporación lo requiera.

En el momento de la vinculación o asignación de activos en la Corporación el Área de almacén y Recursos Humanos entregaran a la persona o empresa contratada un formato que deberá firmar donde recibe el activo y se compromete a devolverlo en buen estado en el momento de retiro, cese de actividades, traslado o cuando la corporación lo requiera.

El control de inventario de activos se realizará cada seis meses, en el cual cada empleado deberá confirmar los activos asignados al inicio de sus funciones, dicho control será realizado por el Área de almacén y al apoyo del Área de Sistemas.

El jefe del Área de inventario planificará el control de activos presentando un cronograma, proponiendo la fecha para el inicio del mismo, cronograma que deberá ser aprobado para la ejecución del mismo por parte de la Junta Directiva de la Corporación. Los formularios del control de inventario serán comparados con los registros actuales.

Cada jefe de área y persona con activo asignado, deberá proporcionar toda información sobre los activos a su cargo desde el inicio y de los que se les ha sido entregado durante el periodo de desempeño de sus funciones.

En caso de existir diferencia de información, se deberá presentar los respaldos de las asignaciones de inventario, los mismos que deberán registrar las firmas del empleado.

Cuando un empleado sea retirado o promovido de su cargo, deberá devolver todos los activos que se le asignaron en el momento de su contratación o durante el desempeño de sus funciones en perfecto estado, ya sean estas a nivel médico o administrativo.

Todos los activos de las diferentes áreas deberán ser devueltos en perfecto estado, ya sean estas a nivel médico o administrativo.

Si existe algún activo que no pertenezca al organismo este será revisado para verificar si tiene información relevante para la organización, si es así, esta será entregada al organismo.

Los empleados deberán llenar un formulario de devolución de activos entregado por el departamento de inventario en el cual indicaran todos los activos que el organismo les entrego; a su vez indicaran los activos propios del empleado, que utilizó en el organismo durante su función.

Una vez declarados los activos estos serán entregados y revisados para ver su buen estado, si el activo tiene algún daño se evaluará su reparación o reposición del mismo.

Si el activo del empleado contiene información relevante para el organismo esta deberá ser entregada y eliminada del activo del empleado. Si todos los

procesos anteriores se llevaron a cabo el empleado firmará el formulario de devolución de activos dejando constancia de dicho proceso.

Controles de los Recursos Humanos

Objetivo

Asegurar que los empleados, contratistas y usuarios por tercera parte entiendan sus responsabilidades y son adecuados para los roles para los que se les considera, reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones, y que estén conscientes de las amenazas y preocupaciones de seguridad de la información, sus responsabilidades y sus deberes y que estén equipados para apoyar las políticas de seguridad durante el desarrollo de sus funciones.

Controles

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana y el Área Jurídica, deben asegurar que los funcionarios, contratistas y demás colaboradores de la Corporación Médica Clínica Vida, entiendan sus responsabilidades y las funciones de sus roles.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe validar que la información suministrada por los aspirantes a algún cargo disponible sea verás, antes de que su vinculación definitiva. Además, deberá verificar los antecedentes disciplinarios con la Contraloría General de la Nación, Procuraduría y antecedentes de Policía. También el Área de recursos Humanos deberá validar la información académica del personal aspirante al cargo, con el fin de determinar si su perfil se ajusta al requerido por la Corporación.

Como parte de su obligación contractual, los empleados, contratistas y terceras partes deberán estar de acuerdo con los términos, condiciones del contrato que los vincula con la Corporación Médica y responsabilidades con relación a la seguridad de la información. Los contratos serán redactados por el Área Jurídica y revisados por la Junta Directiva de la Clínica.

El jefe de la División Administrativa o quien realice las funciones de Gestión Humana, debe desarrollar un programa de concientización sobre protección de la información para todo el personal. Todo el personal deberá asistir a los cursos que se impartan dentro del programa de concientización, aplicando

los conocimientos adquiridos en sus puestos de trabajo. Este programa deberá ser aprobado por la Junta Directiva de la Corporación.

El Área Jurídica iniciara proceso disciplinario formal para el personal que cometa alguna violación de seguridad y tomará las medidas necesarias basadas en las políticas de la clínica, teniendo autoridad de tomar las medidas que apliquen y de ser necesario finalizar el contrato laboral con el funcionario o contratista e iniciar proceso legal basándose en las leyes que rigen para Colombia.

Al momento de la finalización su contrato u orden de trabajo todos los empleados contratistas o terceras partes deberán devolver los activos asignados por la Corporación que se encuentren en su poder. El área de Almacén entregara una paz y salvo para poder iniciar el proceso de liquidación de elementos a los que tenga derecho y su posterior pago por parte del Área Financiera.

El área de Recursos Humanos notificara al Área de Sistemas cuando un funcionario sea desvinculado o cambiado de su cargo, para que ésta suspenda o modifique los permisos de acceso que tenga el usuario en todos los sistemas de procesamiento de información de la Corporación.

Controles de Seguridad Física del Entrono

Objetivo

Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información, y evitar perdida, daño o puesta en peligro los activos y la interrupción de las actividades de la Corporación Médica.

Controles

Se deberán proteger las áreas seguras del Corporación Médica mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado. Se deberán diseñar y aplicar controles de seguridad físicos en las oficinas, habitaciones de la Clínica, El personal de seguridad verificara el ingreso de las personas en los dos bloques de la Corporación, previniendo el ingreso de armas de fuego, explosivos o cualquier elemento que pueda poner en riesgo las instalaciones de la Corporación o pérdida de activos de la misma.

El área de mantenimiento deberá garantizar el correcto funcionamiento de las cámaras de seguridad, las puertas en cada una de las dependencias y consultorios, así como sus chapas o cerraduras. para apoyar las labores del personal de seguridad en aras de conservar la integridad de las instalaciones de la corporación.

La Dirección de la Clínica deberá gestionar la instalación de elementos de seguridad como extintores de fuego y detectores de humo en las instalaciones de la Corporación y brindar las herramientas necesarias para que el área de mantenimiento instale la respectiva señalización de las diferentes zonas de la corporación entre ellas la salida de emergencias.

Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el administrador y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

La zona de carga ubicada en el bloque administrativo deberá ser controlada por el personal de seguridad de la clínica, evitando el ingreso de personal no autorizado y las labores de terceros como la recolección de residuos o descargue de insumos.

Es totalmente prohibido a los usuarios o terceros, salvo autorización o supervisión expresa de Área de Sistemas, la intervención física o retiro de los recursos de la red de la Corporación (cables, enlaces, estaciones de trabajo, dispositivos de red). Solo el personal autorizado es el encargado exclusivo de intervenir físicamente los recursos de la red de la Clínica.

El cableado eléctrico y de las telecomunicaciones que sostienen los servicios de información de la Clínica deberán ser protegidos mediante tubería, canaleta u otros controles. Los equipos electrónicos críticos deberán ser protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios eléctricos o de telecomunicaciones. El área de mantenimiento verificara periódicamente el correcto funcionamiento de las UPS y del cableado, de ser necesario solicitara apoyo del personal de Sistemas. Las revisiones periódicas deberán quedar registradas en una bitácora que será revisada por el Comité de Seguridad de la Información.

La salida de equipos de equipos de las instalaciones de la corporación debe ser autorizada únicamente por el personal de Sistemas o Almacén de manera escrita, en el momento de la salida el personal de seguridad requerirá dicha orden para poder permitir la salida de cualquier activo. El

área de Sistemas deberá proporcionar las medidas para verificar todos los elementos del equipo que contengan información sensible de la Corporación.

Controles de Gestión de Comunicaciones y Operaciones

Objetivo

Asegurar la operación correcta y segura de los servicios de procesamiento de información manteniendo la integridad y disponibilidad de la información, mantener un grado de seguridad en la prestación de los servicios y minimizar el riesgo de fallas de los sistemas, asegurar la protección de la información en las redes y las infraestructuras de soporte y evitar la divulgación, modificación, retiro o destrucción de activos no autorizada en la Corporación Médica.

Controles

Los procedimientos de operación de la Corporación y los cambios en los servicios y Sistemas de procesamiento de la corporación deberán ser documentados y comunicados s todos los funcionarios de la corporación, el Área de Sistemas se encargará de su publicación y difusión a todo aquel que lo requiera.

Las funciones y las áreas de responsabilidad de la Corporación deberán ser distribuidas para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.

El Área de control interno se encargará de monitorear y revisar el complimiento de compromisos en la prestación del servicio brindados por terceras partes, la gestión de los cambios en los servicios por terceras partes incluyendo mantenimiento y mejora de las políticas existentes de seguridad, así como la reevaluación de los riesgos.

El Área de Sistemas debe implementar controles idóneos de detección, prevención y recuperación para proteger los sistemas de información de la Corporación, como instalación y actualización de antivirus contra códigos maliciosos, asíí como procedimientos apropiados de concientización de los usuarios.

El Área de Sistemas debe establecer y revisar periódicamente políticas de respaldo de información, realizar las respectivas copias de seguridad de la información y del software de la corporación, además de realizar pruebas periódicas de los Backup.

La Gerencia de la corporación Deberá adelantar las gestiones para la adquisición de un sistema de detección de intrusos (IDS) que permita mitigar los riesgos en los servicios de red, el IDS será administrado por el Área de Sistemas.

El Área de Sistemas deberá establecer procedimientos para la gestión de los medios removibles, cuando ya no se requieran, su eliminación deberá hacerse aplicando procedimientos formales para tal fin, como la sobre escritura reiterada.

La documentación del sistema será almacenada en los servidores de la Corporación, el único autorizado para su acceso será el encargado del Área de Sistemas.

Es responsabilidad del Área de Sistemas la puesta en funcionamiento del servidor de correo para la corporación, así como la implementación de medidas que protección de la mensajería electrónica de la Corporación.

El comité de seguridad deberá verificar la aplicación de medidas de seguridad en los procedimientos de intercambio de información. Establecer las políticas y controles que permitan proteger la información asociada con la interconexión de los sistemas de información.

El comité de seguridad deberá evaluar periódicamente la eficacia de los controles de acceso con el objetivo de evitar la modificación no autorizada de información disponible al público.

El Comité de Seguridad con el apoyo del Área de control interno deberá planificar el diseño y aplicación de las auditorias en la Corporación, además deberá responder por su ejecución y registro.

Las fallas que se presenten en los sistemas de la Corporación, serán atendidas por el comité de Gestión de Incidentes, dicho comité deberá registrar, analizar, tomar las medidas adecuadas, en incluirlas en la bitácora para ser tenidas en cuenta en el momento de actualizar los controles o políticas de seguridad.

El Área de Sistemas será la encargada mantener actualizados todos los relojes de los sistemas de la Corporación con una fuente de tiempo confiable.

Controles de Acceso

Objetivo

Controlar el acceso no autorizado a la información de los servicios de procesamiento de información, servicios en red, sistemas operativos y sistemas de información de la Corporación.

Controles

La Alta Gerencia de la Corporación deberá brindar las herramientas necesarias que permitan establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio.

El Área de sistemas será la única autorizada para el registro de usuarios en los sistemas de información de la Corporación, periódicamente gestionará los privilegios de los usuarios, gestionará las contraseñas para los usuarios y revisará sus derechos de acceso. El comité de seguridad de la información Validara el cumplimiento es este control.

Es responsabilidad del Área de Sistemas exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y uso de contraseñas, equipos desatendidos y políticas de escritorio despejado.

La entrega de las credenciales al usuario (nombre de usuario y contraseña) debe realizarse por algún procedimiento que obligue al usuario a cambiar la contraseña en el siguiente inicio de sesión, lo que garantiza que solamente él conoce la contraseña. El oficial de seguridad deberá validar periódicamente que los usuarios solo tengan acceso a los servicios a los cuales tiene autorización.

El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado será responsabilidad única y exclusiva del área de Sistema al igual que la segmentación y administración de la red. la responsabilidad de la gestión de las contraseñas, es única y exclusiva del Área de Seguridad.

El área de sistemas deberá asignar a cada usuario un identificador único y personal con el cual podrá loguearse en la plataforma de la Corporación y

con el cual se podrá hacer seguimiento de sus actividades en el Sistema de Información.

El Área de Sistemas deberá controlar que ningún usuario instale software que puedan anular los controles de seguridad de los sistemas de información o de las aplicaciones. También deberá realizar las configuraciones correspondientes para suspender las sesiones e inactivas y restringir los periodos de conexión en aplicaciones de alto riesgo en la corporación.

Los usuarios encargados de brindar soporte no podrán tener acceso a la información ni a las funciones del sistema de aplicaciones, el oficial de seguridad deberá legitimar el cumplimiento de este control.

Controles de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Objetivo

Garantizar que la seguridad es parte integral de los sistemas de información, protegiendo la confidencialidad, autenticidad o integridad de la información de la Corporación por medios criptográficos, manteniendo la seguridad de los programas de software y de la información del sistema de aplicaciones y reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.

Controles

El Comité de Seguridad de la Información realizara el análisis y especificara los requisitos de seguridad para los nuevos sistemas de información o mejora de los existentes.

Pese a que el Sistema de Información de la Corporación realiza una validación de los datos de entrada y efectúa control de procesamiento interno de los datos, el Área de Sistemas certificara periódicamente la validación de los datos de entrada.

Aun cuando el Sistema de Información de la Corporación realiza cifrado de la información, el Área de Sistemas deberá blindar la transmisión de la información con la implementación de medidas eficaces como VPN o las que apliquen.

El Área de Sistemas debe controlar que bajo ninguna circunstancia los usuarios instalen software en los sistemas operativos de los equipos de la Corporación, la instalación de software está permitida únicamente por parte de esta Área, el usuario que desee instalar algún software deberá pedir Autorización Al Comité de Seguridad.

Controles de Gestión de Incidentes de la Seguridad de la Información

Objetivo

Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente, y se aplique un enfoque consistente y eficaz.

Controles

Es obligación de todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información de la Corporación informar al Comité de Atención de Incidentes de Seguridad sobre cualquier incidente de seguridad de la información o debilidad de la seguridad que se presente.

El comité de atención de incidentes de seguridad es el único responsable de atender los incidentes de seguridad o debilidades de seguridad y recolectar la evidencia necesaria, los lineamientos de atención, antes y después del incidente, están descritos en sus funciones.

Controles de Gestión de la Continuidad del Negocio

Objetivo

Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

Controles

El comité de seguridad de la información debe identificar los eventos que pueden ocasionar interrupciones en los procesos de la Corporación, así como sus consecuencias para la seguridad de la Información.

Los planes de contingencia para mantener o recuperar las operaciones y asegurar la disponibilidad de la información después de una interrupción o falla de los procesos son responsabilidad del Comité de atención a incidentes de seguridad.

La alta Gerencia debe estar comprometida con los planes de continuidad del negocio, deberá brindar las herramientas necesarias para someterlos a pruebas periódicas que permitan su actualización y la validación de su eficacia.

La alta gerencia dará los lineamientos para desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización, el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Controles de Cumplimiento

Objetivo

Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

Controles

Es responsabilidad del Área Jurídica identificar los requisitos estatutarios y de legislación aplicable a la Corporación, verificar el cumplimiento de requisitos legales, reglamentarios y contractuales sobre el cual pueda existir derechos de propiedad intelectual.

El Área de Talento Humano será responsable de monitorear que los activos de la corporación sean utilizados exclusivamente para propósitos laborales.

Los encargados de cada Área serán los encargados de garantizar que los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para el cumplimiento de las políticas de seguridad.

El comité de seguridad de la información debe verificar periódicamente los sistemas de información de la Corporación y determinara si cumple con las normas de implementación de seguridad.

El comité de seguridad de la información debe planificar y acordar cuidadosamente los requisitos y actividades de las auditorias en la

Corporación con el propósito de minimizar al máximo el riesgo de interrupción del servicio. Además, deberá proteger el acceso a las herramientas de auditoria de los sistemas de información de personal no autorizado.

ANEXO 15.

GOBIERNO DEL SISTEMA DE GESTIÓN

Gobierno del Sistema de Gestión

Comité de Seguridad de la Información

El comité de Seguridad de la Información para la Corporación Médica Clínica Vida de la ciudad de Quibdó estará conformado de la siguiente manera:

- Oficial de Seguridad de la información
- Director General Administrativo
- Responsable de Talento Humano
- Responsable del Área de infraestructura
- Responsable de Auditoria Interna
- Responsable de Jurídico
- Responsable de Seguridad

Objetivos del Comité de Seguridad

Asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en la Corporación, así como de la formulación y mantenimiento de una política y controles de seguridad de la información a través de todo el organismo.

Funciones del Comité.

El Comité de Seguridad de la Información de la Corporación Médica Clínica Vida tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la Corporación.

2. Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la Corporación.

3. Acompañar e impulsar el desarrollo de proyectos de seguridad.

4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Corporación.

5. Recomendar roles y responsabilidades específicas que se relacionen con la seguridad de la información.

6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

9. Promover la difusión y sensibilización de la seguridad de la información dentro de la Corporación.

10. Poner en conocimiento a la Gerencia de la Corporación, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

11. Las demás funciones inherentes a la naturaleza del Comité.

Comité de Gestión de Incidentes

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la Corporación y sus integrantes serán designados por la gerencia de la misma.

Esta guía de gestión de incidentes de seguridad de la información plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad en la Corporación Médica Clínica Vida, quienes se encargarán de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargarán de:

Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.

Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.

Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.

Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).

Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.

Certificación de productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.

Configuración y Administración de Dispositivos de Seguridad: Se encargarán de la administración adecuada de los elementos de seguridad informática.

Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

Investigación y Desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Declaración y Notificación de Incidentes

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la Corporación.

La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y

eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

A continuación, se describe un proceso de notificación de incidentes de seguridad que podría ser adoptado por la Corporación:

Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por la Corporación. El incidente puede ser notificado a través de cualquier canal de comunicación (Telefónico, Correo, Aplicativo) es importante resaltar que debe existir un formato el cual el usuario que reporta el incidente debe diligenciar con la mayor cantidad posible de información relacionada con el incidente.

El primer punto de contacto identificará el tipo de incidente analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de Tecnologías de la Información. En caso de ser catalogado como un incidente de seguridad se notificarán a la persona encargada de la atención de incidentes o a quien haga sus veces para que tome las decisiones correspondientes.

El primer punto de contacto será el encargado de realizar el seguimiento del incidente hasta su cierre definitivo.

Si el incidente de seguridad es identificado por otra línea diferente a un usuario de la Corporación, a través de los elementos de detección o administradores de Tecnologías de la Información, este es notificado directamente a la persona encargada de atención de incidentes quien tomará las acciones necesarias de atención. Se notificará al primer punto de contacto sobre la presentación de un incidente de seguridad para que realice la documentación respectiva y esté atento al seguimiento y desarrollo del mismo.

El punto de contacto clave dentro de la gestión de incidentes es la persona encargada de la atención de los mismos, el cual se encarga de coordinar y asignar las actividades con las partes interesadas. Estos últimos se encargan de solicitar el apoyo a las personas involucradas con el proceso con el fin de la correcta ejecución de actividades que den solución al incidente.

La persona encargada de la atención de incidentes tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad y es la persona que notificará a las altas directivas de la entidad.

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias. (MinTic)