RESUMEN - TESIS DE GRADO

AUTORES	**JHON JAIRO VARGAS LASCARRO** **YAQUELINE MANDÓN CASTRO** **GUILLERMO GERARDINO SÁNCHEZ**
FACULTAD	**DE INGENIERÍAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**Magister ADRIANA MOSQUERA CARRASCAL**
TÍTULO DE LA TESIS	**DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LOS REGISTROS DE LOS USUARIOS DE LA BIBLIOTECA CHAID NEME, BASADO EN LA NORMA NTC-ISO-IEC 27001:2013**

RESUMEN
(70 palabras aproximadamente)

EN LA ACTUALIDAD, LA INFORMACIÓN ES CONSIDERADA COMO UN ELEMENTO PRIMORDIAL EN CUALQUIER TIPO DE ORGANIZACIÓN, INDEPENDIENTE DE SU TIPO O ACTIVIDAD COMERCIAL, SIN IMPORTAR SU TAMAÑO Y NATURALEZA, SE ENCUENTRAN VINCULADAS DE ALGUNA MANERA CON LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC) Y CUENTAN CON LOS RECURSOS ADECUADOS PARA SU SOSTENIMIENTO. SIN EMBARGO, LOS RESPONSABLES DENTRO DE LAS ORGANIZACIONES NO SON CONSCIENTES DE LOS RIESGOS Y AMENAZAS QUE EXISTEN EN EL CIBERESPACIO

CARACTERÍSTICAS

PÁGINAS: 186	PLANOS:	ILUSTRACIONES: 0	CD-ROM: 1

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LOS REGISTROS DE LOS USUARIOS DE LA BIBLIOTECA CHAID NEME, BASADO EN LA NORMA NTC-ISO-IEC 27001:2013

AUTORES:

JHON JAIRO VARGAS LASCARRO

YAQUELINE MANDÓN CASTRO

GUILLERMO GERARDINO SÁNCHEZ

Director

Magister ADRIANA MOSQUERA CARRASCAL

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

Ocaña, Colombia **Agosto de 2017**

Índice

Capítulo 1. Diseño de un sistema de gestión de seguridad de la información de los registros de los usuarios de la biblioteca Chaid Neme, basado en la norma NTC-ISO-IEC 27001:2013.....1
1.1 Planteamiento del problema 1
1.2 Formulación del problema.....3
1.3 Objetivos 3
1.3.1 Objetivo general.....3
1.3.2 Objetivos específicos.....3
1.4 Delimitaciones 6
1.4.1 Conceptual.....6
1.4.2 Geográfica. 6
1.4.3 Temporal.....6
1.4.4 Operativa 6

Capítulo 2. Marco referencial 8
2.1 Marco histórico 8
2.2 Marco teórico.....10
2.3 Marco conceptual.....14
2.4 Marco legal 19

Capitulo 3. Diseño metodologico 26
3.1 Tipo de investigacion 26
3.2 Población y muestra 26
3.3 Técnicas e instrumentos de recolección de datos 27
3.4 Informe de auditoria.....28

Capítulo 4. Resultados.....29
4.1 Realizar un diagnóstico para identificar las vulnerabilidades y amenazas de seguridad de información de los servicios y procesos de la Biblioteca recolectando la información interna y externa, por medio de los procesos descritos en la norma NTC-ISO/IEC 2001:2013. 29
4.2 Establecer las políticas, procesos y procedimientos de seguridad necesarios para mitigar los riesgos y mejorar la seguridad de la información de la Biblioteca. 53
4.3 Aplicar los controles de la norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información. 130

5. Conclusiones 152

6. Recomendaciones.....154

Referencias 156

Apéndices 162

Lista de tablas

Tabla 1. Situaciones encontradas.....31

Tabla 2. Situaciones relevantes.....35

Tabla 3. Planear 40

Tabla 4. Hacer.....42

Tabla 5. Verificar y actuar.....51

Tabla 6. Diagnóstico consolidado.....53

Lista de apéndices

Apéndice A. Entrevista.....163

Apéndice B. Encuesta 164

Apéndice C. Modelo lista de chequeo.....166

Apéndice D. Modelo lista de verificación. 167

Apéndice E. Políticas de seguridad.....168

Capítulo 1. Diseño de un sistema de gestión de seguridad de la información de los registros de los usuarios de la biblioteca Chaid Neme, basado en la norma NTC-ISO-IEC 27001:2013

1.1 Planteamiento del problema

En la actualidad, la información es considerada como un elemento primordial en cualquier tipo de organización, independiente de su tipo o actividad comercial, sin importar su tamaño y naturaleza, se encuentran vinculadas de alguna manera con las Tecnologías de Información y Comunicación (TIC) y cuentan con los recursos adecuados para su sostenimiento. Sin embargo, los responsables dentro de las organizaciones no son conscientes de los riesgos y amenazas que existen en el ciberespacio, un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar la información; conllevando a que no incluyan un presupuesto adecuado para implementar seguridad de la información en la empresa. (Naya De Vita Montiel, 2008)

Las entidades deben mantener una adecuada gestión de sus activos de información con la finalidad de asegurar y controlar su debido acceso, tratamiento y uso; por lo que, cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones. El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial. (Iso 27001, 2012)

En la Biblioteca Chaid Neme de la Ciudad de Ocaña, se ha implementado servicios informáticos con el fin de mejorar sus procesos, procedimientos y ofrecer una mejor atención a la comunidad estudiantil, pero se observa la poca importancia dada a la seguridad informática para proteger los activos de información existentes. En esta dependencia, no se garantiza la confidencialidad, disponibilidad en integridad de dicha información, pues no se manejan adecuadamente los controles relacionados con la seguridad de la información que manejan, desde el punto de vista del factor tecnológico así como el del factor humano que trabaja en ella. Cada una de las plataformas implementadas deben contemplar los riesgos en el control de información siguiendo un plan donde se reevalúen, auditen y apliquen políticas de control.

Es así que esta dependencia, objeto del presente trabajo, aún no cuenta con un sistema de seguridad que le permita mantener a salvo su principal activo, la información, tomando como referente sistemas de seguridad habituales que no siempre garantizan resultados efectivos, puesto que no cuentan con un profesional a cargo, así mismo los usuarios no cuentan con la capacitación, conocimiento y responsabilidad al momento de interactuar con la base de datos, permitiendo accesos a personal ajeno a la institución y no autorizado, divulgación de contraseñas, sistema de autenticación débil, entre otros problemas.

Estos riegos a corto o mediano plazo pueden desembocar en pérdida, alteración o lectura no permitida de esa información y provocar una serie de eventos desfavorables en todo lo relacionado al manejo de la información y por tal motivo, la estabilidad institucional.

De seguir con esta falta de seguridad en el manejo de la información, la Biblioteca detendrá sus servicios en cualquier momento, conllevando a un mal servicio a sus estudiantes, docentes, empleados y comunidad en general, haciendo más lentos sus procesos ocasionando una mala imagen y robo o pérdida de información de carácter privado, sumado a un gasto financiero al aplicar planes correctivos, lo cual puede incidir en graves pérdidas económicas y de información.

1.2 Formulación del problema

¿Qué estrategia se debe plantear para soportar la seguridad de la información en los procesos de la biblioteca Chaid Neme de la ciudad de Ocaña?

1.3 Objetivos

1.3.1 Objetivo general. Diseñar un sistema de gestión de seguridad de la información, basado en la norma NTC-ISO-IEC 27001:2013, para la Biblioteca Chaid Neme de la Ciudad de Ocaña.

1.3.2 Objetivos específicos. Realizar un diagnóstico para identificar las vulnerabilidades y amenazas de seguridad de información de los servicios y procesos de la Biblioteca recolectando la información interna y externa, por medio de los procesos descritos en la norma NTC-ISO/IEC 27001:2013.

Formalizar el sistema de seguridad mediante la documentación de las políticas, programas y procedimientos establecidos para gestionar los riesgos de seguridad de información de la dependencia.

Aplicar los controles de la norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información.

Justificación

La continua evolución, crecimiento y sofisticación de la tecnología, al igual que los ataques cibernéticos en las organizaciones, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger a la compañía ante las amenazas a los activos informáticos (Ministerio, 2016). Una empresa bien estructurada garantiza una prolongada continuidad en un entorno cambiante y riesgoso, razón por la cual debe integrar cada uno de los detalles que se convierten en insumos para sus procesos misionales. Dentro de dichos insumos se encuentra la información, que consiste en uno de los cimientos sobre los cuales se estructura toda organización. Sin embargo, se encuentra expuesta a riesgos en su seguridad; por tal motivo, las empresas actuales se preocupan por mitigarlos y evitar que pongan en peligro su normal funcionamiento.

La Universidad Francisco de Paula Santander fomenta la calidad de sus procesos académicos y de gestión institucional, donde la biblioteca Chaid Neme es un ente crítico en pro

de la operación normal de los procesos académicos administrativos, velando por el funcionamiento eficiente su información, siendo clasificada, correcta y disponible. Por tal motivo se hace necesario establecer políticas y objetivos de seguridad adecuados por medio de un sistema de gestión que las coordine e integre efectivamente.

De igual forma, la biblioteca, como dependencia de la ciudad de Ocaña, día a día se preocupa por implementar mejores prácticas que le permitan fortalecerse, y disminuir las amenazas y debilidades identificadas en el planteamiento del problema; contemplando diversas herramientas que sirvan de orientación generando un importante compromiso con la seguridad de la información, permitiendo grandes alcances en ella.

Así mismo, cabe resaltar que por medio de este proyecto se pretende entregar una herramienta apropiada para que cada uno de los funcionarios activos de la dependencia, reconozcan la importancia de resguardar la información, contribuyendo al desempeño de sus labores de una manera óptima, garantizando la confidencialidad, integridad y disponibilidad de la misma.

En ese orden de ideas, se hace necesario diseñar un sistema de seguridad Informática que permita salvaguardar los recursos informáticos de la biblioteca de la universidad, procurando a la dependencia a cumplir sus objetivos, con el fin de mejorar las medidas de seguridad que se orienten a prevenir y/o detectar cada uno de los riesgos que comprometan la disponibilidad, integridad y confidencialidad de la información a través de los cuales se gestiona la información

de la biblioteca, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

1.4 Delimitaciones

1.4.1 Conceptual. Los elementos que se tendrán en cuenta para construir el marco conceptual de la presente investigación se relacionan a continuación: Seguridad de la Información, Sistema de Gestión de Seguridad de la Información (SGSI),

1.4.2 Geográfica. El proyecto se adelantará en la ciudad de Ocaña en Norte de Santander

1.4.3 Temporal. El tiempo estimado para la realización de dicho proyecto será de cuatro semanas, contados a partir de la aprobación del anteproyecto.

1.4.4 Operativa. Para cumplir efectivamente las metas propuestas y dar la atención a los riesgos presentados, se prevén las siguientes situaciones:

Complemento de bibliografía, debido a insuficiencia de fuentes citadas en este documento.

Insuficiencia de las técnicas de recolección de información propuestas en este anteproyecto, por lo que en caso de requerirse se adicionarán, reformarán o suprimirán interrogantes, así como adición de nuevas técnicas, ya sean encuestas, entrevistas o pautas de observación.

Durante la realización del presente trabajo de investigación, se aplicarán entrevistas a las personas afectadas por la problemática planteada; para lo cual se hará necesario solventar las dificultades presentadas durante el transcurso de la investigación como la carencia de tiempo para desarrollar todas las actividades pertinentes dentro del calendario fijado, entre otras.

Cabe recalcar que el trabajo se desarrollará de acuerdo a lo estipulado en el anteproyecto. De surgir en el desarrollo del mismo los cambios significativos serán consultados y realizados en acción conjunta con el director del proyecto y comunicados mediante oficios al Comité Curricular**.**

Capítulo 2. Marco referencial

2.1 Marco histórico

La seguridad ha existido desde los anales de la historia y su evolución ha ido ligada de una manera u otra a la del ser humano en todo su ámbito de actuación.

En la antigüedad el hombre se enfrentaba a diversos peligros que ponían en riesgo su supervivencia, de tal forma que centró sus esfuerzos en poner todos los medios necesarios para salvaguardarla. Debido a ello generó herramientas de protección ante los peligros que le acechaban, principalmente peligros naturales, como fuego, inundaciones, ataques de animales, entre otros, dando lugar a las primeras armas para protegerse, creadas con elementos naturales como piedras o madera. De forma natural estaba desarrollando la primera seguridad: la física. (Aucal, 2015)

Esta preocupación inicial de preservar la vida, se convirtió en una necesidad obligatoria para salvaguardar la especia y evitar su extinción. Desde este momento el ser humano se ha enfrentado a toda clase de amenazas durante su largo camino en busca de la seguridad.
Hoy en día el objetivo de la seguridad ha evolucionado, dejando atrás el único objetivo de preservar la especie humana y diversificándolo buscando otros orientados a la seguridad en diferentes ámbitos. De la misma forma que los objetivos de la seguridad han ido evolucionando, la evolución de la seguridad en las empresas no ha quedado atrás y ha experimentado un cambio

sustancial desde sus inicios, principalmente motivado por los avances tecnológicos a los que se ha visto expuesta. (Aucal, 2015)

En la década de los 70, la seguridad en las empresas estaba centrada en garantizar el buen uso de la información por parte de los empleados confiando en el sentido común para garantizar la seguridad de la organización. Sin embargo y debido a la inclusión y evolución de la tecnología, aparecieron nuevos riesgos que hicieron que esta "seguridad" quedara obsoleta. Uno de los principales motivos por los que el avance de la tecnología propulsó un cambio en la tendencia de seguridad de las empresas vino motivado principalmente por los virus que se convirtieron en los principales motores de crecimiento para la Seguridad de la Información a nivel mundial debido a la globalidad de sus objetivos (Aucal, 2015)

Existen antecedentes de proyectos relacionados con Sistemas de Gestión de Seguridad de la Información, entre los que cabe destacar:

Sistema de gestión de seguridad de la información para la oficina de control y vigilancia en la corporación autónoma de la frontera nororiental "Corponor" territorial Ocaña. Se propone un sistema de gestión de seguridad de la información para la oficina de control y vigilancia de CORPONOR territorial Ocaña; esta propuesta tiene como fin aportar a la corporación a aumentar la cantidad y calidad de los controles informáticos, a detectar los niveles de madurez tanto de las características físicas como lógicas que dan soporte al proceso y almacenamiento de la información, a dejar sentados los elementos conceptuales y teóricos que les permitirán a las personas que allí trabajan tomar las decisiones adecuadas para utilizar

adecuadamente la tecnología y contribuir a disminuir los niveles de inseguridad de la información de la organización. (Milagros, 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. Mediante un SGSI – Sistema de Gestión de Seguridad de la Información, el Área de Contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar conseguirá minimizar considerablemente el riesgo de que su productividad se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Casadiegos, 2014)

2.2 Marco teórico

Al abarcar contenidos teóricos a la investigación cabe resaltar las teorías en las cuales se ha enfocado a través de los años para realizar un sistema de gestión de seguridad de la información, que se apropiado para alcanzar el éxito deseado y se adapte a las necesidades presentes en la organización que desee implantarlo.

Teoría de la información. La Teoría de la Información nos muestra, entre otras cosas, el camino a seguir para determinar la cantidad de información útil a partir de unos datos. Y para comprimir la información de manera que los datos se representen de una manera eficiente. Nace

de la necesidad de optimizar los contenidos de las informaciones, en una época histórica en la que la comunicación alcanzaba un destacado papel (Shannon, 1948), esto después del nacimiento del código binario (Hartley, 1927) y los primeros pasos de encriptación (Turing, 1936). En consecuencia, se debía encontrar una forma en la cual determinar "la cantidad de información" que entregaba un mensaje.

El mayor investigador de este tema fue Claude Shannon quién aportó el concepto de que la información debe dejar de verse como inmaterial y subjetiva, sino que como perfectamente material y cuantificable. Así pasó a considerarse de una manera independiente un dispositivo de representación y se dio la posibilidad de hablar de procesos de representación y manipulación de la información sin hacer énfasis si era el cerebro o un ordenador quien realizaba dichos procesos. Esto permitió, dar el primer paso para la cibernética: el control de las máquinas para realizar tareas humanas. (Arredondo, 2014)

Definición de información: - Es el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando técnicas criptográficas entre otras herramientas. - La teoría de la información (Ramio Aguirre Jorge, 2006) mide la cantidad de información que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.

Seguridad de la información desde la Teoría de las Limitaciones

El eslabón más débil de la cadena. A cualquier profesional le suena: "La seguridad es como una cadena, es tan fuerte como el eslabón más débil". Esto se dice por varios motivos: Para enfatizar la naturaleza de seguridad como proceso, como sistema, pero también para entender que se trata de una posición de defensa débil, es decir, el defensor tiene que defender todos los puntos, mientras que al atacante le basta con encontrar un punto vulnerable para tener éxito en su ataque. (Ramos A. , 2007)

Sin embargo, aunque se está convencido de que esto es así, muy pocos (por no decir, ninguno) realiza la gestión de este proceso conforme a esta máxima. Porque si se gestionará la seguridad teniendo este paradigma en mente, lo mejor sería emplear la misma estrategia que cualquier otro sistema cuya producción esté gobernada por su factor limitante. Me explico, después de identificarlo, habría que hacer que este factor limitante produjese al máximo nivel. (Ramos A. , 2007)

Esta forma de gestionar la seguridad cambiaría sobremanera el enfoque actual del proceso de gestión. Si se sigue lo establecido en los estándares, por ejemplo, el estándar ISO/IEC 27001 que establece las pautas para montar un Sistema de Gestión de la Seguridad de la Información (SGSI) "certificable", hay que llevar a cabo un análisis de riesgos que nos permita identificar el nivel de riesgo por cada área o dominio del alcance establecido y pasar a gestionar el riesgo en función de la estrategia definida. (Ramos A. , 2007)

Si se plantea la seguridad como un sistema en el que el output fuera el nivel de seguridad de la organización (parece obvio, ¿no?), el máximo nivel estaría marcado por el máximo caudal que pudiera gestionar el cuello de botella del sistema, es decir, el nivel de seguridad de la organización sería el del eslabón más débil de la cadena. (Ramos A. , 2007)

¿Cuál es la diferencia entre estas dos maneras de gestionar la seguridad? la diferencia es que no tendría tanto interés realizar un análisis de riesgos como el hecho de encontrar cuál es el factor limitante, cuál es el eslabón más débil, puesto que sería el que marcaría el nivel de seguridad de nuestra organización. A partir de ahí, si se quiere elevar el nivel de seguridad de nuestra organización, se debería gestionar esa limitación y eso, ya se sabe, hay que preguntarle a Goldratt el cómo. (Ramos, 2007)

Teoría de la seguridad por oscuridad Gaming. Shannon buscó la seguridad contra el atacante con poderes computacionales ilimitados: si la información transmite cierta información, a continuación, el atacante de Shannon seguramente va a extraer esa información. Diffie y Hellman refinaron el modelo atacantes de Shannon al tener en cuenta el hecho de que los atacantes reales son computacionalmente limitados. Esta idea se convirtió en uno de los grandes nuevos paradigmas en ciencias de la computación, y condujo a la criptografía moderna. (Campos, 2011)

Shannon también buscó la seguridad contra el atacante con poderes lógicos y observacionales ilimitadas, expresada a través de la máxima de que "el enemigo conoce el sistema". Este punto de vista todavía es refrendado de la criptografía. La formulación popular,

que se remonta a Kerckhoffs, es que "no hay seguridad por oscuridad", lo que significa que los algoritmos no se pueden mantener ocultos al atacante, y que la seguridad sólo deben confiar en las claves secretas. De hecho, la criptografía moderna va más allá de Shannon o Kerckhoffs en asumir tácitamente que si hay un algoritmo que puede romper el sistema, entonces el atacante seguramente encontrará ese algoritmo. El atacante no es visto como un equipo omnipotente más, pero él todavía se interpreta como un programador omnipotente. (Campos, 2011)

Así que el paso de Diffie-Hellman de ilimitado a potencias computacionales limitados no se ha extendido a un paso de la ilimitada a los limitados poderes lógicos o de programación. Es la hipótesis de que todos los algoritmos factibles finalmente serán descubiertos y aplican realmente diferente de la suposición de que todo lo que es computable el tiempo se puede calcular. Aquí se exploran algunas maneras para refinar los modelos actuales del atacante y del defensor, teniendo en cuenta lo limitado de sus facultades lógicas y programación. Si el atacante adaptativo consulta activo el sistema para buscar a sus vulnerabilidades, el sistema puede ganar un poco de seguridad al aprender activamente los métodos del atacante, y la adaptación a ellos. (Campos, 2011)

2.3 Marco conceptual

La información hoy en día, es uno de los más importantes activos no solo para las empresas y organizaciones, si no para cada individuo. Por este motivo la misma requiere ser asegurada y protegida en forma apropiada. La Seguridad de la Información es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de

minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio. Y en el caso de cada individuo de proteger la identidad y la privacidad. (Compuchannel, 2016)

Acción correctiva. Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición. (ISO, 2005)

Acción preventiva. Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI. (ISO, 2005)

Activo. Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización. (ISO, 2005)

Alcance. Ámbito de la organización que queda sometido al SGSI. Este debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno. (ISO, 2005)

Amenaza. Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o la organización. (ISO, 2005)

Análisis de riesgos. Uso sistemático de la información para identificar fuentes y estimar el riesgo. (ISO, 2005)

Autenticación. Proceso que tiene por objetivo asegurar la identificación de una persona o sistema (ISO, 2005)

Confidencialidad. Acceso a la información por parte únicamente de quienes estén autorizados. Característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados, (ISO, 2005)

Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota control es también utilizado como sinónimo de salvaguarda o contramedida (ISO, 2005)

Disponibilidad. Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada (ISO, 2005)

Evaluación de riesgos. Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo. (ISO, 2005)

Gestión de riesgos. Es un proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73.2002]. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (ISO, 2005)

Incidente. Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO, 2005)

Integridad. Es el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos. (ISO, 2005)

ISO. Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares. (ISO, 2005)

ISO 27001. Es un estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005. (ISO, 2005)

ISO 27002. Es un código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007. (ISO, 2005)

PDCA. Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). (ISO, 2005)

Política de seguridad. Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002.2005]. Intención y dirección general expresada formalmente por la Dirección. (ISO, 2005)

Riesgo. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73.2002]. Combinación de la probabilidad de un evento y sus consecuencias. (ISO, 2005)

Riesgo residual. Según [ISO/IEC Guía 73.2002] El riesgo que permanece tras el tratamiento del riesgo. (ISO, 2005)

Seguridad de la información. Según [ISO/IEC 27002.2005]. Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas. (ISO, 2005)

Selección de controles. Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable. (ISO, 2005)

SGSI. Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001.2005]. La parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (ISO, 2005)

Tratamiento de riesgos. Según [ISO/IEC Guía 73.2002]. Proceso de selección e implementación de medidas para modificar el riesgo. (ISO, 2005)

Vulnerabilidad. Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza (ISO, 2005)

2.4 Marco legal

Siempre que se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. que sean aplicables en el desarrollo de sus actividades. De manera general se puede mencionar el tema de seguridad social, cumplir con la biblioteca, permisos, licencias de construcción, etc. pero en lo que se refiere específicamente a seguridad de la información, estas son las Leyes vigentes al día de hoy:

ISO 27001. La norma ISO 27001 fue publicada en octubre de 2005, esencialmente la sustitución de la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. Sí BS7799 era un estándar de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. Es esto en contra de la cual se concede la certificación. Hoy en día más de mil certificados están en su lugar, en todo el mundo. (Castro & Ciacedo, 2013)

En la publicación, la norma ISO 27001 mejora el contenido de la norma BS7799-2 y armonizada con otros estándares. Un esquema se ha presentado por varios organismos de certificación para la conversión de la certificación BS7799 con la certificación ISO27001. (Castro & Ciacedo, 2013)

El objetivo de la norma en sí misma es "proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI)". En cuanto a su adopción, esto debería ser una decisión estratégica. Además, "El diseño y la aplicación de la información del sistema de gestión de seguridad de una organización están influenciados por las necesidades de la organización y objetivos, requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización." (Castro & Ciacedo, 2013)

La versión 2005 de la norma en gran medida empleada del PDCA, Plan-Do-Check-Act modelo para estructurar los procesos, y reflejen los principios establecidos en las directrices

OECG (ver oecd.org). Sin embargo, la versión más reciente, de 2013, pone más énfasis en la medición y evaluación de lo bien SGSI de una organización está realizando. Una sección sobre la contratación externa también se añadió con esta versión, y se prestó mayor atención al contexto de la organización de seguridad de la información. (Castro & Ciacedo, 2013)

Certificación del Sistema de Gestión de Seguridad de la Información con ISO/IEC 27001 – ICONTEC. El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), es el Organismo Nacional de Normalización de Colombia. Entre sus labores se destaca la creación de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. ICONTEC es el representante de la Organización Internacional para la Estandarización (ISO), en Colombia. (NTC-ISO/IEC, 2006)

El estándar para la seguridad de la información ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información ((NTC-ISO/IEC, 2006)

Abarca:

- Organización de la seguridad de la información.
- Política de seguridad.
- Gestión de activos.
- Control de acceso.
- Seguridad de los recursos humanos.
- Cumplimiento.

- Seguridad física y del entorno.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de las comunicaciones y operaciones.
- Gestión de la continuidad del negocio.
- Gestión de incidentes de seguridad de la información. (ICONTEC, 2014)

Ley 23 De 1982 Sobre derechos de autor. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. (Ley 23 de 1982, 2014)

Ley 44 de 1993. Por la cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal.

Ley N° 44 de 1993 (5 de febrero) modifica y adiciona la Ley N° 23 de 1982 y se modifica la Ley N° 29 de 1944. Mediante la adición de disposiciones y medidas especiales para el Registro Nacional del Derecho de Autor, las sociedades de gestión colectiva de derechos de autor y derechos conexos, sanciones y otros derechos. (autor, 2014)

El Registro Nacional del Derecho de Autor es competencia de la Unidad Administrativa Especial - Dirección Nacional del Derecho de Autor, con carácter único para todo el territorio

nacional.

Ley 719 de 2001. DECRETO 1721 DE 2002 (Agosto 6) "Por el cual se reglamenta la Ley 719 de 2001, que modificó las Leyes 23 de 1982 y 44 de 1993". EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA, en ejercicio de sus facultades constitucionales, en especial las conferidas por el Artículo 189 numeral 11 de la Constitución Política de Colombia, DECRETA: Derecho exclusivo. El autor de una obra musical, o su derechohabiente, tiene el derecho exclusivo de realizar, autorizar o prohibir cualquier comunicación al público de su obra por medios alámbricos o inalámbricos, comprendida su puesta a disposición del público, de tal forma que los miembros del público puedan acceder a éstas desde el lugar y en el momento que cada uno de ellos elija. (Ley 719 de 2001, 2014)

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. (Archivo General, 1999)

Ambito 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. (Ley 527 De 1999 , 2014)

Ley Estatutaria 1266 Del 31 De Diciembre De 2008. Decreto N° 2952 de 2010 por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008, EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. En ejercicio de sus facultades constitucionales y legales, en especial, las conferidas por el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en los artículos 12 y 13 de la Ley 1266 de 2008.

Que el 31 de diciembre de 2008 se expidió la Ley Estatutaria N° 1266 por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 Del 5 De Enero 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". (Ley 1273 5 de enero de 2009)

El 5 de Enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano: Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; Capitulo Segundo: De los atentados informáticos y otras infracciones.

Como se puede ver, esta Ley está muy ligada a la ISO 27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 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 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. (Secretaria Senado, 2012)

Capitulo 3. Diseño metodologico

3.1 Tipo de investigacion

Para el desarrollo de la investigación se acudirá a la investigación descriptiva porque ésta busca especificar las propiedades, características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Describe tendencias de un grupo o población. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar como se relacionan éstas. (Hernandez, 2010)

Teniendo en cuenta que el objeto del estudio inicialmente es establecer el Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los usuarios de la biblioteca Chaid Neme, para lograr este fin se necesita caracterizar el objeto de estudio, identificar los objetos que tienen dicha característica, describir el contexto en el cual se está desarrollando el objeto de estudio, cuantificar que tan grande es la problemática. (Hernandez, 2010)

3.2 Población y muestra

La población está definida por los procesos que manejan los usuarios de la biblioteca Chaid Neme.

Considerando que la población objeto de la investigación, cuantitativamente es reducida, se trabajará con el total de la población.

3.3 Técnicas e instrumentos de recolección de datos

Para la Auditoria de Cumplimiento la recolección de la información será recopilada por medio de encuestas, observación directa, listas de chequeo, y entrevistas no estructuradas, realizadas al personal administrativo de la biblioteca Chaid Neme.

La encuesta la define el Profesional García Ferrado como "una investigación realizada sobre una muestra de sujetos representativa de un colectivo más amplio, utilizando procedimientos estandarizados de interrogación con intención de obtener mediciones cuantitativas de una gran variedad de características objetivas y subjetivas de la población" (Estadistica, 2013).

La entrevista no estructurada siendo esta terminología definida por Natalia Jimeno Molins, donde explica el tipo de entrevista utilizada por el proyecto, en la que abre el grado de libertad de preguntas y respuestas, las preguntas no son realizadas a través de un formato rígido o específico, sino que ocurren con cierto grado de espontaneidad. (Jimeno)

Según la observación directa es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, sin intervención, con el fin de tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de

conocimientos que constituye la ciencia ha sido lograda mediante la observación. Observar científicamente significa observar con un objetivo claro, definido y preciso: el investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación. (Ferrer, s.f.)

La lista de chequeo, como herramienta metodológica está compuesta por una serie de ítems, factores, propiedades, aspectos, componentes, criterios, dimensiones o comportamientos, necesarios de tomarse en cuenta, para realizar una tarea, controlar y evaluar detalladamente el desarrollo de un proyecto, evento, producto o actividad. Dichos componentes se organizan de manera coherente para permitir que se evalúe de manera efectiva, la presencia o ausencia de los elementos individuales enumerados o por porcentaje de cumplimiento u ocurrencia. (Ferrer, s.f.)

3.4 Informe de auditoria

Se tabulará de acuerdo a las técnicas recomendadas para obtener el mejor efecto posible, donde se tomaran resultados para análisis de los datos y determinar el estado en el que se encuentra la seguridad de información en los Procesos Soportados por el Área de Sistemas de la biblioteca Chaid Neme

Capítulo 4. Resultados

4.1 Diagnóstico para identificar las vulnerabilidades y amenazas de seguridad de información de los servicios y procesos de la Biblioteca recolectando la información interna y externa, por medio de los procesos descritos en la norma NTC-ISO/IEC 27001:2013.

Dentro de este diagnóstico se recopilo la información por medio de encuestas, observación directa, listas de chequeo, y entrevistas no estructuradas, realizadas al personal administrativo de la biblioteca Chaid Neme, así como la observación con el fin de determinar las vulnerabilidades, debilidades y amenazas de la seguridad de la información. (Ver apéndice A, B, C y D)

Los resultados obtenidos fueron los siguientes:

El estado actual de la seguridad de la información de la Biblioteca CHAID NEME.

- **Sistemas.** La biblioteca CHAID NEME es una entidad que soporta sus procesos misionales, las cuales les permiten diligenciar cada uno de los trámites necesarios para dar cumplimiento a todas sus funciones.

- La biblioteca CHAID NEME cuenta con cinco empleados de los cuales tres utilizan un computador y dos empleados no utilizan, ya que estos dos funcionarios prestan sus servicios en servicios generales y este cargo no amerita la utilización de computadores o dispositivos electrónicos. Esto quiere decir que los procesos administrativos tales como

dirección, secretaria y auxiliar de biblioteca dependen fundamentalmente de equipos de cómputo para el cumplimiento de las funciones correspondientes.

Situaciones Encontradas. A continuación veremos en la tabla 1 de forma detallada las situaciones encontradas que representan riesgo y falencia en cuanto a seguridad de la información se refiere en la biblioteca CHAID NEME con las posibles causas y soluciones.

Para poder obtener esta información, se realizó una visita a las instalaciones físicas de la biblioteca CHAID NEME pues es el lugar de donde se realiza el presente estudio y de donde proviene la información directa y confiable para el posterior análisis. Se tuvo en cuentas métodos de recolección de información tales como entrevistas con funcionarios y directivos de la biblioteca CHAID NEME y la observación directa de procesos realizados en los dispositivos de computo.

Dentro de la tabla es preciso aclarar ciertos términos y/o abreviaturas para una fácil, correcta y rápida interpretación. Los términos y abreviaturas son los siguientes:

Empresa. Lugar o establecimiento donde se realizó el estudio. En este caso se hizo en la biblioteca CHAID NEME en OCAÑA.

Ref. Referencia o código para ordenar numéricamente en orden ascendente las situaciones encontradas

Causas. Motivos por los cuales ocurren las falencias o situaciones riesgosas.

Solución. Posible alternativa de mejora para mitigar parcialmente o definitivamente la falencia o riesgo que comprometa la seguridad de la información y fortalecer los procesos de manejo de información dentro de la biblioteca CHAID NEME

Tabla 1
Situaciones encontradas

Empresa biblioteca CHAID NEME			**Día** 01 **Mes** 04 **Año** 17
Ref.	**Situaciones**	**Causas**	**Solución**
001	Faltan buenas prácticas en la utilización de contraseñas de accesos a los equipos.	Falta de conocimientos de buenas prácticas en seguridad de la información.	Capacitación al personal administrativo.
002	Instalación de Software sin certificado de seguridad reconocido.	Ausencia de políticas de seguridad de la información en donde se reglamente la instalación del Software.	Diseño e implementación de una política adecuada donde se contemple todo lo relacionado con el Software.
003	Ausencia parcial de cultura de copias de seguridad y restauración (Backup) de la información sensible de la empresa.	Desconociendo de buenas prácticas de seguridad de la información	Capacitación al personal de organización. Creación de procedimientos para el crear Backup.
004	Inclusión de datos personales en las contraseñas de acceso y poca frecuencia en el cambio de las mismas.	Falta de implementación de las políticas de seguridad de la información y de buenas prácticas.	Reestructuración de la política existente y la capacitación al personal en buenas partes.
006	Utilización incorrecta de las cuentas de correo electrónico institucionales.	Falta de políticas de seguridad de la información y de buenas prácticas de seguridad de la información.	Reestructuración de la política existente y la capacitación al personal en buenas partes.
007	Incumplimiento en algunas funciones de los empleados.	Inconsistencia en el manual de procesos y procedimientos.	Adecuación y apropiación del manual de procesos y procedimientos.
008	Malos manejos en la adquisición y la implementación de Tecnologías de la Información.	Desconocimientos en adquisición de Tecnologías de la Información	Estructuración de un Plan de Estratégico de Tecnologías de la Información
009	Desconocimientos de la seguridad de la información por parte de la alta gerencia.	Falta de políticas de seguridad de la información y de buenas prácticas.	Implementación de políticas de seguridad de la Información y capacitación al personal administrativo.
010	Se observó que el proceso de selección de personal debe ser más riguroso	Inexistencia de criterios de selección, dentro de una política establecida.	Estructuración e implementación del proceso de gestión humana en la organización (reclutamiento, selección, capacitación, etc)
011	Mal procedimiento en la entrega de cargos, o empalmes mal ejecutados	Inexistencia de criterios dentro de la política que	Estructurar en la política institucional, los respectivos

	entre el funcionario saliente y entrante.	establece la terminación de contrato.	empalmes a la hora de finalización de contratos.
012	No se contempla la entrega de las políticas de seguridad de la información a funcionarios	Desconocimiento de la importancia de la política de seguridad de la información para la organización.	Directrices de las alta gerencia para la implantación la políticas de seguridad de la información.
013	Inconsistencias en el tratamiento de la seguridad de la información.	Desconocimiento de la importancia de salvaguardar la confidencialidad, integridad y disponibilidad	Contratación y capacitación del personal y Tecnología adecuada que permita salvaguardar la información
014	Ausencia de las penalidades contempladas para quienes infrinjan las normas.	Inexistencia de una política de seguridad de la información que contemple dichas sanciones	Elaboración de una política de seguridad de la información que contemple dichas restricciones.
015	La biblioteca CHAID NEME no cuenta con un Manual de Seguridad de la Información	Desconocimiento de la importancia de implementar políticas de seguridad de la información, para tener buenas prácticas en el buen uso seguro de la información.	Implementar las políticas de seguridad de la información.
016	No se realizan revisiones periódicas a las políticas de seguridad de la información.	No cuenta con comité de seguridad de la información que esté al tanto de los cambios en cuanto a seguridad de la Información.	Crear un Comité de Seguridad de la Información.
017	No existe control de las devoluciones de activos, por parte del usuario al momento de finalizar el contrato o empleo.	Falta de control de los activos de la empresa. No existe ni siquiera el acta por el cual el empleado se hace responsable de los activos que utiliza mientras tiene alguna vinculación con la biblioteca	Formalizar el proceso, llenar las actas de entrega de activos al momento de emplear y actas de entrega al momento que se desvincula el funcionario o contratista.
018	No existen políticas para gestionar los medios removibles, para proteger la información contenida en las diferentes formas almacenamiento.	No se tiene conciencia de la importancia de proteger los diferentes sitios donde se almacena la información.	Definir dentro de las políticas de seguridad la gestión de los medios removibles dentro de la entidad.
019	No se encuentran protegidos los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte, como el dispositivo con interfaz USB para firmado digital.	No existe conciencia sobre la protección que se le debe dar a estos medios.	Especificar dentro de las políticas de seguridad de la información la forma como se deben proteger estos medios.
020	No está oficializada la asignación de la función de administrador de la seguridad a la ingeniera de sistemas.	No está actualizado el manual de funciones de cada cargo de la biblioteca CHAID NEME	Actualizar el Manual de funciones de acuerdo a las nuevas funciones de cada empleado.
021	No existe ningún procedimiento para otorgar y/o revocar el acceso y privilegios a los sistemas informáticos.	No está establecido un comité de calidad, no existen procedimientos formales.	Establecer un procedimiento formal para este caso.
022	Solo cuentan con antivirus para la protección de los equipos de	Confianza en el equipo de trabajo, y falta de inversión	Tomar conciencia de la importancia de establecer medidas de seguridad

	cómputo, no tienen instalados otra medida de seguridad como IDS, FIREWALLS, entre otros. La manera como protegen sus servidores físicamente es aislándolos del personal no autorizado y de manera lógica con contraseñas de acceso.	en el aspecto de seguridad.	tanto físicas como lógicas para salvaguardar el activo más importante de la empresa como lo es la información.
023	No existe una bitácora que recopile las veces que se le realizan revisiones a las instalaciones físicas, verbalmente indican que se realizan con mucha frecuencia pero no existe la evidencia.	Le restan importancia a la formalidad que deben tener estos procesos, de documentar cada vez que se realicen revisiones.	Llevar un registro cada vez que se realicen revisiones físicas y reportan los inconsistencias detectadas.
024	No existe ningún control para los visitantes, y ellos no son acompañados para visitar las áreas de la biblioteca CHAID NEME.	Falta de políticas de establezcan el ingreso controlado a las instalaciones la biblioteca CHAID NEME.	Establecer dentro de las Políticas de Seguridad de la información el control de acceso físico a las instalaciones.
025	No existe un sistema interno de grabación de circuito cerrado de tv.	Falta de inversión en seguridad física	Implementar un sistema interno de grabación de circuito cerrado de tv.
026	No se realizan cambios de las cerraduras con regularidad.	Exceso de confianza.	Establecer una política que regule la realización de cambios en la cerradura con frecuencia.
027	La biblioteca CHAID NEME no cuenta con alarmas.	Desconocimiento o exceso de confianza	Implementar e incluir en la Política, la obligatoriedad de tener monitoreada la alarma por un ente central.
028	No existe alarma de detección de humo y tampoco está conectada a la central de bomberos	Desconocimiento o exceso de confianza	Crear el plan de emergencias y evacuación.
029	No existe medidas de seguridad que garanticen la continuidad del suministro eléctrico	No tienen plan de contingencia. No existe planta eléctrica en La biblioteca CHAID NEME	Adquirir una Planta Eléctrica. Establecer mecanismos para poder continuar sin el fluido eléctrico.
030	No existen procedimientos para la eliminación de manera segura de información o dispositivos de cómputo. Cuando ya no es útil es alojada aun archivador físico o los dispositivos de cómputo se donan.	Falta de procedimientos para controlar, la información y dispositivos que no son utilizados.	Desarrollar un comité de calidad y actualizar las políticas de seguridad de la información que contemplen esta parte
031	No existe un funcionario encargado de la verificar que todas las funciones de cada quien se realicen de manera correcta.	No existen comités de calidad ni de control interno.	Establecer un comité de Calidad y Control interno.
032	No existe control interno, o alguien que haga sus veces para verificar que se realizan los procedimientos como así están estipulados.	No existe control Interno	Establecer el control interno en La biblioteca CHAID NEME

033	No existe protección contra código malicioso	No cuentan con herramientas especializadas para este tipo de inconvenientes.	Adquirir nuevas herramientas de seguridad de la información e implementar las Políticas de Seguridad de la información.
034	No se lleva un registro de actividades y supervisión y nunca se han realizado auditorias de Sistemas.	Falta de personal Capacitado en el área de Auditoria, y no le dan importancia a los registros de supervisión y actividades.	Desarrollar un plan de auditorías y concienciar a los funcionarios encargados del área de la importancia de llevar registros de las actividades y supervisión.
035	Gestión de requerimientos para adquirir nuevos sistemas de información o mejorar los existentes.	Falta de planeación	Planear y gestionar los requerimientos que contribuyan a la toma de decisiones en el momento de adquirir nuevos sistemas de información o mejorar los existentes
036	No se garantizan las características fundamentales de la seguridad de la información en las aplicaciones.	No se estiman los riesgos inherentes a la información y el valor que ésta tiene para la organización	Tipificar, clasificar la información que se transmite hacia y desde la red y que opera bajo las plataformas organizacionales
037	No existe un procedimiento de control formal para realizar cambios a los sistemas	Desconocimiento de la importancia de identificar los activos de la organización, sus funciones y su utilización	Documentar detalladamente todo el proceso de adquisición y mantenimiento y cambios en los sistemas
038	No se realiza supervisión y seguimiento de sistemas contratados externamente	Falta de Gestión y pertinencia a las contrataciones	Mantener de manera organizada el proceso de seguimientos a las diferentes contrataciones.
039	En la política de seguridad de la información existente, no se contempla la relación con los suministradores ni gestión de riesgos presentes en este proceso	No se contempla el proceso de adquisición como factor importante de la seguridad de la información	Ampliar el alcance y contemplar factores estratégicos en la política de seguridad de la información
040	Falta documentación y control de servicios prestados por terceros	No se contempla como proceso importante tener seguimiento de los temas que tienen que ver con terceros	Plantear dentro de las políticas y gestión de riesgos la trazabilidad de procesos con terceros.
041	No se cuenta con un proceso de control para mantener las licencias de software actualizadas	No se contempla en las políticas de seguridad de la información el seguimiento y actualización de productos software	Se debe plantear en la política de seguridad de la información la periódica actualización de software que lo requiera

Elaborado (Nombre y Firma)	**Aprobó (Nombre y Firma)**
JHON JAIRO VARGAS LASCARRO	**JHON JAIRO VARGAS LASCARRO**
YAQUELINE MANDÓN CASTRO	**YAQUELINE MANDÓN CASTRO**
GUILLERMO GERARDINO SÁNCHEZ	**GUILLERMO GERARDINO SÁNCHEZ**

Fuente: Autores del proyecto.

Situaciones relevantes. Para nuestro criterio todas las situaciones encontradas son relevantes por lo que se necesita urgente ejecución de plan de mejoramiento e implementar políticas de seguridad de la información.

Tabla 2
Situaciones relevantes

Empresa	**Día**	**Mes**	**Año**
biblioteca CHAID NEME	01	04	17

Ref.	**Situaciones**	**Causas**	**Solución**
001	Faltan buenas prácticas en la utilización de contraseñas de accesos a los equipos.	Falta de conocimientos de buenas prácticas en seguridad de la información.	Capacitación al personal administrativo.
002	Instalación de Software sin certificado de seguridad reconocido.	Ausencia de políticas de seguridad de la información en donde se reglamente la instalación del Software.	Diseño e implementación de una política adecuada donde se contemple todo lo relacionado con el Software.
003	Ausencia parcial de cultura de copias de seguridad y restauración (Backup) de la información sensible de la empresa.	Desconociendo de buenas prácticas de seguridad de la información	Capacitación al personal de organización. Creación de procedimientos para el crear Backup.
004	Inclusión de datos personales en las contraseñas de acceso y poca frecuencia en el cambio de las mismas.	Falta de implementación de las políticas de seguridad de la información y de buenas prácticas.	Reestructuración de la política existente y la capacitación al personal en buenas partes.
006	Malos manejos en las cuentas de correo electrónico institucionales.	Falta de políticas de seguridad de la información y de buenas prácticas de seguridad de la información.	Reestructuración de la política existente y la capacitación al personal en buenas partes.
007	Incumplimiento en algunas funciones de los empleados.	Inconsistencia en el manual de procesos y procedimientos.	Adecuación del manual de procesos y procedimientos.
008	Malos manejos en la adquisición y la implementación de TI.	Desconocimientos en adquisición de TI	Estructuración de un Plan de Estratégico de TI
009	Desconocimientos de la seguridad de la información por parte de la alta gerencia.	Falta de políticas de seguridad de la información y de buenas prácticas.	Implementación de políticas de seguridad de la Información y capacitación al personal administrativo.
010	Se observó que el proceso de selección de personal debe ser más riguroso	Inexistencia de criterios de selección, dentro de una política establecida.	Estructuración de las políticas, en donde se estipula criterios de antes y después de la contratación.
011	Inconsistencia en la entrega de cargos, o empalmes pertinentes.	Inexistencia de criterios dentro de la política que establece la terminación de contrato.	Estructurar en la política institucional, los respectivos empalmes a la hora de finalización de contratos.
012	No se contempla la entrega de las políticas de seguridad de la información a funcionarios	Desconocimiento de la importancia de la política de seguridad de la información	Directrices de las alta gerencia para la implantación la políticas de seguridad de la información.

		para la organización.	
013	Inconsistencias en el tratamiento de la seguridad de la información.	Desconocimiento de la importancia de salvaguardar la confidencialidad, integridad y disponibilidad	Contratación y capacitación del personal y Tecnología adecuada que permita salvaguardad la información
014	Ausencia de las penalidades contempladas para quienes infrinjan las normas.	Inexistencia de una política de seguridad de la información que contemple dichas sanciones	Elaboración de una política de seguridad de la información que contemple dichas restricciones.
015	La biblioteca CHAID NEME no cuenta con un Manual de Seguridad de la Información	Desconocimiento de la importancia de implementar políticas de seguridad de la información, para tener buenas prácticas en el buen uso seguro de la información.	Implementar las políticas de seguridad de la información.
016	No se realizan revisiones periódicas a las políticas de seguridad de la información.	No cuenta con comité de seguridad de la información que esté al tanto de los cambios en cuanto a seguridad de la Información.	Crear un Comité de Seguridad de la Información.
017	No existe control de las devoluciones de activos, por parte del usuario al momento de finalizar el contrato o empleo.	Falta de control de los activos de la empresa. No existe ni siquiera el acta por el cual el empleado se hace responsable de los activos que utiliza mientras tiene alguna vinculación con la biblioteca	Formalizar el proceso, llenar las actas de entrega de activos al momento de emplear y actas de entrega al momento que se desvincula el funcionario o contratista.
018	No existen políticas para gestionar los medios removibles, para proteger la información contenida en las diferentes formas almacenamiento.	No se tiene conciencia de la importancia de proteger los diferentes sitios donde se almacena la información.	Definir dentro de las políticas de seguridad la gestión de los medios removibles dentro de la entidad.
019	No se encuentran protegidos los medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte, como el dispositivo con interfaz USB para firmado digital.	No existe conciencia sobre la protección que se le debe dar a estos medios.	Especificar dentro de las políticas de seguridad de la información la forma como se deben proteger estos medios.
020	No está oficializada la asignación de la función de administrador de la seguridad a la ingeniera de sistemas.	No está actualizado el manual de funciones de cada cargo de la biblioteca CHAID NEME	Actualizar el Manual de funciones de acuerdo a las nuevas funciones de cada empleado.
021	No existe ningún procedimiento para otorgar y/o revocar el acceso y privilegios a los sistemas informáticos.	No está establecido un comité de calidad, no existen procedimientos formales.	Establecer un procedimiento formal para este caso.
022	Solo cuentan con antivirus para la protección de los equipos de cómputo, no tienen instalados otra medida de seguridad como IDS, FIREWALLS, entre otros. La manera como protegen sus	Confianza en el equipo de trabajo, y falta de inversión en el aspecto de seguridad.	Tomar conciencia de la importancia de establecer medidas de seguridad tanto físicas como lógicas para salvaguardar el activo más importante de la empresa como lo es la información.

	servidores físicamente es aislándolos del personal no autorizado y de manera lógica con contraseñas de acceso.		
023	No existe una bitácora que recopile las veces que se le realizan revisiones a las instalaciones físicas, verbalmente indican que se realizan con mucha frecuencia pero no existe la evidencia.	Le restan importancia a la formalidad que deben tener estos procesos, de documentar cada vez que se realicen revisiones.	Llevar un registro cada vez que se realicen revisiones físicas y reportan los inconsistencias detectadas.
024	No existe ningún control para los visitantes, y ellos no son acompañados para visitar las áreas de la biblioteca CHAID NEME.	Falta de políticas de establezcan el ingreso controlado a las instalaciones la biblioteca CHAID NEME.	Establecer dentro de las Políticas de Seguridad de la información el control de acceso físico a las instalaciones.
025	No existe un sistema interno de grabación de circuito cerrado de tv.	Falta de inversión en seguridad física	Implementar un sistema interno de grabación de circuito cerrado de tv.
026	No se realizan cambios de las cerraduras con regularidad.	Exceso de confianza.	Establecer una política que regule la realización de cambios en la cerradura con frecuencia.
027	La biblioteca CHAID NEME no cuenta con alarmas.	Desconocimiento o exceso de confianza	Implementar e incluir en la Política, la obligatoriedad de tener monitoreada la alarma por un ente central.
028	No existe alarma de detección de humo y tampoco está conectada a la central de bomberos	Desconocimiento o exceso de confianza	Crear el plan de emergencias y evacuación.
029	No existe medidas de seguridad que garanticen la continuidad del suministro eléctrico	No tienen plan de contingencia. No existe planta eléctrica en La biblioteca CHAID NEME	Adquirir una Planta Eléctrica. Establecer mecanismos para poder continuar sin el fluido eléctrico.
030	No existen procedimientos para la eliminación de manera segura de información o dispositivos de cómputo. Cuando ya no es útil es alojada aun archivador físico o los dispositivos de cómputo se donan.	Falta de procedimientos para controlar, la información y dispositivos que no son utilizados.	Desarrollar un comité de calidad y actualizar las políticas de seguridad de la información que contemplen esta parte
031	No existe un funcionario encargado de la verificar que todas las funciones de cada quien se realicen de manera correcta.	No existen comités de calidad ni de control interno.	Establecer un comité de Calidad y Control interno.
032	No existe control interno, o alguien que haga sus veces para verificar que se realizan los procedimientos como así están estipulados.	No existe control Interno	Establecer el control interno en La biblioteca CHAID NEME
033	No existe protección contra código malicioso	No cuentan con herramientas especializadas para este tipo de inconvenientes.	Adquirir nuevas herramientas de seguridad de la información e implementar las Políticas de Seguridad de la información.
034	No se lleva un registro de	Falta de personal Capacitado	Desarrollar un plan de auditorías y

	actividades y supervisión y nunca se han realizado auditorias de Sistemas.	en el área de Auditoria, y no le dan importancia a los registros de supervisión y actividades.	concienciar a los funcionarios encargados del área de la importancia de llevar registros de las actividades y supervisión.
035	Gestión de requerimientos para adquirir nuevos sistemas de información o mejorar los existentes.	Falta de planeación	Planear y gestionar los requerimientos que contribuyan a la toma de decisiones en el momento de adquirir nuevos sistemas de información o mejorar los existentes
036	No se garantizan las características fundamentales de la seguridad de la información en las aplicaciones.	No se estiman los riesgos inherentes a la información y el valor que ésta tiene para la organización	Tipificar, clasificar la información que se transmite hacia y desde la red y que opera bajo las plataformas organizacionales
037	No existe un procedimiento de control formal para realizar cambios a los sistemas	Desconocimiento de la importancia de identificar los activos de la organización, sus funciones y su utilización	Documentar detalladamente todo el proceso de adquisición y mantenimiento y cambios en los sistemas
038	No se realiza supervisión y seguimiento de sistemas contratados externamente	Falta de Gestión y pertinencia a las contrataciones	Mantener de manera organizada el proceso de seguimientos a las diferentes contrataciones.
039	En la política de seguridad de la información existente, no se contempla la relación con los suministradores ni gestión de riesgos presentes en este proceso	No se contempla el proceso de adquisición como factor importante de la seguridad de la información	Ampliar el alcance y contemplar factores estratégicos en la política de seguridad de la información
040	Falta documentación y control de servicios prestados por terceros	No se contempla como proceso importante tener seguimiento de los temas que tienen que ver con terceros	Plantear dentro de las políticas y gestión de riesgos la trazabilidad de procesos con terceros.
041	No se cuenta con un proceso de control para mantener las licencias de software actualizadas	No se contempla en las políticas de seguridad de la información el seguimiento y actualización de productos software	Se debe plantear en la política de seguridad de la información la periódica actualización de software que lo requiera

Elaborado (Nombre y Firma)	**Aprobó (Nombre y Firma)**
JHON JAIRO VARGAS LASCARRO	**JHON JAIRO VARGAS LASCARRO**
YAQUELINE MANDÓN CASTRO	**YAQUELINE MANDÓN CASTRO**
GUILLERMO GERARDINO SÁNCHEZ	**GUILLERMO GERARDINO SÁNCHEZ**

Fuente: Autores del proyecto.

Como toda organización, La Biblioteca Chaid Neme busca que su funcionamiento se realice con seguridad, eficiencia y transparencia; sin embargo, su atención se centra en otros aspectos, desconociendo que el manejo de la información también se constituye en un eje fundamental para el adecuado ejercicio de su labor.

Una vez verificada el área administrativa y operativa La Biblioteca Chaid Neme se puede evidenciar que los controles relacionados con la seguridad de la información que manejan, no están acordes para garantizar la confidencialidad, disponibilidad e integridad de la misma, desde el punto de vista del factor tecnológico, al igual que el del factor humano que labora en la Empresa.

Una vez establecido un acercamiento directo con el gerente general de la Biblioteca y sus empleados, y realizada la entrevista respectiva, basada en los controles de la norma NTC-ISO-IEC 27001:2013, se logra identificar que la empresa se encuentra débil en lo que a seguridad en la información se refiere.

El gerente es consciente de la necesidad de implementar dichos controles que ayuden a organizar la entidad, protegiendo la información de fugas y usos maliciosos, ya sea por parte del personal interno o externo a la entidad.

Teniendo en cuenta el análisis GAP realizado en la Biblioteca, se logra identificar en los diferentes ciclos de la metodología PHVA lo siguiente:

Tabla 3
Planear

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA
1	La Biblioteca cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI?	No cumple	No se está haciendo
2	La Biblioteca creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	No cumple	No existe
3	La Biblioteca contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	Cumple parcialmente	Se definió y aprobó pero no está documentado
4	La Biblioteca ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	No cumple	No se está haciendo
5	La Biblioteca ha identificado las partes interesadas, necesidades y expectativas de éstas respecto al Sistema de Gestión de Seguridad de la Información?	No cumple	No se está haciendo
6	La Biblioteca ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	Cumple parcialmente	Se realiza pero no bajo la norma
7	En la Biblioteca se ha definido un Comité de Seguridad de la Información?	No cumple	No existe
8	La Biblioteca cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	No cumple	No existe
9	En la Biblioteca existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No cumple	No existe
10	En la Biblioteca existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	No cumple	No existe
11	La Biblioteca tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	No cumple	No se está haciendo
12	La Biblioteca ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	No cumple	No existe
13	La Biblioteca ha evaluado las competencias	No cumple	No se está

	de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?		haciendo
14	La Biblioteca tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	No cumple	No existe
15	La Biblioteca tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple	No existe

Fuente. Autores del proyecto

Se evidencia que existe toda la intención de mejorar y comenzar a implementar un sistema de seguridad de la información, de una meta del 30%, solo un 1.5% se está cumpliendo; dichos resultados se pueden establecer sosteniendo que existe la aprobación por parte del superior jerárquico de iniciar el proyecto, de igual manera, ha evaluado los objetivos y necesidades que tienen con respecto a la implementación de dicho sistema.

No obstante por el momento no cuenta con ningún factor relevante, tales como un comité de seguridad de la información, ni documentos con políticas, roles, responsabilidades, y autoridades en seguridad; así mismo, no tiene establecido ningún proceso para identificar, analizar, valorar y tratar los riesgos en cuanto a seguridad de la información se refiere.

Tabla 4
Hacer

	ANEXO	ESTADO	EVIDENCIA
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**		
A5.1	Orientación de la dirección para la gestión de la seguridad de la información		
A5.1.1	Políticas para la seguridad de la información	No cumple	No existe
A5.1.2	Revisión de las políticas para la seguridad de la información.	No cumple	No existe
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A6.1	Organización interna		
A6.1.1	Roles y responsabilidades para la seguridad de la información	No cumple	No existe
A6.1.2	Separación de deberes	No cumple	No se está haciendo
A6.1.3	Contacto con las autoridades	No cumple	No se está haciendo
A6.1.4	Contacto con grupos de interés especial	No cumple	No se está haciendo
A6.1.5	Seguridad de la información en la gestión de proyectos.	No cumple	No existe
A6.2	Dispositivos móviles y teletrabajo		
A6.2.1	Política para dispositivos móviles	Cumple parcialmente	El acceso a la red a través de dispositivos móviles, está restringido, pero no se encuentra documentado
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A7.1	Antes de asumir el empleo		
A7.1.1	Selección	Cumple parcialmente	Existe un perfil para cada cargo, pero no está documentado y actualizado en su totalidad
A7.1.2	Términos y condiciones del empleo	Cumple parcialmente	Existen cláusulas de confidencialidad de la información en los contratos de los empleados, pero no está documentado de manera completa
A7.1	Durante la ejecución del empleo		
A7.2.1	Responsabilidades de la dirección	Cumple parcialmente	Conocen de la importancia de la seguridad de la información, pero no está documentado formalmente
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Cumple parcialmente	Conocen de la importancia de la seguridad de la información, pero no está documentado formalmente
A7.2.3	Proceso disciplinario	Cumple parcialmente	Una fuga de información, puede ocasionar la terminación del contrato
A7.3	Terminación y cambio de empleo		
A7.3.1	Terminación o cambio de responsabilidades de empleo	Cumple parcialmente	Cada empleado es responsable del manejo de la información de acuerdo con la claúsula de confidencialidad, una vez terminado

			el contrato, pero no existe un control
A8	**GESTIÓN DE ACTIVOS**		
A8.1	Responsabilidad por los activos		
A8.1.1	Inventario de activos	Cumple parcialmente	Existe un inventario de activos con características incompletas e informal
A8.1.2	Propiedad de los activos	Cumple parcialmente	A la hora de asignación de cargos se hace entrega de los equipos, los cuales deben ser entregados mediante acta una vez finalice la contratación, sin embargo, no está formalmente documentado
A8.1.3	Uso aceptable de los activos	Cumple parcialmente	Cada uno es responsable del procesamiento de la información y del uso que le dé a los equipos asignados, no obstante, no se encuentra formalmente documentado
A8.1.4	Devolución de activos	Cumple satisfactoriamente	Una vez finalizada la labor contractual, cada uno hace entrega de los equipos asignados mediante un acta.
A8.2	Clasificación de la información		
A8.2.1	Clasificación de la información	Cumple parcialmente	La información manejada contiene una reserva clasificada a nivel externo (restringido), e interno (empleados y asociados), siendo libre el acceso a la información para los empleados y personalizada para cada uno de los asociados
A8.2.2	Etiquetado de la información	No cumple	No existe un conjunto de procedimientos para el etiquetado de la información
A8.2.3	Manejo de activos	No cumple	No existe procedimiento para el manejo de activos
A8.3	Manejo de medios		
A8.3.1	Gestión de medio removibles	No cumple	No existe restricción del uso de medios removibles.
A8.3.2	Disposición de los medios	No cumple	No existe un control, ni procedimientos formales, para el uso de la información cuando ya no se requiera
A8.3.3	Transferencia de medios físicos	No cumple	No existe un control, ni procedimientos formales, para el uso de la información
A9	**CONTROL DE ACCESO**		
A9.1	Requisitos del negocio para el control de acceso		
A9.1.1	Política de control de acceso	No cumple	No existe política de control de acceso
A9.1.2	Acceso a redes y a servicios en red	Cumple parcialmente	Se asignan unos perfiles a los usuarios del Software SILOG de acuerdo con las funciones que desempeñan, sin embargo, no está documentado formalmente
A9.2	Gestión de acceso de usuarios		
A9.2.1	Registro y cancelación del registro de usuarios	Cumple parcialmente	Se asignan unos perfiles a los usuarios del Software SILOG de acuerdo con las funciones que desempeñan; sin embargo, no está documentado formalmente
A9.2.2	Suministro de acceso de usuarios	Cumple parcialmente	El acceso al software SILOG se hace previa autorización del gerente o del agente encargado, no obstante, no se hace de

			manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas
A9.2.3	Gestión de derechos de acceso privilegiado	Cumple parcialmente	El acceso al software SILOG se hace previa autorización del gerente o del agente encargado, no obstante, no se hace de manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas
A9.2.4	Gestión de información de autenticación secreta de usuarios	Cumple parcialmente	El acceso al software SILOG se hace previa autorización del gerente o del agente encargado, no obstante, no se hace de manera formal. Así mismo, no existe asignación de contraseñas a los usuarios para el ingreso a los sistemas
A9.2.5	Revisión de los derechos de acceso de usuarios	No cumple	Una vez asignados los perfiles a los usuarios del Software, no se vuelve a hacer ningún control sobre los mismos
A9.2.6	Retiro o ajuste de los derechos de acceso	Cumple parcialmente	Una vez finalizada la labor contractual, cada uno hace entrega de los equipos asignados mediante un acta. Así mismo se deshabilita los permisos y usuarios para el acceso al Software
A9.3	Responsabilidades de los usuarios		
A9.3.1	Uso de información de autenticación secreta	No cumple	A pesar de que existe una claúsula de confidencialidad al momento de la contratación, no existe una política que oriente el uso de información secreta
A9.4	Control de acceso a sistemas y aplicaciones		
A9.4.1	Restricción de acceso a la información	No cumple	No existe política de control de acceso
A9.4.2	Procedimiento de ingreso seguro	No cumple	No existe política de control de acceso
A9.4.3	Sistema de gestión de contraseñas	No cumple	El ingreso a los computadores no exige contraseñas. Para el ingreso al software en el cual sí se requiere contraseña, no existe sistema de gestión de las mismas
A9.4.4	Uso de programas utilitarios privilegiados	No cumple	No está restringido la instalación y uso de estos programas
A9.4.5	Control de acceso a códigos fuente de programas	No cumple	No está restringido el acceso a los códigos fuentes
A10	**CRIPTOGRAFIA**		
A10.1	Controles criptográficos		
A10.1.1	Política sobre el uso de controles criptográficos	No cumple	No existe política para la protección de la información
A10.1.2	Gestión de llaves	No cumple	No existe política para la protección de la información
A11	**SEGURIDAD FISICA Y DEL ENTORNO**		
A11.1	Áreas seguras	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A11.1.1	Perímetro de seguridad física	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A11.1.2	Controles de acceso físicos	Cumple parcialmente	El área de información se encuentra ubicada de manera segura, sin embargo, no está formalmente documentada

A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Cumple parcialmente	El área de información central cuenta con una estructura física nueva diseñada, para la prevención de riesgos naturales. Cabe señalar, que las agencias están expuestas ya que sus estructuras físicas no cuentan con las mismas características de la Edificación principal
A11.1.4	Protección contra amenazas externas y ambientales.	No cumple	No existen procedimientos para trabajo en áreas seguras
A11.1.5	Trabajo en áreas seguras.	Cumple parcialmente	Tanto la nueva estructura física, como la de las demás agencias están diseñadas con áreas que permiten el aislamiento de personas no autorizadas y ajenas a la entidad que puedan afectar el procesamiento de la información.
A11.1.6	Áreas de carga, despacho y acceso público	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A11.2	Equipos		
A11.2.1	Ubicación y protección de los equipos	Cumple satisfactoriamente	Cada equipo se encuentra ubicado de manera segura en las instalaciones, para evitar el fácil acceso de personal no autorizado
A11.2.2	Servicios de suministro	No cumple	No existe protección para los equipos ante cualquier interrupción o fallas en el suministro de la energía
A11.2.3	Seguridad en el cableado.	Cumple parcialmente	El cableado se encuentra canalizado en la nueva edificación (gerencia - área administrativa), sin embargo, en las agencias de despacho, éste no se encuentra protegido.
A11.2.4	Mantenimiento de los equipos.	Cumple parcialmente	Sólo se hacen mantenimientos correctivos
A11.2.5	Retiro de activos	Cumple parcialmente	Ningún equipo se retira sin autorización, sin embargo, no existe un formato de solicitud de retiro establecido
A11.2.6	Disposición segura o reutilización de equipos	No cumple	No existe restricción del uso de medios removibles.
A11.2.7	Equipos de usuario desatendido	No cumple	No existe protección alguna a los equipos desatendidos.
A11.2.8	Política de escritorio limpio y pantalla limpia	No cumple	No existe política de escritorio limpio, cada uno personaliza el escritorio a su manera.
A12	**SEGURIDAD DE LAS OPERACIONES**		
A12.1	Procedimientos operacionales y responsabilidades		
A12.1.1	Procedimientos de operación documentados	No cumple	No existe documentación para los procedimientos de operación.
A12.1.2	Gestión de cambios	No cumple	No existe control alguno sobre los cambios que surjan en la organización.
A12.1.3	Gestión de capacidad	No aplica	No posee ambientes de desarrollo y pruebas
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No aplica	No posee ambientes de desarrollo y pruebas
A12.2	Protección contra códigos maliciosos		

A12.2.1	Controles contra códigos maliciosos	No cumple	No existe una política claramente definida que permita tomar conciencia y restrinja el acceso a fuentes que vulneren los sistemas de información
A12.3	Copias de respaldo		
A12.3.1	Respaldo de la información	No cumple	No se realizan copias de seguridad regularmente del sistema y menos puestas a prueba
A12.4	Registro y seguimiento		
A12.4.1	Registro de eventos	No cumple	No se controlan los eventos y las fallas de la seguridad de la información.
A12.4.2	Protección de la información de registro	Cumple parcialmente	El área de manejo de información se encuentra apartada al acceso de personal externo; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido
A12.4.3	Registros del administrador y del operador	No cumple	No existe revisiones ni registros para la actividades desarrolladas
A12.4.4	Sincronización de relojes	No cumple	No existe sincronización referente a tiempo en los sistemas de procesamiento de información
A12.5	Control de software operacional		
A12.5.1	Instalación de software en sistemas operativos	No cumple	No existe una política de seguridad que restrinja la instalación de software en los sistemas operativos.
A12.6	Gestión de la vulnerabilidad técnica		
A12.6.1	Gestión de las vulnerabilidades técnicas	No cumple	No se tienen plenamente identificadas las vulnerabilidades que puedan afectar el normal funcionamiento de los sistemas de información
A12.6.2	Restricciones sobre la instalación de software	No cumple	No existen reglas que orienten la instalación de software por parte de los usuarios.
A12.7	Consideraciones sobre auditorias de sistemas de información		
A12.7.1	Controles de auditorías de sistemas de información	No cumple	No se realizan actividades de auditoría.
A13	**SEGURIDAD DE LAS COMUNICACIONES**		
A13.1	Gestión de la seguridad de las redes		
A13.1.1	Controles de redes	No cumple	No existe gestión y control en la red de la Biblioteca para proteger la información
A13.1.2	Seguridad de los servicios de red	No cumple	Existe exposición y vulnerabilidad de los servicios de red, no existen mecanismos de seguridad
A13.1.3	Separación en las redes	No cumple	No se evidencia separación en la red de los servicios de información y usuarios.
A13.2	Transferencia de información		
A13.2.3	Mensajería Electrónica	No cumple	Manejan un solo correo electrónico para toda la Biblioteca, no se evidencia control para lo enviado y recepcionado.

A13.2.4	Acuerdos de confidencialidad o de no divulgación	Cumple parcialmente	Existen cláusulas de confidencialidad de la información en los contratos de los empleados, pero no está documentado de manera completa, no obstante no se realiza una revisión periódica, para verificar el funcionamiento de la misma.
A14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A14.1	Requisitos de seguridad de los sistemas de información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	No cumple	No existen requisitos relacionados con la seguridad de la información.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	No cumple	No existen requisitos relacionados con la seguridad de la información.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	No cumple	No existe documentado los protocolos de protección de transacciones
A14.2	Seguridad en los procesos de Desarrollo y de Soporte		
A.14.2.1	Procedimientos de control de cambios en sistemas	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.2	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.3	Restricciones en los cambios a los paquetes de software	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.4	Principio de Construcción de los Sistemas Seguros.	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.5	Ambiente de desarrollo seguro	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.6	Desarrollo contratado externamente	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.7	Pruebas de seguridad de sistemas	No aplica	No posee área de desarrollo de aplicaciones
A.14.2.8	Prueba de aceptación de sistemas	No aplica	No posee área de desarrollo de aplicaciones
A14.3	Datos de prueba		
A.14.3.1	Protección de datos de prueba	No aplica	No posee área de desarrollo de aplicaciones
A15	**RELACIONES CON LOS PROVEEDORES**		
A15.1	Seguridad de la información en las relaciones con los proveedores.		
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Cumple parcialmente	Existe un contrato de confidencialidad con el proveedor del software, sin embargo se han visto afectados por situaciones que involucran la seguridad de la Biblioteca.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Cumple parcialmente	Existe un contrato de confidencialidad con el proveedor del software, sin embargo se han visto afectados por situaciones que involucran la seguridad de la Biblioteca.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Cumple parcialmente	El software está diseñado con parámetros de seguridad que permitan la minimización de los riesgos asociados a la

			información, se encuentra definido con el proveedor pero no se gestiona
A15.2	Gestión de la prestación de servicios de proveedores		
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Cumple parcialmente	Solo se hace de manera correctiva, en el evento de que sucede cualquier anomalía.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Cumple parcialmente	De acuerdo a las necesidades del negocio se conviene con el proveedor sobre las mejoras a realizar para que el software sea actualizado y optimizado.
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		
A16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A16.1.1	Responsabilidades y procedimientos	No cumple	No están definidos las responsabilidades y procedimientos para garantizar una respuesta rápida ante posibles incidentes en la información
A16.1.2	Reporte de eventos de seguridad de la información	No cumple	No existe un canal de gestión donde se puedan registrar los eventos de seguridad de la información.
A16.1.3	Reporte de debilidades de seguridad de la información	Cumple parcialmente	Cualquier eventualidad es informada por los usuarios del sistema, sin embargo no se encuentra un procedimiento formalmente definido
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	No cumple	No existen políticas de seguridad de la información
A16.1.5	Respuesta a incidentes de seguridad de la información	No cumple	No existen políticas de seguridad de la información
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	No cumple	No existe un canal de gestión donde se puedan registrar los eventos de seguridad de la información.
A16.1.7	Recolección de evidencia	No cumple	La organización no tiene procedimientos definidos para el manejo de la información
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**		
A17.1	Continuidad de Seguridad de la información		
A17.1.1	Planificación de la continuidad de la seguridad de la información	No cumple	No existe un plan de contingencia para la continuidad del negocio, en el evento de ser afectado por algún incidente interno o externo.
A17.1.2	Implementación de la continuidad de la seguridad de la información	No cumple	No existe un plan de contingencia para la continuidad del negocio, en el evento de ser afectado por algún incidente interno o externo.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No cumple	No existe un plan de contingencia para la continuidad del negocio, en el evento de ser afectado por algún incidente interno o externo.

A17.2	Redundancias		
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	No aplica	La Biblioteca no posee este tipo de instalaciones
A18	**CUMPLIMIENTO**		
A18.1	Cumplimiento de requisitos legales y contractuales		
A18.1.1	Identificación de la legislación aplicable.	No cumple	No existe documentación explícita relacionada con los sistemas de información y su reglamentación legal
A18.1.2	Derechos propiedad intelectual (DPI)	No aplica	La Biblioteca no posee patentes de software de desarrollo propio, utiliza software comerciales para su operación
A18.1.3	Protección de registros	No cumple	No existe documentación explícita relacionada con los sistemas de información y su reglamentación legal
A18.1.4	Privacidad y protección de información de datos personales	No cumple	A pesar de que se protege la información, no se hace siguiendo parámetros legales claramente definidos
A18.1.5	Reglamentación de controles criptográficos.	No aplica	No aplica para la Biblioteca por la naturaleza del servicio
A18.2	Revisiones de seguridad de la información		
A18.2.1	Revisión independiente de la seguridad de la información	No cumple	No existe una política para la seguridad de la información, que permita su posterior revisión
A18.2.2	Revisión del cumplimiento técnico	Cumple parcialmente	Los sistemas de información SILOG y SIIGO que utiliza la Biblioteca se revisan pero no se documenta

Fuente. Autores del proyecto

Empíricamente existen procesos que ayudan a proteger en un mínimo porcentaje la información, entre esos los siguientes: El acceso a las redes a través de los dispositivos móviles, están restringidos, existe un perfil para cada cargo, el cual es tenido en cuenta a la hora de la selección, existen cláusulas de confidencialidad de la información en los contratos de los empleados. Conocen de la importancia de la seguridad de la información y hacen énfasis en ello. De igual manera, tienen claro que una infracción en términos de fuga de información, puede ocasionar la terminación del contrato, por tal razón, cada uno es responsable del manejo de la información de acuerdo con la cláusula de confidencialidad, una vez terminado el contrato, pero no existe un control.

Se logra evidenciar que existe un inventario de activos con características incompletas e informales. A la hora de asignación de cargos se hace entrega de los equipos, los cuales deben ser devueltos mediante acta una vez

Así mismo, la información manejada contiene una reserva clasificada a nivel externo (restringido), e interno (empleados y asociados), siendo libre el acceso a la información para los empleados y personalizada para cada uno de los asociados

Con relación al acceso físico, el área de manejo de información se encuentra apartada al acceso de personal externo y de manera segura; no obstante, el ingreso de dichas personas no se encuentra formalmente restringido.

Es interesante resaltar que el área de información central cuenta con una estructura física nueva diseñada, para la prevención de riesgos naturales, sin embargo, las agencias están expuestas ya que sus estructuras no cuentan con las mismas características de la edificación principal.

Todo lo anterior se encuentra establecido, pero no está formalmente documentado.

Tabla 5
Verificar y actuar

		VERIFICAR	
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de la Información?	Cumple parcialmente	La Biblioteca no tiene la metodología documentada pero si realiza seguimiento a la seguridad de la información
2	La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?	No cumple	La Biblioteca no tiene un SGSI implementado
3	La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	La Biblioteca no tiene un SGSI implementado
4	La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	No cumple	La Biblioteca no tiene un SGSI implementado
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre	No cumple	La Biblioteca no tiene un SGSI implementado

	el desempeño de la seguridad de la información?		
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple	La Biblioteca no tiene un SGSI implementado
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoría?	No cumple	No se está haciendo
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	No cumple	No se está haciendo
9	La entidad revisa la eficacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	No cumple	No se está haciendo
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información después de las acciones tomadas?	No cumple	No posee SGSI
11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	No cumple	No se está haciendo
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	No cumple	No posee SGSI

Fuente. Autores del proyecto

Al no existir un Sistema de seguridad de la información implementado, estas fases del proceso poco se pueden observar; sin embargo, al hacer énfasis al verificar, cumple con un 1.3%, teniendo en cuenta que la Biblioteca no tiene la metodología documentada pero si realiza seguimiento a la seguridad de la información de manera empírica.

Tabla 6
Diagnóstico consolidado

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	1,5%
LOGRO2	HACER	40%	7,8%
LOGRO3	VERIFICAR	15%	1,3%
	ACTUAR	15%	0,0%
	TOTAL	100%	10,6%

Fuente. Autores del proyecto

En síntesis, una vez identificada la postura de seguridad para los procesos de misión crítica de la Biblioteca definidos en el alcance, se aclara la visión de construcción de un marco para la implementación de un SGSI en La Biblioteca Chaid Neme, teniendo en cuenta las debilidades encontradas, que permita materializar las intenciones de dar un manejo seguro a la información, reduciendo las posibles vulnerabilidades a las que se enfrenta a diario.

4.2 Establecer las políticas, procesos y procedimientos de seguridad necesarios para mitigar los riesgos y mejorar la seguridad de la información de la Biblioteca.

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las

políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

Importancia de las políticas de seguridad de la información. Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

Fases de implementación de las políticas de seguridad de información

Desarrollo de las políticas. En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos.

Justificación de la creación de política. Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

Alcance. Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

Roles y responsabilidades. Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

Revisión de la política. Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

Aprobación de la Política. Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

Cumplimiento. Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

Comunicación. Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los

funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

Monitoreo. Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

Mantenimiento. Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

Retiro. Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

Recomendaciones para la redacción de una política de seguridad de la información. A continuación se presenta una serie de recomendaciones para realizar redacción de políticas de seguridad y privacidad de la información en la Entidad:

La política debe tener como parte de su texto la declaración en la cual se indica ¿qué es lo que se desea hacer?, ¿qué regula la política?, ¿cuál es la directriz que deben seguir los funcionarios, contratistas y/o terceros?, todo esto alineado con la estrategia de la organización.

Alinearse con el alcance del Modelo de Seguridad y Privacidad de la Información.

Debe especificarse a quién (es) va dirigida la política, se debe identificar fácilmente quien (es) deben cumplir la política.

En los casos que aplique se hace referencia de la regulación mediante la cual se soporta la política.

En caso que aplique la política debe indicar las excepciones a la misma y a quienes les aplica la excepción.

- Datos de las personas o roles de la entidad que pueden brindar información sobre la política.
- Nombre, rol o responsable de quien autoriza la política.
- Describir los pasos y procedimientos para realizar ajustes a la política.
- Explicación de las consecuencias que se pueden tener en caso de que un funcionario, contratista o tercero incumpla la política.
- Fecha que inicia la vigencia de la política.

Es importante aclarar que una política NO es un estándar, es decir, no debe indicar como se ejecutará ninguna labor o control de manera específica, NO indica tecnologías específicas de uso. Son declaraciones muy generales y de alto nivel que plasman un objetivo a cumplir por parte de la organización.

Alcance. El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la BIBLIOTECA CHAID NEME, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar un acuerdo de confidencialidad, que los compromete con el cumplimiento de las políticas de seguridad aquí descritas. Los usuarios de los activos de información de la Entidad se han clasificado así:

- Colaboradores de Planta: se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.
- Funcionarios de la BIBLIOTECA CHAID NEME: Se definen como los empleados de la BIBLIOTECA CHAID NEME que son susceptibles de manipular sistemas de información.
- Contratistas: se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:

- Colaboradores en Misión;
- Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos;
- Personas naturales que prestan servicios independientes a la Entidad;
- Proveedores de recursos informáticos.

- Entidades de Control

- Procuraduría;

- Revisoría Fiscal;
- Contraloría General de la República;
-

- Otras Entidades

- DIAN;
- ICONTEC

Enunciado de aplicabilidad, los objetivos de control y los controles que son relevantes al SGSI de la organización.

Política de seguridad. Dentro de los apéndices (apéndice E), se puede detallar las políticas de seguridad a implementar, su aplicabilidad, objetivos de control y controles correspondientes.

El alcance y las políticas del sistema de gestión de seguridad de la información (SGSI) para la biblioteca Chaid Neme.

Introducción. Con el ánimo de mejorar la estrategia de Seguridad de la información de la Biblioteca Chaid Neme, en adelante La biblioteca, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos tecnológicos, buscando

niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

Objetivo. Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la BIBLIOTECA CHAID NEME establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

El presente documento define los lineamientos que debe seguir la BIBLIOTECA CHAID NEME con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

Requisitos legales y/o reglamentarios. Para la implementación de la estrategia de seguridad de la información, la BIBLIOTECA CHAID NEME debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las entidades que las regulan y aglutinan.

Definiciones. Para los propósitos de este documento se aplican los siguientes términos y definiciones:

Activo. Cualquier bien que tenga valor para la organización.

Acuerdo de Confidencialidad. Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la BIBLIOTECA CHAID NEME.

Administradores. Usuarios a quienes la BIBLIOTECA CHAID NEME ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la BIBLIOTECA CHAID NEME quienes estarán bajo la dirección de la Vicepresidencia de tecnología y soluciones de información de la Entidad.

Amenaza. Causa potencial de un incidente no deseado, que puede ocasionar daño o poner en riesgo a un sistema u organización.

Backup. Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

Coordinación de Planeación e Innovación. Es el responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como. COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.

Comité de Seguridad. Equipo de trabajo conformado por el presidente ejecutivo, coordinador de tecnología o los funcionarios que hagan sus veces.

Contraseña. Clave de acceso a un recurso informático.

Control. Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Directrices. Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

Servicios de procesamiento de información. Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

Seguridad de la Información. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio, trazabilidad y confiabilidad pueden estar involucradas.

Evento de seguridad de la información. Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Firewall. Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos no autorizados.

Incidente de seguridad de la información. Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información confidencial (RESERVADA). Información administrada por la BIBLIOTECA CHAID NEME en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.

Información confidencial (CONFIDENCIAL). Información generada por la BIBLIOTECA CHAID NEME en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO). Información generada por la BIBLIOTECA CHAID NEME en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

Información pública. Es la información administrada por la BIBLIOTECA CHAID NEME en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.

LAN. Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).

Licencia de Software. Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.

Copyright. Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras

formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.

Propiedad Intelectual. Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.

Open Source (Fuente Abierta). Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.

Software Libre. Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.

Software pirata. Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley. Software de Dominio Público. Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.

Freeware. Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.

Shareware. Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.

Módem (Modulador - Demodulador de señales). Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.

Monitoreo. Verificación de las actividades de un usuario con respecto a los recursos informáticos de La biblioteca.

OTP (One Time Password). Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

Plan de contingencia. Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de La biblioteca en casos de desastres y otros casos que impidan el funcionamiento normal.

Política. Toda intención y directriz expresada formalmente por la dirección.

Protector de pantalla. Programa que se activa a voluntad del usuario, ó automáticamente después de un tiempo en el que no ha habido actividad.

Proxy. Servidor que actúa como puerta de entrada a la Red Internet.

Recursos informáticos. Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.

Riesgo. Combinación de la probabilidad de un evento y sus consecuencias.

Análisis de Riesgos. Uso sistemático de la información para identificar las fuentes y estimar el riesgo. Evaluación de Riesgos. Todo proceso de análisis y valoración del riesgo.

Valoración del riesgo. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Router. Equipo que permite la comunicación entre dos o más redes de computadores.

Sesión. Conexión establecida por un usuario con un Sistema de Información.

Sistema de control de acceso. Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.

Sistema de detección de intrusos (IDS). Es un conjunto de hardware y software que ayuda en la detección de accesos ó intentos de acceso no autorizados a los recursos informáticos de La biblioteca.

Sistema de encriptación. Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.

Sistema multiusuario. Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.

Sistema operativo. Software que controla los recursos físicos de un computador.

Sistema sensible. Es aquel que administra información confidencial ó de uso interno que no debe ser conocida por el público en general.

Tercera parte. Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

Usuario. Toda persona que pueda tener acceso a un recurso informático de la BIBLIOTECA CHAID NEME

Usuarios de red y correo. Usuarios a los cuales la BIBLIOTECA CHAID NEME les entrega un identificador de cliente para acceso a sus recursos informáticos.

Usuarios externos. Son aquellos clientes externos que utilizan los recursos informáticos de la BIBLIOTECA CHAID NEME a través de Internet ó de otros medios y tienen acceso únicamente a información clasificada como pública.

Usuarios externos con contrato. Usuarios externos con los cuales la BIBLIOTECA CHAID NEME establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.

Vulnerabilidad. Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Responsable. Compromiso de la dirección

- La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información.
- Mediante el establecimiento de una política de seguridad de la información;
- Asegurando que se establezcan objetivos y planes de seguridad de la información; o Estableciendo funciones y responsabilidades de la seguridad de la información;
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidades de la mejora continua;
- Asegurando que se realizan auditorías internas.

Gestión de los recursos

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de

la misión y visión de la BIBLIOTECA CHAID NEME.

- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales; o Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.

Procedimiento. Comunicación de las políticas de seguridad.

Los miembros del Comité de Seguridad, conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

Aplicación de las políticas de seguridad.

Las políticas de seguridad informática se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

Políticas de seguridad de la BIBLIOTECA CHAID NEME. Este claustro bibliográfico reconoce abiertamente la importancia de la seguridad de la información así como la necesidad de

su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la BIBLIOTECA CHAID NEME con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

Políticas generales de seguridad de la información. Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en.

a) Directrices de la organización en seguridad de la información.
b) Aspectos organizativos de la seguridad de la información.
c) Seguridad ligada a los recursos humanos.

d) Gestión de activos.

e) Control de accesos.

f) Cifrado.

g) Seguridad física y ambiental.

h) Seguridad en la operativa.

i) Seguridad en las telecomunicaciones.

j) Adquisición, desarrollo y mantenimiento de los sistemas de información.

k) Relaciones con suministradores.

l) Gestión de incidentes en la seguridad de la información.

m) Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

n) Cumplimiento.

Dispositivos para movilidad y teletrabajo.

Dispositivos móviles. Al interior de la BIBLIOTECA CHAID NEME, se reconoce el alto grado de exposición que presenta la información y los datos de la institución almacenados en dispositivos móviles (computadores portátiles, notebooks, PDA, Smartphone, entre otros.). Corresponde a la dirección administrativa y funcionarios gestores de los recursos tecnológicos, elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad de la información en materia de redes.

- Los usuarios necesitaran permiso para instalar o desinstalar aplicaciones en los dispositivos móviles. Que sean de propiedad de la organización, No se les permite acceder al sistema y a las aplicaciones virtuales de las máquinas.
- No acceder a los enlaces solicitados a través de SMS/MMS/Email podría ser código malicioso.

- La configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área asignada para tal fin.

- Para computadores portátiles, lo recomendable es que los usuarios pertenezcan al dominio de red existente en la organización, con políticas de complejidad y caducidad adecuadas. En el caso de teléfonos móviles/tablets, el PIN o contraseña del dispositivo debe, al menos, existir. En el caso de dispositivos Android, deben evitarse los controles de acceso basados en patrones de puntos, siendo lo más deseable el control biométrico por huella dactilar, en aquellos dispositivos que lo soporten. En caso que sea necesario un PIN o contraseña, se recomienda forzar teclado alfanumérico, y cierta complejidad en la contraseña exigiendo letras minúsculas, mayúsculas y números, así como el bloqueo temporal según se va fallando en la autenticación. En algunos dispositivos con

información muy sensible, podría Activarse incluso el check de borrado completo del dispositivo si hay 10 fallos seguidos en la autenticación.

Tanto en computadores portátiles como en Smartphone y tablets, habrá de activarse las políticas de bloqueo de sesión (o de apagado de pantalla) solicitando autenticación o PIN para volver a interactuar con el dispositivo. El periodo máximo de inactividad antes de dicho bloqueo se recomienda que se fije en 1 minuto para Smartphone y tablets, así como 3 minutos para computadores portátiles.

Tapar físicamente las cámaras integradas, el malware de hoy en día permite activar la webcam incorporada en dispositivos móviles a voluntad del atacante, por lo que es posible disponer de una cámara y un micrófono de forma remota, escuchando y viendo al usuario. A fin de proteger la privacidad del usuario, así como de la información hablada por su parte (y que pueda ser monitorizada en remoto, a través del micrófono), se recomienda bloquear físicamente la webcam con cinta aislante negra, con la opacidad necesaria para que no se pueda ver nada. Igualmente, en computadores portátiles, se recomienda desactivar el micrófono incorporado en el equipo

Computación en nube. la información producida por los procesos de l la BIBLIOTECA CHAID NEME, no debe ser alojada en dispositivos de almacenamiento en la nube, ya que se expondría a afectarse la integridad y confidencialidad de los datos, en caso tal de contratarse un servicio de cloud computing para la institución, podrán alojarse los archivos que requieran copias de seguridad, almacenamiento y difusión masiva.

Política de uso de portátiles.

- Protección de la información
- El antivirus siempre debe estar activo y actualizado
- No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de la biblioteca
- Seguir las políticas de acceso remoto
- Toda la información que es confidencial debe estar cifrada.
- Cuando el equipo deba ser devuelto a la BIBLIOTECA CHAID NEME para reparación, mantenimiento etc. La información confidencial deberá respaldarse en una copia de seguridad y posteriormente borrada.
- De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas
- Protección del equipo portátil
- No dejar el computador móvil en lugares públicos
- Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su equipaje mano.
- No es permitido que el computador portátil sea utilizado por familiares y/o amigos

Seguridad ligada a los recursos humanos. Se debe considerar como recurso humano a todo el personal interno, externo, temporal en el aseguramiento de las responsabilidades que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de Hurto, fraude, sabotaje o uso inadecuado de los activos de información.

Todos y cada uno de los individuos que conforman la organización deben estar conscientes de las vulnerabilidades y amenazas que afectan la seguridad de la información y sus obligaciones y deberes en cuanto a acatar la política de seguridad de la organización; establecida para la reducción del riesgo de error humano.

La responsabilidad de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

Cuando un usuario inicie su relación laboral con la BIBLIOTECA CHAID NEME se debe diligenciar el documento de entrega de inventario.

Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

Cuando un funcionario de la BIBLIOTECA CHAID NEME inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

Antes de la contratación. Para toda persona que ingrese a la BIBLIOTECA CHAID NEME, la dirección administrativa debe asegurar las responsabilidades sobre seguridad de la información de manera previa a la contratación. Así mismo incluir un acuerdo de confidencialidad, Esta tarea debe reflejarse en una adecuada descripción del cargo, funciones, investigación de antecedentes y en los términos y condiciones de la contratación.

Durante la contratación. Definición de las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de los empleados la BIBLIOTECA CHAID NEME.

A todos los usuarios empleados, contratistas y terceras personas se les proporcionará un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad de la información y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de mitigar los posibles riesgos de seguridad.

Se deberá establecer un proceso disciplinario normal para gestionar las brechas en seguridad.

Se debe realizar una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.

Cese o cambio de puesto de trabajo. La dirección debe asegurar que todos los funcionarios, que no laboren más en la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que la institución lo considere conveniente, incluso después de la finalización del puesto de trabajo o del contrato; también que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.

Se debe realizar devolución de los activos de la organización por parte de los empleados responsables, para esto se debe verificar el inventario de activos regularmente.

Examinar qué accesos necesita revocar apremiantemente y priorizada mente.

Realizar un seguimiento del uso del e-mail de estas personas antes de salir definitivamente de la empresa, para evitar fuga confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).

Acuerdo de confidencialidad. Para el uso de los recursos tecnológicos las bibliotecas, todo usuario debe firmar un acuerdo de confidencialidad (Anexo G) y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware.

Cada dependencia debe operar bajo término de perfiles que asocien a los usuarios con sus respectivas funciones y tareas, estos deben predefinirse y actualizarse por cada estamento

organizativo; cada usuario debe cumplir con unos parámetros de buenas prácticas de seguridad de la información, descritos a continuación los usuarios deben portar dentro de las instalaciones de la institución un carné que los identifique como funcionarios y/o contratistas.

- Cada usuario que se denomine como personal interno será responsable por el mal uso del equipo de cómputo en el cual realiza sus tareas, incluyendo infecciones de virus.

- Los usuarios no deben bajo ninguna circunstancias descargar de internet archivos, que pudiera ser considerado pornográfico, difamatoria, racista, videos, música, entre otros. o que atente contra las buenas costumbres o principios, excepto que sus funciones administrativas así lo amerite.
- Los usuarios no deben utilizar los dispositivos electrónicos propios de la institución para su uso personal, es por ello que no deberán acceder desde estos a redes sociales ni correos electrónicos personales.

- Todos los usuarios deben realizar el envío de información únicamente a través del correo institucional.

- Se plantea que los usuarios que se adscriben como personal interno deben utilizar cuentas de usuario para acceso al sistema de los computadores a su cargo.

- Los usuarios no deben utilizar memorias USB para el tránsito de información en los equipos de cómputo propios de la entidad.

Responsabilidades de usuarios externos. Se entiende por usuario externo a las personas que hagan parte de organizaciones externas que tengan convenios o relaciones con la biblioteca. Todos los usuarios denominados como externos o terceros y personal de empresas externas, deben estar autorizados por un miembro del personal de la organización, quien será responsable del control y vigilancia del uso adecuado de la información y los recursos tecnológicos institucionales, del uso que estos tengan; ellos deben acatar los siguientes reglamentos.

Registro de las compañías que reciben información privada.

El personal de la BIBLIOTECA CHAID NEME que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

Transferencia de la custodia de información de un funcionario que deja biblioteca.

Cuando un empleado se retira de la BIBLIOTECA CHAID NEME, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

Gestión de activos.

Responsabilidad sobre los activos.

- Mantener la protección adecuada de los activos de la organización.
- Todos los activos se deben incluir en el inventario y deben tener un propietario designado.
- Se deben identificar los propietarios para todos los activos y asignar la responsabilidad para el mantenimiento de los controles. La implementación de los controles específicos puede ser delegada por el propietario según el caso, pero él sigue siendo responsable de la protección adecuada de los activos.
- Los recursos informáticos de la BIBLIOTECA CHAID NEME, dispuestos para la operación registral, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de la biblioteca usuaria de este servicio. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización de la Presidencia.
- El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica en línea, debe someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

Clasificación de la Información

- La información se debe clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

- La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se debe utilizar un

esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

- Toda la información generada por la Organización debe estar disponible para funcionarios tanto externos como internos que requieran del acceso y consulta de ésta, siempre y cuando se manejen los controles de acceso y confidencialidad apropiados.
- Se deben asignar responsabilidades en cuanto a la propiedad de los activos de información a usuarios encargados de mantener la integridad de la información. Es responsabilidad del administrador de la información asignar los respectivos controles de acceso a la información.

- Eliminación Segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por La biblioteca, antes de su entrega se les realizara un proceso de borrado seguro en la información.

- Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el comité de seguridad.

Manejo de los soportes de almacenamiento.

- Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores

de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio.

- Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados.

Control de accesos.

Política de control de acceso. Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. Los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de La biblioteca.

El acceso de los usuarios a los sistemas de información y acceso al sistema debe estar controlado y gestionado por perfiles de usuarios y contraseñas de accesos a dichos sistemas, El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales. Por consiguiente se deben tener en cuenta los siguientes parámetros.

- Cada usuario es responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, su nombre de usuario y contraseña necesarios para acceder al

sistema, grupo de trabajo y/o dominio de red, por lo que se deberá mantener de forma confidencial.

Política de contraseñas. La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

- Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.

- La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

- Todos los usuarios deben cambiar su contraseña por lo menos una vez cada 30 días.

- Bajo ninguna circunstancia los usuarios deberán guardar sus contraseñas, en ningún tipo de papel, agenda, entre otros.

- Una contraseña para ser considerada segura debe poseer las siguientes características. Longitud, Las contraseñas deben tener como mínimo 8 caracteres de extensión, aleatoriedad. Una contraseña debe ser difícil de descifrar. Se deben utilizar combinaciones de palabras y

números, fechas entre otros., Complejidad. se deben utilizar una mezcla de números y letras, signos de puntuación, caracteres especiales, mayúsculas y minúsculas en sus contraseñas; Exclusividad. se debe utilizar una contraseña por cada uno de las cuentas de usuario y correos electrónicos que utilice; Actualización. Las contraseñas deben ser cambiadas cada 2 o 3 meses, Gestión. los usuarios no deben dar a conocer sus contraseñas, ni plasmarlas en ningún documento o apuntador ya sea físico o digital, ni pegarlas en los monitores, debajo de los teclados, tampoco en un fichero de texto que lleve el nombre contraseñas.

- No se debe revela la contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.

- No se debe compartir la contraseña con familiares y/o amigos.

- No se debe utilizar la característica de "Recordar o guardar Contraseña".

- Se recomienda no incluir en las contraseñas datos personales, tampoco nombre de familiares, ni de mascotas.
- Se debe evitar compartir la contraseña en respuesta a un ejemplo de petición por correo electrónico o por teléfono, para verificar su identidad, incluso si parece ser de una compañía o persona de confianza.

Cifrado. Proteger la confidencialidad, autenticidad o integridad de la información que se envía y se recibe, aplicando controles criptográficos.

Se recomienda utilizar un sistema de cifrado en pre-boot, que pida una contraseña de acceso y descifrado del disco duro. De esta manera, en caso de pérdida o Hurto, no servirá para nada extraer el disco duro y montarlo desde otra plataforma puesto que el mismo estará cifrado completamente. En Microsoft Windows se encuentra la herramienta Bitlocker. Así mismo puede utilizarse Truecrypt como alternativa, aunque es recomendable Bitlocker por estar soportada por Microsoft de forma corporativa. En caso que no se desee hacer un cifrado completo del disco, al menos será altamente recomendable que la información tratada en local se guarde en un contenedor cifrado. Para este fin, se recomienda la utilización de soluciones como Truecrypt, compatible con sistemas operativos Windows, Mac y Linux.

- Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD´s, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

- Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

Seguridad física y ambiental.

Áreas Seguras. Evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

Los servicios de procesamiento de información sensible o crítica deben estar ubicados en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados, Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia.

La protección suministrada debe estar acorde con los riesgos identificados.

Seguridad de los Equipos. Evitar pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.

Los equipos deberían estar protegidos contra amenazas físicas y ambientales.

La protección del equipo (incluyendo el utilizado por fuera) es necesaria para reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño. También se debería considerar la ubicación y la eliminación de los equipos. Es posible que se requieran controles especiales para la protección contra amenazas físicas y para salvaguardar los servicios de soporte tales como energía eléctrica e infraestructura de cableado.

Los equipos que hacen parte de la infraestructura tecnológica de la BIBLIOTECA CHAID NEME, tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados

y protegidos adecuadamente para prevenir la pérdida, daño, Hurto o acceso no autorizado a los mismos. De igual manera, se deben adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los equipos servidores, dispositivos activos de red que contengan información y servicios de carácter institucional, deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su sesión. Todos los usuarios deben bloquear la sesión al retirarse de los dispositivos.
- No se deben introducir dispositivos extraíbles como memorias USB, cámaras, entre otros. ya que pueden ser portadores de software malicioso y además se pueden utilizar para copiar información sensible de la biblioteca.
- En caso de daño o mantenimiento se debe tener cuidado con el proceso desinstalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. Garantizar la

protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o Hurto.

Los equipos de cómputo deben estar correctamente protegidos y controlados por personal de la institución el cual debe tener conocimiento acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información de la institución.

Sistema de vigilancia con cámaras de seguridad. Éste sistema deberá desarrollarse por las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones a la seguridad y tranquilidad en lo relacionado con la vida y los bienes propios o de terceros y la fabricación, comercialización, instalación y utilización de equipos para la vigilancia y seguridad privada, blindajes y transporte con este mismo fin.

- Se deben establecer las zonas bajo video vigilancia en donde estarán instaladas las cámaras, éstas se ubicaran dentro y fuera del edificio es decir en la entrada principal, pasillos, biblioteca, aulas de clase que hay dentro de la biblioteca, áreas de acceso restringido,
- El sistema de video vigilancia se empleara únicamente a efectos de protección y seguridad. El sistema contribuye a garantizar la seguridad tanto de los edificios de la organización, su personal y visitantes como de los bienes contenidos en sus instalaciones y la información allí almacenada.

- En caso de necesidad, se recomienda contemplar y complementar con otros sistemas de seguridad físicos, por ejemplo sistemas de control de acceso y sistemas de detección de intrusiones.

- El sistema no deberá ser usado para ningún otro fin distinto, como por ejemplo vigilar el trabajo de los funcionarios u otros miembros del personal. El sistema se utilizará como herramienta de investigación o como prueba en investigaciones internas o procedimientos disciplinarios cuyo propósito exclusivo sea investigar un incidente de seguridad física.

Seguridad en la operativa. Protección contra software malicioso y *hacking**:** todos los sistemas informáticos utilizados en la entidad deben ser protegidos teniendo en cuenta las diferentes áreas que involucre controles humanos, físicos técnicos y administrativos; se deben implementar medidas que mitiguen los riesgos asociados a amenazas de software malicioso y técnicas de hacking.

La BIBLIOTECA CHAID NEME, establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la Dirección administrativa autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente. Sobre el particular se establece los siguientes lineamientos.

- No se permite la desinstalación y/o desactivación de software y herramientas de seguridad.

- No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- No se permite utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo o avalado por la administración de la institución.
- En caso de presentarse fallas en la transmisión por medio de la red de datos de la institución, se debe informar a la persona encargada de administrar la red, y este deberá aplicar las medidas correctivas para descartar posibles intrusiones realizando seguimiento al tráfico de la red, y en caso de detectarse se deberá tomar medidas en el caso.

Recursos compartidos. Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio.

- Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.
- Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.
- Acceso no autorizado a los sistemas de información de la Entidad.
- Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de cifrado y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.
- Posibilidad de acceso no implica permiso de uso.

- Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.
- Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.
- A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al comité de seguridad.
- Manejo de sesiones en sistemas informáticos
- Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.
- Notificación de sospecha de pérdida, divulgación ó uso indebido de información.
- Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del comité de seguridad.
- Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores.
- Toda la información que sea crítica para la organización debe ser etiquetada de acuerdo a los niveles establecidos en el presente documento. USO INTERNO y CONFIDENCIAL.
- Control de recursos informáticos entregados a los usuarios.
- Cuando un usuario inicie su relación laboral con biblioteca se debe diligenciar el documento de entrega de inventario.
- Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso

tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

- Cuando un funcionario de La biblioteca inicie su relación laboral se debe diligenciar el documento de entrega de inventario.
- Configuración de sistema operativo de las estaciones de trabajo.
- Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.
- Apagado de equipos en la noche
- Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche.
- Tiempo limitado de conexión en aplicaciones de alto riesgo
- Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.
- Bloqueo estación de trabajo.
- Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min. Por otra parte el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente necesaria para la labor desempeñada.
- Ambientes separados de producción y desarrollo.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción.

Cumplimiento del procedimiento para cambios y/o actualizaciones. Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluados en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

Documentación de cambios y/o actualizaciones. Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

Catalogación de programas. Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa

Prueba por parte del área encargada.

- Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.
- Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.
- Dependencia de la autenticación de usuario en el sistema operativo.

Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

Incorporación de contraseñas en el software. Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por la BIBLIOTECA CHAID NEME o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política "Cambios periódicos de contraseñas".

Acceso del usuario a los comandos del sistema operativo. Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

Se requieren registros de auditoria en sistemas que manejan información sensible.

Todo sistema que maneje información sensible para la BIBLIOTECA CHAID NEME debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

Registros para los usuarios privilegiados en los sistemas en producción que lo permitan. Toda actividad realizada en los sistemas por usuarios con privilegios de

administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alterno de control.

Los registros del sistema deben incluir eventos relevantes para la seguridad. Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

Resistencia de los registros contra desactivación, modificación y eliminación. Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

Procesos controlados para la modificación de información del negocio en producción. La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Presidencia.

Validación de entradas en los desarrollos. El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

Diseño de seguridad para aplicaciones. El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para la BIBLIOTECA CHAID NEME.

Personas autorizadas para leer los registros de auditoria. Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoria interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

Archivo histórico de contraseñas. En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada (ver política "Las contraseñas creadas por usuarios no deben ser reutilizadas") y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

Políticas para administradores de sistemas

Soporte para usuarios con privilegios especiales. Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad. Todos los privilegios sobre los recursos informáticos de la BIBLIOTECA CHAID NEME otorgados a un

usuario deben eliminarse en el momento que éste abandone la Entidad y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

Cuando y como pueden asignar contraseñas los administradores. Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

Límite de intentos consecutivos de ingreso al sistema. El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados. a) ser suspendido hasta nueva reactivación por parte del administrador; b) ser temporalmente bloqueado (no menos de 5 minutos); c) ser desconectado si se trata de una conexión telefónica.

Cambio de contraseñas por defecto. Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política “Contraseñas fuertes”.

Cambio de contraseñas después de compromiso detectado en un sistema multiusuario. Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

Administración de los buzones de correo. Los administradores deben establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico, mensualmente se realizará una revisión de control sobre cada uno de los buzones creados para determinar cuáles requieren una depuración para que no alcancen su límite de espacio asignado.

Brindar acceso a personal externo. El ingeniero de soporte y web master velará porque individuos que no sean empleados, contratistas o consultores de la BIBLIOTECA CHAID NEME no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Presidencia o el comité de seguridad.

Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado. Antes de otorgarle acceso a un tercero a los recursos tecnológicos de la BIBLIOTECA CHAID NEME se requiere la firma de un formato, acuerdo o autorización de la direccion. Es obligatoria la firma del acuerdo de confidencialidad.

Restricción de administración remota a través de Internet. La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para cifrado del canal de comunicaciones.

Dos usuarios requeridos para todos los administradores. Administradores de sistemas multiusuarios deben tener dos identificaciones de usuario una con privilegios de administración y otra con privilegios de usuario normal.

Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito. Sin autorización escrita Dirección de TI de la biblioteca, los administradores no deben otorgarle privilegios de administración a ningún usuario.

Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado. Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

Remoción de software para la detección de vulnerabilidades cuando no esté en uso. Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas o en cifrado del software como tal.

Manejo administrativo de seguridad para todos los componentes de la red. Los parámetros de configuración de todos los dispositivos conectados a la red de La biblioteca deben cumplir con las políticas y estándares internos de seguridad.

Información a capturar cuando un crimen informático o abuso es sospechado. Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea.

La información a recolectar incluye configuración actual del sistema, copias de seguridad y todos los archivos potencialmente involucrados.

Sincronización de relojes para un registro exacto de eventos en la red. Los dispositivos multiusuario conectados a la red interna de la BIBLIOTECA CHAID NEME deben tener sus relojes sincronizados con la hora oficial.

Revisión regular de los registros del sistema. El área de sistemas debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

Confidencialidad en la información relacionada con investigaciones internas. Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

Información con múltiples niveles de clasificación en un mismo sistema. Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

Segmentación de recursos informáticos por prioridad de recuperación. Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero. Todos los

departamentos deberán usar el mismo marco para preparar los planes de contingencia a los sistemas de información.

Software de identificación de vulnerabilidades. Para asegurar que el equipo técnico de la BIBLIOTECA CHAID NEME ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de Cortafuegos y Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS (Instrusion Detection System), detección de virus y bloqueo de correo no deseado.

En dónde usar controles de acceso para sistemas informáticos. Todo computador que almacene información sensible de la Biblioteca, debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales. Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

Habilitación de Logs en Sistemas y Aplicaciones. Se debe habilitar la gestión de logs (archivos de transacción) en los sistemas y aplicaciones críticas de la BIBLIOTECA CHAID NEME

Monitoreo de Sistemas. Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

Mantenimiento de los Sistemas. Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de la BIBLIOTECA CHAID NEME

Verificación física de equipos críticos. Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.

Copias de seguridad. Se deben elaborar más de una copia de seguridad con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

Período de almacenamiento de registros de auditoria. Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

Tipo de datos a los que se les debe hacer backup y con qué frecuencia. A toda información sensible y software crítico de la BIBLIOTECA CHAID NEME residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el

procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

Seguridad en las telecomunicaciones. Se debe garantizar que el servicio de red utilizado por La biblioteca se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el comité de seguridad puede efectuar escaneos de la red con la finalidad de resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

Revisión de accesos de usuarios. Se debe realizar por control de auditoría la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

Gestión de la seguridad en las redes. La configuración de los dispositivos activos de red, debe estar siempre documentada, se deberá tener copia de respaldo de las configuraciones. Todos los equipos de tecnología deben estar registrados y aplicarles permanentemente mantenimientos preventivos.

Para el fin pertinente se deben cumplir las siguientes premisas.

- Impedir el acceso del personal no autorizado a los servicios en red.
- Se deberán controlar los accesos a servicios internos y externos conectados en red.
- Se deberán emplear mecanismos de autenticación adecuados que se apliquen a los usuarios y

equipos. Los métodos de autenticación que pueden tener son. implementación de redes locales virtuales, filtrado de direcciones IP a nivel de Host o Subredes.

- El encargado de administrar la red deberá llevar estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).
- Se deberá realizar segmentación de dominios de broadcast, para separar cada instancia de la biblioteca, fraccionando un segmento para funcionarios, docentes, estudiantes, invitados; esto deberá aplicar para la red cableada e inalámbrica y un segmento para Smartphone.
- Se deben tener grupos de trabajo o dominios de red para los usuarios de orden administrativo.
- Hacer o intentar hacer cualquier cosa que afecte negativamente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas.
- Acceder al sistema o red, monitorear datos o tráfico.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Atentar contra la vulnerabilidad del sistema o redes.
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.
- Navegación en internet. el uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la biblioteca y debe ser utilizado por los usuarios para realizar las funciones establecidas para su rol, por lo cual se definen los siguientes parámetros para su uso.
- Abstenerse de acceder a sitios web que salten la seguridad del servidor de acceso a Internet (proxy) o intentar hacerlo.

- No se deberá descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- No se permitirá el acceso y el uso de mensajería instantánea como Facebook, Yahoo, Skype, twitter y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades de la organización.
- No se podrá realizar La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y personal encargado de los recursos tecnológicos, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- Todos los usuarios de la biblioteca, deben ser responsables de dar uso adecuado a este

recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

- Correo electrónico. todos los usuarios a los que se les sea asignada una cuenta de correo electrónico de carácter institucional deberán responsabilizarse de su uso, de todos los mensajes y archivos transmitidos y recibidos; así mismo esta debe ser usada solo para envío y recepción de información de índole corporativa, no se permitirá el uso y acceso de correo electrónicos de otro tipo dentro del ámbito institucional. Los usuarios deberán tener en cuenta lo siguiente.

- Los mensajes y la información contenida en los buzones del correo electrónico son propiedad de la biblioteca, y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- No se permitirá enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- No se permite la utilización de la dirección de correo electrónico de la biblioteca, como punto de contacto en comunidades interactivas, redes sociales, tales como Facebook, twitter, entre otras, o cualquier otro sitio que no tenga que ver con las actividades institucionales.
- No se deberá realizar envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- No se deben enviar archivos de música y videos. En caso de requerir hacer un envío de este

tipo de archivos deberá ser exclusivamente de contenido didáctico y/o educativo.

- Los usuarios de la biblioteca, deben evitar la utilización de la cuenta de correo electrónico institucional para el envío o reenvío de mensajes spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), hoax (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros usuarios o que sea contrario a las políticas y normas institucionales.
- La contraseña de acceso al correo electrónico, debe ser cambiada periódicamente por cada usuario.
- Los usuarios no deberán abrir enlaces sospechosos llegados por correos electrónicos por ejemplo de bancos, tiendas, entre otros. ya que pueden ser víctimas de phishing.
- No completar datos personales en mensaje de correos electrónicos sospechosos.
- Eliminar periódicamente los correos no deseados (spam o sospechoso).
- Prohibición de uso de Internet para propósitos personales. El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política “Instrucciones para el uso de recursos informáticos”.
- Formalidad del correo electrónico. Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.
- Preferencia por el uso del correo electrónico. Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
- Uso de correo electrónico. La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro usuario.

- Revisión del correo electrónico. Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.
- Mensajes prohibidos. Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros ó que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.
- Acciones para frenar el SPAM. En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas.
- Todo buzón de correo debe tener un responsable. Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.
- Enviando software e información sensible a través de Internet. Software e información sensible de La biblioteca que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.
- Intercambio de información a través de Internet. La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

Recursos tecnológicos. La instalación o desinstalación de cualquier elemento software o hardware en los equipos de cómputo de la organización, es responsabilidad del funcionario

encargado del manejo de los elementos tecnológicos, y por tanto será el único autorizado para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la institución a través de la Dirección.

- Los usuarios no deberán realizar modificaciones en los dispositivos de cómputo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales del dispositivo, fondo de escritorio y protector de pantalla institucional, entre otros. Estos cambios pueden ser realizados únicamente por el funcionario encargado de los recursos de Tecnología.
- Sólo usuarios autorizados pueden realizar actividades de administración remota de dispositivos de red, equipos de cómputo o servidores de la infraestructura de procesamiento de información de la biblioteca; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración que garanticen los principios básicos de seguridad de la información.
- No se permitirá la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. Deben haber constantes revisiones para verificar lo anterior expuesto y en caso de detectarse un evento de este tipo se deberá proceder a desinstalar el material encontrado y tomar las medidas correctivas correspondientes.

Políticas de uso de firewall.

Detección de intrusos. Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

Toda conexión externa debe estar protegida por el firewall. Toda conexión a los servidores de la BIBLIOTECA CHAID NEME proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

Toda conexión hacia Internet debe pasar por el Firewall. El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

Filtrado de contenido activo en el Proxy. La dirección de TI de las bibliotecas, debe asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como applets de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de La biblioteca

Firewall debe correr sobre un computador dedicado o appliance. Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

Inventario de conexiones. Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

El sistema interno de direccionamiento de red no debe ser público. Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

Revisión periódica y reautorización de privilegios de usuarios. Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios a la Presidencia.

Datos sensibles enviados a través de redes externas deben estar encriptados. Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

Sincronización de relojes para un registro exacto de eventos en la red. Los dispositivos multiusuario conectados a la red interna de La biblioteca deben tener sus relojes sincronizados con la hora oficial.

Reglas de uso de la Intranet. La BIBLIOTECA CHAID NEME utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o

trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

Prohibición de publicitar la imagen de la BIBLIOTECA CHAID NEME en sitios diferentes a los institucionales. La publicación de logos, marcas o cualquier tipo de información sobre la BIBLIOTECA CHAID NEME o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización de la Presidencia. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

Prohibición establecer conexiones a los sitios Web de la BIBLIOTECA CHAID NEME. Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de la BIBLIOTECA CHAID NEME por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización de la Presidencia, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

Prohibición de anuncios en sitios Web particulares. Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados de la BIBLIOTECA CHAID NEME o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con la BIBLIOTECA CHAID NEME

Adquisición, desarrollo y mantenimiento de los sistemas de información. Adquisición, Desarrollo y Mantenimiento de Sistemas Software.

- Garantizar que la seguridad sea una parte integral de los sistemas de información.
- Se debe realizar un estudio de necesidades para así preparar el plan de desarrollo tecnológico.
- Se debe asegurar de que los programas desarrollados o adquiridos provean medidas de control o, de interoperabilidad con otros sistemas. Con este fin, el personal encargado del desarrollo o adquisición de programas o de otros componentes de programación debe tomar en cuenta que. Sean compatibles con el equipo existente o cumplan con las especificaciones mínimas del proponente de la programación, Provean crecimiento, flexibilidad y adaptabilidad, sean funcionales en arquitectura; Existan maneras de controlar la creación y privilegios de los usuarios.
- El software de aplicaciones y software de base sólo debe ser puesto en producción después de ser probado; se deben incluir pruebas sobre la funcionalidad, la seguridad, los efectos sobre otros sistemas y las facilidades de usuario, y deben ser realizadas en ambiente de pruebas.

Relaciones con suministradores.

Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado. Antes de otorgarle acceso a un tercero a los recursos tecnológicos de la BIBLIOTECA CHAID NEME se requiere la firma de un formato, acuerdo o autorización de la Presidencia. Es obligatoria la firma del acuerdo de confidencialidad.

Acuerdos con terceros que manejan información o cualquier recurso informático de la BIBLIOTECA CHAID NEME. Todos los acuerdos relacionados con el manejo de información o de recursos de informática de la BIBLIOTECA CHAID NEME por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a La biblioteca ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de la BIBLIOTECA CHAID NEME.

Definición clara de las responsabilidades de seguridad informática de terceros. Socios de negocios, proveedores, clientes y otros asociados a los negocios de la BIBLIOTECA CHAID NEME deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con la BIBLIOTECA CHAID NEME y verificada por la Presidencia, el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante su estadía en las instalaciones de la BIBLIOTECA CHAID NEME, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados.

Uso del aplicativo entregado. La BIBLIOTECA CHAID NEME ha suscrito con los fabricantes y proveedores un contrato de “LICENCIA DE USO” para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a la BIBLIOTECA CHAID NEME Adicional a esto cada usuario, dependiendo

de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados. Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más.

La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la BIBLIOTECA CHAID NEME.

Gestión de incidentes en la seguridad de la información

Comité de Seguridad de la información. El comité está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia con respecto al programa de seguridad de la información dentro de la organización.

El comité debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad De la información, dentro de la Entidad.

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización. Revisión y valoración de la Política de Seguridad de la Información.

- Alineación e integración de la seguridad a los objetivos del negocio.

- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización. Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.

- Reportar, a través de reuniones semestrales a la Presidencia el estado de la seguridad y protección de la información en la compañía y la necesidad de nuevos proyectos en temas de seguridad de la información

- Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información

- Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.
- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la

organización.

- Supervisar y controlar de los cambios significativos en la exposición de los activos de información a las principales amenazas. Revisar y seguir los incidentes de seguridad de la información.

- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la compañía.

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda).

- Mejoras en las actividades inherentes a la Seguridad de la BIBLIOTECA CHAID NEME y sus procesos.

- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de la BIBLIOTECA CHAID NEME

- Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.

Cambio en los roles del ciclo de certificación.

- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de la BIBLIOTECA CHAID NEME, El Presidente Convoca al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

- Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por todos su miembros.

- Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

▪ Oficial de Seguridad de la Información

Oficial de Seguridad de la Información (Jefe de Riesgos o persona designada para los temas de seguridad de la Entidad).

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.

- Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base

este mapa para cualquier proyecto nuevo que se implemente.

- Dirigir el programa de manejo y seguimiento de incidentes.

- Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía. Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.
- Crear y mantener un Programa de Concientización en seguridad de la información.

- Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

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.

- Procedimientos de contingencia. Los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.

- Procedimientos de retorno. Los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.

- Procedimientos de recuperación. Los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.

- Actualización periódica. El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad. Un análisis de impacto al negocio debe ser realizado como mínimo una vez al año, con el objeto de determinar la necesidad de la disponibilidad de la información en el grado y escala de tiempo requeridos después de una interrupción de las funciones críticas de la Organización.

- El Plan de Continuidad debe estar alineado con los riesgos identificados que puedan causar interrupción al servicio. Para este caso, se debe tener en cuenta las posibles consecuencias para la seguridad de la información.

Políticas generales de la presidencia

Evaluación y tratamiento del riesgo. La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deben guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos de la BIBLIOTECA CHAID NEME por lo menos una vez al año utilizando el procedimiento Interno. “Análisis de riesgos”

Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos. No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Presidencia.

Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados. Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la Entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

Entrenamiento compartido para labores técnicas críticas. Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de la BIBLIOTECA CHAID NEME.

Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias. Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor. La contingencia de sistemas que se acuerdan con terceros deberá disponer de una infraestructura y de un modelo de soporte acorde a las necesidades de la BIBLIOTECA CHAID NEME

Personal competente en el Centro de Cómputo para dar pronta solución a problemas. Con el fin de garantizar la continuidad de los sistemas de información, la BIBLIOTECA CHAID NEME deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

Chequeo de virus en archivos recibidos en correo electrónico. La BIBLIOTECA CHAID NEME debe procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

Contacto con grupos especializados en seguridad informática. El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer las nuevas medidas en cuanto a seguridad de la información se va presentando.

Actualización, mantenimiento y divulgación de las políticas de seguridad de la información. Éste documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

El Jefe de Riesgos o la persona designada por la presidencia deben aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

Cumplimiento. Auditoría y cumplimiento, todos los procesos de seguridad de la información y recursos tecnológicos, deben estar siempre sometidos a intervenciones de control y revisión los cuales arrojen datos que contribuyan a la toma de decisiones en cuanto a mejora o replanteamiento de parámetros previamente establecidos; todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos. La entidad no debe emprender procesos de desarrollo mantenimiento de sistemas software que tengan asociados riesgos altos no mitigados.

Todo uso y seguimiento a los recursos de TI en la BIBLIOTECA CHAID NEME, debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional en materia.

Cumplimiento con la seguridad de la información. Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de la BIBLIOTECA CHAID NEME y al comité de seguridad.

Medidas disciplinarias por incumplimiento de políticas de seguridad. Todo incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en alguna sede de la BIBLIOTECA CHAID NEME, esta podrá suspender la prestación de cualquier servicio de información.

Protección por Defecto de Copyright. Todos los colaboradores de la BIBLIOTECA CHAID NEME deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.

Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

Actualización, mantenimiento y divulgacionde las políticas de seguridad de la información. Éste documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

El Jefe de Riesgos o la persona designada por la presidencia deben aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

Comité de seguridad. El Comité de Seguridad de la información está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia con respecto al programa de seguridad de la información dentro de la organización.

El comité debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad De la información, dentro de la Entidad.

Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización. Revisión y valoración de la Política de Seguridad de la Información.

Alineación e integración de la seguridad a los objetivos del negocio.

Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización. Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.

Reportar, a través de reuniones semestrales a la Presidencia el estado de la seguridad y protección de la información en la compañía y la necesidad de nuevos proyectos en temas de seguridad de la información

Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información

Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.

Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.

Supervisar y controlar de los cambios significativos en la exposición de los activos de información a las principales amenazas. Revisar y seguir los incidentes de seguridad de la información.

Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la compañía.

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda).

Mejoras en las actividades inherentes a la Seguridad de la BIBLIOTECA CHAID NEME y sus procesos.

Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de la BIBLIOTECA CHAID NEME

Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.

Cambio en los roles del ciclo de certificación.

Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de la BIBLIOTECA CHAID NEME. El Presidente

Convoca al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por todos su miembros.

Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

Oficial de Seguridad de la Información. Oficial de Seguridad de la Información (Jefe de Riesgos o persona designada para los temas de seguridad de la Entidad).

Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.

Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.

Dirigir el programa de manejo y seguimiento de incidentes.

Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía. Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.

Crear y mantener un Programa de Concientización en seguridad de la información.

Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

4.3 Aplicar los controles de la norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información.

Los controles que se sugieren implementar para mitigar los riesgos identificados en la fase de "evaluación y priorización de riesgos", así como sus responsables y tiempos aproximados de implementación se pueden encontrar en los planes de acción.

Plan de Acción. Evaluar riesgo. El plan de acción satisface los requerimientos del negocio en el momento de verificar y auditar las decisiones de la gerencia a través del logro de los objetivos del departamento de Informática y Tecnología así como responder a las amenazas reduciendo su complejidad incrementando su objetividad e identificando factores de decisión importantes lo que hace posible la intervención directa de la empresa en un todo colaborándole al área en la evaluación del impacto que cada uno de los cambios planteados en el modelo

conllevan, involucrando funciones a cada uno de los miembros de la organización tomando en consideración diferentes tipos de riesgos que estructuran el plan de riesgos.

Controles a implementar

Políticas y procedimientos de evaluación de riesgos. La administración deberá implementar unas reuniones gerenciales para asegurarse que dentro de la organización existan direcciones claras en todas las iniciativas de seguridad, que se aplique una metodología continua y que con frecuencia se llevan a cabo las evaluaciones correspondientes al ciclo de vida del SGSI teniendo en cuenta todo el equipo multidisciplinario para mantener actualizadas las evaluaciones de riesgos, resultados de auditorías inspecciones e incidentes. Este control debe ser implementado por la Gerencia General en un plazo no mayor a 10 meses.

Revisiones de Grupos Especializados. La Gerencia General debe solicitar la revisión de grupos especializados externos para que ellos realicen la verificación tanto de las normas establecidas por el auditor interno como por la Vicepresidencia de Informática y Tecnología de esta manera se le dará total continuidad y trasparencia al proceso. Este control debe ser implementado por Gerencia General y Departamento de Informática y Tecnología en un plazo no mayor a 6 meses.

Definición de un marco referencial de riesgos. La Gerencia General debe establecer una evaluación sistemática de riesgos incorporando los riesgos de la información más relevantes que hagan parte de los objetivos de la organización y que son la base de datos fundamental para

determinar la forma en la que los riesgos deben ser manejados a un nivel aceptable. Este control debe ser implementado por la Gerencia General en un plazo no mayor a 3 meses.

Procedimiento de evaluación de riesgos. La Gerencia General deberá comprobar que los riesgos identificados hacen parte tanto de factores externos, como de factores internos así como revisar los resultados de las auditorías internas y de las revisiones de las inspecciones e incidentes identificados. Este control debe ser implementado por la Gerencia General en un plazo no mayor a 5 meses.

Reportes a la Gerencia para su revisión y acuerdo de aceptación. La Vicepresidencia de Informática y Tecnología deberá emitir reportes periódicos a la gerencia para su revisión y acuerdo con cada uno de los riesgos identificados, así como crear en el área la política de la periodicidad de los mismos. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Plan de acción. La Gerencia deberá determinar el plan de acción contra los riesgos, se debe establecer la estrategia para evitar, mitigar o aceptar el riesgo. Este control debe ser implementado por la Gerencia General en un plazo no mayor a 4 meses.

Plan de acción. Administración de la calidad. El plan de acción satisface los requerimientos del negocio cuando satisface los requerimiento del cliente de Informática y Tecnología, se hace posible a través de la planeación, implementación y mantenimiento de estándares y sistemas de administración que estén presentes en las diferentes fases del desarrollo

con entregables de usuario claros y con responsabilidades explicitas en el modelo; se busca establecer con el control una cultura de calidad y se hace un entrenamiento al usuario final con los planes de calidad y sus responsabilidades de aseguramiento de la misma estableciendo buenas prácticas de control de calidad.

Controles a implementar

Políticas y procedimientos relacionados con el aseguramiento de la calidad. La organización deberá desarrollar y periódicamente revisar y actualizar una política de administración consistente con el plan general de la calidad formalmente definida y documentada. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Metodología del ciclo de vida de desarrollo de sistemas. El departamento de Informática y Tecnología deberá fijar, realizar y documentar la metodología adecuada para el ciclo de vida en el desarrollo de los sistemas tanto adquiridos como desarrollados internamente. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Marco Referencial de adquisición y mantenimiento para la infraestructura de tecnología. El departamento de Informática y Tecnología deberá construir un marco referencial que incluya pasos a seguir para los procesos de adquisición, programación, documentación y pruebas estableciendo los parámetros y aplicación de correcciones para cada caso. Este control

debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 semanas.

Enfoque de aseguramiento de la calidad de la organización. La organización deberá desarrollar una reunión de la post-implementación para asegurar que todos los sistemas nuevos o modificados sean desarrollados y puestos en producción verificando que el equipo de proyecto este siguiendo la metodología del ciclo de vida respetando siempre los lineamientos del mismo. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Plan de acción. Administrar Cambios. El plan de acción satisface los requerimientos de minimizar la probabilidad de interrupciones m alteraciones no autorizadas y errores y se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura en funcionamiento del departamento de Informática y Tecnología, se toman en consideración la identificación de los cambios, procedimientos de categorización, priorización y emergencia, evaluación del impacto así como el rediseño de los procesos del negocio.

Controles a implementar

Control de cambios. La Vicepresidencia de Informática y Tecnología deberá asegurar que la administración de cambios así como el control y la distribución de todo el sistema serán integrados apropiadamente en un sistema completo de administración de configuración siendo

este un proceso automático para soportar el registro y el seguimiento de cada actividad que se realice. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 9 meses.

Software instalado por el usuario. La Vicepresidencia de Informática y tecnología deberá dar las restricciones explicitas para descargar e instalar software por parte de los usuarios. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Restricciones de uso del software. La organización en pleno y sin excepción deberá obedecer y acatar las restricciones impartidas por el departamento de TI. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 4 meses.

Documentación de los sistemas de información. La organización deberá asegurar que esté disponible en todo momento y para quien solicite la adecuada documentación para el sistema de información y sus componentes, salvaguardarla en todo momento y solo hacer distribución de la misma al personal autorizado. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Políticas y procedimientos de administración de la configuración. La organización debe desarrollar revisar y actualizar una política de administración de la configuración formalmente definida y documentada que sean para facilitar la implantación de la política de administración

de la configuración y delos controles asociados. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 4 meses.

Configuración básica. La organización deberá desarrollar, documentar y mantener actualizada la configuración básica que por defecto deben manejar cada uno de los usuarios en todos los sistemas de información computarizados y un inventario de los componentes constitutivos del sistema. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 6 meses.

Configuración de opciones. La organización deberá configurar el ambiente de seguridad de los productos de tecnología de información del modo más restrictivo posible, consistente con los requisitos operacionales de los sistemas de información. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 4 meses.

Bitácora de control de cambios. El área de Informática y Tecnología deberá establecer una bitácora de control de cambios sobre los sistemas de información computarizados. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Plan de acción. Asegurar la continuidad de los servicios. El plan de acción satisface los requerimientos de asegurabilidad de los servicios de TI estén permanentemente disponibles y asegurar un impacto mínimo en el negocio en el evento que ocurra una interrupción mayor, se hace posible a través de un plan de continuidad probado y funcional que este perfectamente

alineado con el plan de continuidad del negocio. Toma en consideración procedimientos alternativos, respaldo y recuperación, clasificación con base en la criticidad, pruebas y entrenamiento sistemático, procesos de escalamiento y monitoreo y administración de problemas.

Políticas y procedimientos del plan de contingencia. La organización deberá desarrollar y revisar periódicamente una política de plan de contingencia con el propósito de identificar los roles, responsabilidades y cumplimiento de los mismos así como el procedimiento documentado para facilitar la implantación de las políticas en el plan de negocio. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Plan de contingencia. La organización debe desarrollar e implementar un plan de contingencia para los sistemas de información y designar un veedor para que revise y apruebe el plan de contingencia, así como distribuir las copias del mismo al personal que interviene en el proceso. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 12 meses.

Entrenamiento para la contingencia. La organización deberá capacitar de manera eficaz al personal involucrado con el plan de contingencia con sus roles y responsabilidades con respecto a los sistemas de información y proveer constantemente esta capacitación para una respuesta efectiva en el momento de crisis. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 semanas.

Probar el plan de contingencia. La organización deberá probar el plan de contingencia para los sistemas de información, determinar si el mismo es efectivo y la organización se encuentra en el punto clave para ejecutarlo. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Actualización del plan de contingencia. La organización debe revisar el plan de contingencia, los problemas detectados durante su ejecución y prueba del miso. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Sitio alterno de almacenamiento. La organización deberá buscar un sitio alterno que le permita alojar la información de respaldo. El sitio debe estar geográficamente separado del sitio base para que no esté expuesto a ninguna amenaza y debe estar configurado de manera que sea rápida, oportuna y efectiva la recuperación de la información en caso tal que se necesite. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Sitio alterno de procesamiento. La organización debe identificar un sitio alterno para el procesamiento de la información e iniciar los acuerdos necesarios que permitan reiniciar las operaciones cuando no esté disponible el sitio primario de operaciones. El sitio de procesamiento debe estar completamente configurado para soportar el mínimo de capacidad de las operaciones aparte de estar completamente adecuado para su uso. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Servicio de telecomunicaciones. La Organización debe tener un servicio alterno de comunicaciones cuando este no esté disponible. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 semanas.

Backup de los sistemas de información. La organización debe respaldar y almacenar toda la información en una ubicación completamente segura de todos los sistemas críticos de información. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Recuperación y reconstitución de los sistemas de información. La organización debe incluir una recuperación y reconstitución completa del sistema de información como parte de la prueba del plan de contingencia asi mismo debe emplear mecanismos con procedimientos de soporte para permitir que el sistema de información sea recuperado y reconstituido al estado original del sistema después de una interrupción o falla. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Plan de acción. Garantizar la seguridad de sistemas. Salvaguardar la información contra los usos no autorizados y que la misma no se divulgada, modificada, dañada o extraviada, se hace posible mediante controles de acceso lógicos y programas que restrinjan el uso a los usuarios no autorizados. Toma en consideración requerimiento de confidencialidad y privacidad, autenticaciones y control de acceso, identificaciones de usuario, administración de llaves criptográficas, manejo reporte y seguimiento de incidentes, prevención y detección de virus, herramientas para el monitoreo y pruebas y reportes de intrusión.

Controles a implementar

Política y procedimientos de control de acceso. La organización debe tener una política de control de acceso definida y documentada. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Revisión gerencial de cuentas de usuario. La Gerencia deberá contar con un proceso de control para revisar y confirmar periódicamente los derechos de acceso. Se lleva a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes y alteraciones no autorizadas o accidentales. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Accesos inválidos en el sistema. El sistema de información debe tener un límite de intentos inválidos en el acceso durante un periodo de tiempo y por seguridad realizar el bloqueo del mismo para el ingreso. Deberá hacerlo de forma automática y solo podrá levantar dicha restricción el área de TI. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 semana.

Administración de cuentas de usuario. La gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberán incluirse los procedimientos de aprobación formal que indique el propietario de los datos o del sistema que otorga a su vez los privilegios de

acceso. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Supervisión y revisión de control de acceso. La organización deberá revisar y supervisar las actividades de los usuarios con respecto a la aplicación y uso de los controles de accesos a los sistemas de información. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Acceso remoto. La Organización deberá documentar, monitorear y controlar todos y cada uno de los métodos de acceso remoto a cada uno de los sistemas de información para cualquier función relacionada con la empresa. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Concientización respecto a la seguridad de TI. La organización se asegura que todos y cada uno de los usuarios incluyendo la junta directiva estén conscientes de la gran importancia del sistema de seguridad de la información antes de autorizar el acceso a cualquier sistema de información. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Entrenamiento de seguridad. La organización deberá identificar personal con los perfiles y responsabilidades significativas en el SGSI, documentar cada uno de estos perfiles y responsabilidades y proporcionales a los mismos un entrenamiento acorde a su cargo. Este

control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 5 meses.

Registros de entrenamiento de seguridad. La organización debe monitorear y documentar las actividades de entrenamiento individual de seguridad básico y específico. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Eventos auditables. El sistema de información deberá generar registros de auditoria para los eventos de transacciones que afectan la contabilidad, inventarios o Bancos y eventos fallidos de inicio de sesión. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Contenido de los registros de auditoria. Los sistemas de información computarizados deben capturar suficiente información en cada uno de los registros de auditoria para establecer que eventos ocurrieron, sus fuentes y resultados. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Capacidad de almacenamiento para los Logs de auditoria. La organización asigna suficiente capacidad de almacenamiento y configura los registros de la auditoria para prevenir que no se excedan los espacios. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 meses.

Procesamiento de la auditoria. En el evento de una falla en el registro de la auditoria el sistema de información alertara de inmediato a las personas encargadas de salvaguardarla para que tomen las acciones necesarias. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Protección de la información de auditoria. El Sistema de Información Computarizado protege la información de acceso no autorizado, modificación, y borrado. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Categorización de la información. La gerencia deberá implementar procedimientos que aseguren que todos los datos son clasificados en términos de sensibilidad, mediante decisiones explicitas y formales, aun con los datos que no requieran protección. Los dueños de los mismos deben determinar la ubicación o la disposición de sus datos y determinar quienes pueden compartir los mismos. Debe quedar evidencia explicita de la aprobación y de la disposición sobre el mismo. El esquema de clasificación debe tener los criterios de intercambio de datos entre organizaciones teniendo en cuenta la seguridad y el cumplimiento. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología, Audito Interno en un plazo no mayor a 3 meses.

Política y procedimientos de acreditación y certificación. La organización deberá desarrollar y periódicamente revisar y actualizar la política de acreditación y certificación verificar que la misma está totalmente documentada así como los procedimientos documentados

para facilitar la implantación de las políticas de acreditación y certificación. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Certificación de seguridad. La organización debe dirigir una valoración de los controles de seguridad de cada sistema de información para determinar hasta qué punto cada control se implementa de forma correcta y que se han estado ejecutando de la manera que se tenía planeado de acuerdo a los requerimientos del SGSI. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Plan de acción y logros. La organización debe desarrollar y actualizar un plan de acción para el sistema de información que documente los planes de la organización, implementaciones y evolución de acciones tomadas para detectar cualquier deficiencia notada durante la valoración de los controles de seguridad, para reducir o eliminar todas las vulnerabilidades conocidas. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Monitoreo continuo. La organización debería supervisar que los controles de seguridad se mantengan de una forma continua. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Política y procedimientos de respuesta a incidentes. La organización debe tener desarrollada una política de respuesta a incidentes formalmente definida y documentada para

facilitar que cada procedimiento tenga una política implantada de respuesta a incidentes. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología, Auditor Interno en un plazo no mayor a 3 meses.

Manejo de incidentes. La organización debe implementar una actividad de manejo de incidentes para los eventos de seguridad el cual debe tener. preparación, detección de análisis, contención, erradicación, y recuperación. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología, Auditor Interno en un plazo no mayor a 3 meses.

Reporte de violación de actividades de seguridad. La administración de la función de los servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean reportadas, registradas, revisadas y escaladas de forma apropiada y en forma regular para resolver e identificar los incidentes que involucren actividades no autorizadas, Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Reporte de incidentes. La organización deberá reportar de forma inmediata los informes de incidentes a las autoridades que asi se estipulen. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Incidente de accidentes y respuesta. La organización deberá proporcionar a los usuarios ayuda para el manejo de cada incidente de seguridad. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Política y procedimientos para la planificación de la seguridad. La organización deberá desarrollar y periódicamente revisar la política para la planificación de la seguridad. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 5 meses.

Plan del sistema de seguridad de la información. La organización debe desarrollar un plan de seguridad para el sistema de información que proporcione una apreciación global de los requisitos de seguridad para los sistemas y una descripción para los controles de seguridad. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Actualizar plan del sistema de seguridad de la información. la organización debe revisar el plan de seguridad para detectar desviaciones y efectuar las correcciones. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Reglas de conducta. La organización debe establecer y hacer prontamente disponible a todos los usuarios de los sistemas de información y las reglas que definen sus responsabilidades y conductas esperadas con respecto a los usos de los sistemas de información. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 4 meses.

Control de los usuarios sobre sus cuentas. Los usuarios deben controlar la actividad generada desde su propia cuenta, se establecerán los mecanismos de información que permitan supervisar la actividad normal así como alertarlos sobre las actividades inusuales. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Vigilancia de seguridad. La administración de seguridad de TI, debe asegurar que toda actividad quede registrada y que cualquier cosa que indique una inminente violación de seguridad será notificada a todos aquellos que puedan verse afectados, sin importar su origen actuando de manera oportuna frente al hecho. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Plan de acción. Administrar los datos. Los requerimientos que se satisfacen con este plan de acción son asegurar que los datos permanezcan completos precisión y validos durante su entrada, actualización y almacenamiento, lo cual se hace posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI, toma en consideración el diseño de formatos, Controles de entrada, procesamiento y salida, identificación, movimiento y administración de la librería de medios, recuperación y respaldo de datos, autenticación e integridad y propiedad de datos.

Controles a implementar

Políticas y procedimientos de administración de datos. la organización deberá diseñar , implementar y revisar de forma periódica el flujo de datos dentro de la función de TI, el proceso de autorización de la documentación fuente, procesos de recolección y seguimiento, transmisión de datos. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 8 meses.

Revisión de todas las aplicaciones críticas. El área de informática y tecnología deberá revisar los módulos que llevan a cabo revisiones de precisión o capturas de datos sensibles, así como las que lleven a cabo rutinas de corrección de errores, procedimiento de salidas y balanceo de las cargas en los aplicativos críticos. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 7 meses.

Revisión de todas las aplicaciones críticas. El área de TI deberá revisar funciones que lleven a cabo las rutinas de corrección de errores de entrada de datos, control de la integridad de los procesos de datos enviados a proceso, distribución de salidas sensitiva sólo a personas autorizadas, procedimientos de balanceo de salidas para control de totales y conciliación de variaciones. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 6 meses.

Políticas y procedimientos de repositorio central de bases de datos. la organización deberá establecer las normas, el diseño y los controles sobre. la organización de la base de datos, sobre los diccionarios de datos, procedimientos de mantenimiento de seguridad de la base de datos, determinación y mantenimiento de la propiedad de las bases de datos, procedimientos de

control de cambios sobre el diseño y contenido de la base de datos y los reportes administrativos y cada pista de auditoria que definen las actividades de bases de datos. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 6 meses.

Políticas y procedimientos de librería de medios y almacenamiento de datos externo. La organización debe definir los controles para. Procedimientos de reconciliación entre registros actuales y registros de datos almacenados, reciclaje de datos y protección de información sensitiva, rotación de medios de datos, inventario de datos de prueba y pruebas de recuperación llevadas a cabo, administración de la librería de medios y del sistema de administración de la librería, medios y funciones del personal en el sitio alterno en el plan de continuidad, asegurar que el archivo cumple con requerimientos legales y de negocio. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Plan de acción. Administrar Instalaciones. Satisface el proporcionar un ambiente físico conveniente que proteja el quipo y al persona de TI contra peligros o fallas humanas, se hace posible a través de la instalación de controles físicos y ambientales adecuados y que sean revisados regularmente para su funcionamiento apropiado, toma en consideración el acceso a las instalaciones, identificaciones del sitio, seguridad física, las políticas de inspección y escalamiento, administración de crisis, salud y seguridad del personal, políticas del mantenimiento preventivo y protección sobre amenazas ambientales.

Controles a implementar.

Políticas y procedimientos de mantenimiento de sistemas. La organización deberá desarrollar y revisar periódicamente una política de mantenimiento de sistemas formalmente definida y documentada. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Mantenimiento periódico. La organización debe fijar, realizar y documentar el preventivo mantenimiento a cada uno de los componentes de los sistemas de información de acuerdo a las especificaciones técnicas determinadas. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 meses.

Acceso a medios. La organización debe asegurar que solo los usuarios autorizados tienen acceso a la información en forma impresa o en medios digitales que puedan ser exportados del sistema de información. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 1 mes.

Autorización de acceso físico. La organización deberá desarrollar y conservar listas con el personal que tiene acceso autorizado a los recursos de los sistemas de información, portando las credenciales que acrediten su vínculo con la compañía. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 2 semanas.

Control de acceso físico. La organización deberá controlar todos los puntos de acceso físico a los recursos de los sistemas de información y verificar autorizaciones de acceso individuales antes de conceder acceso a los recursos. La organización también deberá controlar el acceso a las áreas oficialmente designadas como públicamente accesible, como es apropiado, en acuerdo con la valoración de riesgos de la organización. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 3 meses.

Discreción sobre las instalaciones de tecnología de información. El área de TI deberá asegurar que se mantenga un bajo perfil sobre la identificación física y lógica relacionado con las operaciones de tecnología de información, todo esto debe ser limitado y mantenerse con la reserva adecuada. Este control debe ser implementado por la Vicepresidencia de Informática y Tecnología en un plazo no mayor a 4 meses

5. Conclusiones

Se realizó un diagnóstico para identificar las vulnerabilidades y amenazas de seguridad de información de los servicios y procesos de la Biblioteca recolectando la información interna y externa, por medio de los procesos descritos en la norma NTC-ISO/IEC 27001:2013.

Se logró formalizar el sistema de seguridad mediante la documentación de las políticas, programas y procedimientos establecidos para gestionar los riesgos de seguridad de información de la dependencia.

Se logró desarrollar el método para aplicar los controles de la norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información.

El presente proyecto permitió analizar mediante los controles y objetivos de control de la norma NTC-ISO-IEC 27001.2013 aplicables para la biblioteca cuáles son sus puntos débiles relacionados con la falta de la implementación de un Sistema General de Seguridad en la Información, que podrían convertirse en una fuerte amenaza para el normal cumplimento de sus procesos misionales.

Para el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) en la Biblioteca Chaid Neme, se adoptó la norma ISO 27001.2013 y a sí mismo el ciclo PHVA (Planear, Hacer, Verificar y actuar) que es la metodología de desarrollo e implementación del

SGSI propuesto por la organización ISO, se desarrolló para biblioteca el diseño de la Política de seguridad de la información.

Se estableció que los riesgos a los cuales se encuentra expuesta la empresa, principalmente son por el desconocimiento de buenas prácticas de seguridad de la información, por parte del personal administrativo de la misma.

Con base en lo anterior, se pudo generar un marco de trabajo que servirá de guía para la implementación del SGSI en la biblioteca de forma sostenible y evaluable en el tiempo.

6. Recomendaciones

Es recomendable formalizar el sistema de seguridad mediante la documentación de las políticas, programas y procedimientos establecidos para gestionar los riesgos de seguridad de información de la dependencia.

Se debe aplicar los controles de la norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información.

Concientizar y capacitar desde la Gerencia de la biblioteca a los empleados en los temas relacionados con la seguridad de la información para ir creando cultura, identificación de vulnerabilidades y amenazas de seguridad de la información y modos de trabajo eficaces.

Se recomienda que la organización adopte medidas para el mejoramiento de la red, mediante la segmentación de la misma la cual brindara mayor seguridad a la información y administrando las configuraciones se contribuirá a la seguridad de la información

Periódicamente se debe realizar un seguimiento a los riesgos a los cuales se encuentran expuestos los activos de información, de manera preventiva, y para la constante mitigación del riesgo.

Capacitar constantemente a los funcionarios de la empresa sobre manejo de la información, buenas prácticas de tecnologías de la Información y Comunicación, para que estén a la vanguardia de los cambios tecnológicos que ocurren constantemente en el mundo.

Referencias

Ley 23 de 1982. (15 de Febrero de 2014). Recuperado el 12 de Abril de 2016, de Derecho de autor y propiedad intelectual ley.: http:// http://legislacion.vlex.com.co/vid/ley-derechos-autor-71608275

Ley 44 de 1993 . (03 de Marzo de 2014). Recuperado el 11 de Abril de 2016, de Derecho de autor: http:// http://www.derechodeautor.gov.co/documents

Ley 527 De 1999 . (14 de Junio de 2014). Recuperado el 11 de Abril de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

Ley 719 de 2001. (15 de Junio de 2014). Recuperado el 12 de Abril de 2016, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5533 - ftp://ftp.camara.gov.co/

AMERICANOS, O. D. (07 de Abril de 2013). *TENDENCIAS EN LA SEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA Y EL CARIBE Y RESPUESTAS DE LOS GOBIERNOS.* Recuperado el 26 de Marzo de 2016, de http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf

AMPARO, P. (s.f.). Recuperado el 29 de Marzo de 2016, de http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf

Archivo General. (1999). *Ley 527 de 1999.* Recuperado el 10 de Enero de 2017, de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

Arredondo Tomas. (15 de Junio de 2014). *Shannon, padre de la Teoría de la Información-*. Recuperado el 10 de Abril de 2016, de ttp://bituchile.com/2011/05/teoria-de-la-informacion-concepto-bit-de-la-semana/

Aucal Business School. (15 de marzo de 2015). *La seguridad vista desde sus inicios.* Recuperado el 10 de enero de 2017, de http://www.informacionseguridad.com/754/

Campos Javier. (22 de julio de 2011). *El algoritmo de Diffie-Hellman.* Recuperado el 10 de enero de 2017, de http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/

Casadiegos Santana, A. L. (28 de julio de 2014). *Sistema de gestión de seguridad de la información (SGSI).* Recuperado el 5 de enero de 2017, de http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/901

CASADIEGOS SANTANA, A. L. (28 de Julio 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.* Recuperado el 14 de Abril de 2016, de U iversidad Fran cisco de Paula Santander: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/901

Castro Fabian, Ciacedo Carlos . (27 de nviembre de 2013). *La norma iso 27001* . Recuperado el 29 de diciembre de 2016, de http://es.slideshare.net/Karlos19s/la-norma-iso-27001-2-28689086

CHACÓN HURTADO ANDRES FELIPE, M. S. (21 de Junio de 2012). *INFORMACIÓN PARA COMPUTACIÓN EN NUBES PRIVADAS Y COMUNITARIAS.* Recuperado el 26 de Marzo de 2016, de Universidad ICESI: http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/68436/1/definicio

Compuchannel. (26 de agosto de 2016). *Porque implantar un sistema de gestión de seguridad de información.* Recuperado el 10 de enero de 2017, de

http://www.compuchannel.net/2008/08/26/porque-implantar-un-sistema-de-gestion-de-seguridad-de-informacion/

Dusko Pavlovic. (s.f.). *Teoría de la seguridad por oscuridad Gaming.* Recuperado el 29 de Marzo de 2016, de Cornell University Library: http://arxiv.org/abs/1109.5542v1

ESTADISTICA. (2013). *La encuesta.* Obtenido de http://www.estadistica.mat.uson.mx/Material/queesunaencuesta.pdf

FABIÁN DÍAZ ANDRÉS, C. G. (05 de Agosto de 2011). *IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLOGICAMENTE CON LA MNORMA ISO 27001.* Recuperado el 26 de Marzo de 2016, de NUESTRA SEÑORA DE GRACIA : http://www.konradlorenz.ed

Ferrer Jesús. (s.f.). *Tecnicas de la investigacion.* Recuperado el 5 de enero de 2017, de http://metodologia02.blogspot.com.co/p/tecnicas-de-la-investigacion.html

Hernandez SampierI, Roberto - Fernandez Collado, Carlos – Baptista Lucio, María del pilar. (2010). *"Metodología de la investigación".* Quinta edición Editorial Mac Graw Hills/Interamericana Editores Copyright.

ICONTEC, I. 2. (10 de Junio de 2014). *Certificación del Sistema de Gestión de Seguridad de la Información* . Recuperado el 12 de Abril de 2016, de http://www.icontec.org/index.php/es/sectores/agricultura-y-alimentos/50-colombia/certificacion-s

ISO 27000.es, .. (2005). *Glosario.* Recuperado el 20 de febrero de 2017, de http://www.iso27000.es/glosario.html

Iso 27001. (2012). *Qué es un SGSI.* Recuperado el 5 de diciembre de 2016, de http://www.iso27000.es/sgsi.html

Jimeno Molins Natalia. (s.f.). *Temario especifico y test Técnicos de administración del ministerio de económia y hacienda.* Editorial MAD Copyright-.

Ley 1273 5 de enero de 2009. (s.f.). Recuperado el 29 de Marzo de 2016, de Protección de la información y de los datos : http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Milagros Juarez Fatima. (8 de septiembre de 2014). *Obtenido de normas ISO/IEC 27001.* Recuperado el 15 de junio de 2016, de http://norma07.blogspot.com.co/2014/09/bienvenidos-todos.html

Ministerio de las tecnologias. (2016). *Fortalecimiento de la ciberseguridad.* Recuperado el 5 de diciembre de 2016, de http://www.mintic.gov.co/portal/604/articles-6124_recurso_4.pdf

MOSQUERA QUINTERO, G. C. (02 de Diciembre de 2015). *ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.* Recuperado el 14 de Abril de 2016, de Universidad Francisco de Paula Santander: http://repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/901

Naya De Vita Montiel. (2008). *Tecnologías de información y comunicación para las organizaciones del siglo xxi.* Recuperado el 5 de diciembre de 2016, de http://publicaciones.urbe.edu/index.php/cicag/article/viewArticle/545/1317

Norma Técnica Colombiana NTC-ISO/IEC 27001. (2006). *l Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).* Bogotá: NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001.

PERSONALES, P. D. (s.f.). Recuperado el 12 de ABRIL de 2016, de http://www.sic.gov.co/drupal/sites/default/files/normatividad/Titulo%20V%20Proteccion_Datos_Personales.pdf

Prezi.com. (2 de mayo de 2014). *Auditoría de sistemas.* Recuperado el 9 de mayo de 2016, de https://prezi.com/q-i08kniv6rb/auditoria-de-sistemas/

Ramio Aguirre Jorge. (2006). *Libro Electrónico de Seguridad Informática y Criptografía.* SEXTA EDICIÓN VERSION 4.1.

Ramos, A. (11 de junio de 2007). *El eslabón más débil de la cadena.* Recuperado el 10 de enero de 2017, de http://www.antonio-ramos.es/2007/06/el-eslabn-ms-dbil-de-la-cadena.html

Ramos, A. R. (2007). *El eslabón más débil de la cadena.* Recuperado el 29 de Marzo de 2016, de ISACA madrid: http://www.antonio-ramos.es/2007/06/el-eslabn-ms-dbil-de-la-cadena.html

Reynolds, J. (1991 Julio). *P. Holbroo.* RFC 1244: Site Security Handbook.

Secretaria Senado. (2012). *Ley estatutaria 1581 de 2012.* Recuperado el 29 de Marzo de 2016, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SEGURIDAD, G. D. (s.f.). *INFORMACIÓN EN CONTEXTOS DE MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS DE LA REGIÓN.* Recuperado el 25 de Marzo de 2016, de http://repositorio.utp.edu.co/dspace/bitstream/11059/2514/1/0058A973.pdf

Superintendencia de Industria y Comercio. (15 de Febrero de 2014). *Ley estatutaria 1266 de 2008.* Obtenido de Habeas data.: http://www.sic.gov.co/drupal/sites/default/files/normatividad/Decreto_2952_2010.pdf

universidad francisco de paula santander ocaña. (2016). Obtenido de www.ufpso.edu.co

Apéndices

Apéndice A. Entrevista

Objetivo. Evaluar el nivel de seguridad de la información en la Biblioteca Chaid Neme de la ciudad de Ocaña

1. ¿Cada cuánto se realiza mantenimiento a los recursos informáticos de la Empresa y que evidencia se tiene de los mismos?

2. ¿Cómo cree usted que se encuentra la biblioteca con referencia a la seguridad de la información? Por qué?

3. ¿Qué tipo de capacitación brinda a sus usuarios, en el tema de seguridad de la información?

4. ¿Teniendo en cuenta la seguridad, que políticas maneja para preservar la seguridad de la información?

5. Además de su personal, ¿quién más tiene acceso a cualquiera de sus Sistemas de Información administrativos?

6. ¿Dónde se almacenan las copias de respaldo o backups de la información que se generan en los sistemas de información, cada cuanto se realizan y con qué frecuencia se prueban para ver si funcionan?

7. ¿Cómo se encuentra la empresa económicamente para asumir los retos que demanda la seguridad de la información?

8. ¿Cuáles son las políticas y procedimientos para la selección del personal que ingresará a laborar en la Biblioteca?

9. Cuando se termina la vinculación laboral de un empleado, ¿Cómo se realiza la desvinculación del mismo en lo relacionado con el acceso a los sistemas de la Empresa?

10. ¿Cómo garantiza la continuidad del negocio ante un eventual siniestro?

Apéndice B. Encuesta

Objetivo. Evaluar el nivel de seguridad de la información en la Biblioteca Chaid Neme de la ciudad de Ocaña

Nombre. **Cargo**.

1. Las copias de respaldo de la información es almacenada en.

☐ Caja Fuerte o Bóveda
☐ Estantes o Gavetas
☐ Muebles con cerradura o Archivador
☐ Fuera de la Organización (para prevenir pérdida de datos en el caso de incidencias)

Otras _____

2. La Empresa cuenta con.

Vigilancia	Sí __ No__
Infraestructura sólida y segura	Sí __ No__
Ruta de Evacuación	Sí __ No__
Cámaras de Vigilancia	Sí __ No__
Alarmas	Sí __ No__
Extintores	Sí __ No__
Ruta de Evacuación	Sí __ No__
Instalaciones eléctricas ideales	Sí __ No__

3. El equipo de cómputo a su disposición, cuenta con.

Contraseña, para permitir el acceso de usuarios a los sistemas
Sí __ No__ Algunos__
Antivirus, actualizado
Sí __ No__ Algunos__
Software, con licencia
Sí __ No__ Algunos__
Restricción de accesos a páginas web (redes sociales, etc)
Sí __ No__ Algunos__
Acceso restringido a las aplicaciones, luego de varios intentos
Sí __ No__ Algunos__
Requerimientos necesarios para la realización optima de sus labores
Sí __ No__ Algunos__

4. ¿Con qué frecuencia el equipo de cómputo a su disposición recibe mantenimiento preventivo?

- ☐ Mensualmente
- ☐ Trimestralmente
- ☐ Semestralmente
- ☐ Anualmente
- ☐ Cuando lo requiere
- ☐ Nunca

5. ¿En qué medio respalda la información elaborada desde su puesto de trabajo?

- ☐ CD
- ☐ DVD
- ☐ Memorias USB
- ☐ Impresiones
- ☐ Disco Duro
- ☐ Ninguno

Otras _____

Apéndice C. Modelo lista de chequeo.

Empresa

Día	Mes	Año

Ref.	Situaciones	Causas	Solución

Elaborado (Nombre y Firma)	Aprobó (Nombre y Firma)

Apéndice D. Modelo lista de verificación.

ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA

Apéndice E. Políticas de seguridad

POLÍTICAS DE SEGURIDAD		
POLÍTICAS DE SEGURIDAD LA INFORMACIÓN.	• Dirección de la Alta Gerencia para la Seguridad de la Información.	Control que **Aplica** dentro de la biblioteca, debido a que esta es la autorización de la alta gerencia de la biblioteca, (Gerencia) para el diseño de la política de seguridad de la información.
	• Políticas de Seguridad de la Información.	Control que **Aplica** dentro de la biblioteca, debido que mediante esta se puede proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales, con la legislación y las normativas aplicables en la biblioteca
	• Revisión de las Políticas de Seguridad de la Información.	Control que **Aplica** dentro biblioteca, la política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.		
Organización Interna	• Organización Interna	Control que **Aplica** dentro de biblioteca, debido a que este promueve la gestión de la seguridad de la información dentro de las instalaciones de la institución.
	• Roles y Responsabilidad de Seguridad de la Información.	Control que **Aplica** dentro de la biblioteca, debido a que cada uno de los funcionarios de la institución debe tener obligaciones de acuerdo a la política de seguridad de la información de la institución.
	• Contacto con autoridades.	Control que **aplica** dentro de la biblioteca, debido la institución no tiene contacto con los distintos entes autoritarios tales como: agencia colombiana de protección datos, alianza internacional de protección y seguridad cibernética, Inteco-OSI, entre otros.
	• Seguridad de la Información en la gestión de proyectos.	Control que **no aplica** dentro de la biblioteca, debido la institución no cuenta con políticas de seguridad de la información en la elaboración de proyectos de investigación.
	• Segregación de deberes.	Control que **aplica** dentro de la biblioteca, debido a que consiste en que un trabajador que realiza una tarea puede ser supervisado por otro trabajador para que la tarea se complete de manera satisfactoria.
	• Dispositivos móviles y teletrabajo.	Control que **no aplica** dentro de la biblioteca, debido a que la institución no cuenta con la tecnología necesaria para implementar este tipo de herramientas que facilitan el desempeño de las funciones.
	• Política de dispositivos	Control que **aplica** dentro de la biblioteca, para el regalamiento de la conectividad de los Smartphone a

	móviles.	las redes de la institución
	• Teletrabajo.	Control que **no aplica** dentro de la biblioteca debido a que la institución no cuenta con la tecnología necesaria para implementar este tipo de herramientas que facilitan el desempeño de las funciones.
SEGURIDAD EN LOS RECURSOS HUMANOS.		
Previo al Empleo.	• Previo al Empleo.	Control que **aplica** dentro de la biblioteca para asegurar que los empleados, los contratistas y los terceros entiendan sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de Hurto, fraude o de uso indebido de los recursos.
	• Verificación de antecedentes	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia debe de indagar sobre los antecedentes previos del personal profesional que se encuentra en proceso de contratación, mitigando el riesgo que se puede presentar al contratar personal poco idóneo para la realización de las tareas.
	• Términos y condiciones del empleo.	Control que **aplica** dentro de biblioteca, donde se especifican los términos y condiciones legales y contractuales para los cuales está contratado el personal profesional.
Durante el Empleo.	• Durante el Empleo.	Control que **aplica** dentro de la biblioteca en donde la dirección verifica el cumplimiento de las labores para las cuales fueron contratados.
	• Responsabilidades de la Alta Gerencia.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia de la institución debe tener el compromiso y responsabilidades en todos los procesos realizados por dichos estamentos.
	• Conciencia, educación y entrenamiento de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia puede promulgar la capacitación del personal de la Organización en el manejo de normativas que garanticen la seguridad de los datos.
	• Proceso disciplinario.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia puede establecer procesos disciplinarios, cuando los funcionarios de la misma se excedan de sus funciones.
• Terminación y Cambio de Empleo.	Terminación y Cambio de Empleo.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia debe asegurar que todos los usuarios internos o contratistas de la institución, que ya no laboren, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será pertinente hasta que la institución lo considere.
	• Término de responsabilidades o cambio de empleo.	Control que **aplica** dentro de la biblioteca, debido a que la alta gerencia debe asegurarse que cuando usuarios internos o contratistas cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad

		cuyo cumplimiento será pertinente hasta que la institución lo considere.
GESTIÓN DE ACTIVOS		
Responsabilidad de los Activos.	• Inventario de activos.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia debe tener todos los activos claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
	• Propiedad de activos.	Control que **aplica** dentro de biblioteca debido a que toda la información y activos asociados a los recursos para el tratamiento de la información deben pertenecer a una parte designada de la Organización.
	• Uso aceptable de los activos.	Control que **aplica** dentro de la biblioteca, debido los activos de información deben garantizarse su integridad, disponibilidad y confidencialidad.
	• Clasificación de la Información.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia debe tener la clasificación de la información sensible de la institución y a si mismo medidas que garanticen las características básicas de la misma.
	• Etiquetado de la información.	Control que **aplica** dentro de la biblioteca en donde se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
	• Manejo de activos.	Control que **aplica** dentro de la biblioteca debida los activos de información deben garantizarse su integridad, disponibilidad y confidencialidad.
	• Devolución de activos.	Control que **aplica** dentro de la biblioteca, en donde la alta gerencia debe cerciorarse de la que los activos cuentes al momento de su devolución con la respectiva integridad.
	• Manejo de Medios.	Control que **aplica** dentro de la biblioteca , debido a que en la institución existe una política en donde se evite la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. Estos medios se deberían controlar y proteger de forma física.
	• Gestión de medios removibles.	Control que **aplica** dentro de la biblioteca debido a que la alta gerencia puede regular el uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la institución y estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.
	• Eliminación de medios.	Control que **aplica** dentro de la biblioteca en donde se debe establecer la eliminación de información sensible de la organización de medios removibles como (CDs, DVDs, USBs)

	• Transporte de medios físicos	Control que **aplica** dentro de biblioteca en donde durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
CONTROL DE ACCESO		
Requerimientos de Negocio para el Control de Acceso	• Política de control de acceso	Control que **aplica** dentro de la biblioteca, debido que en la institución pueden reglamentar mecanismos de control de acceso a las instalaciones físicas y a los recursos de la Organización mediante la cartelización y entre otros mecanismos que regulen el acceso del personal y a su vez clasificándolo mediante roles.
	• Política en el uso de servicios de red	Control que **aplica** dentro de la biblioteca debido a que en la Institución pueden reglamentar el uso de los servicios de red con la que la Organización cuenta, mediante restricciones a páginas web, entre otras.
	• Gestión de Accesos de Usuario	Control que **aplica** dentro de la biblioteca debido que la alta gerencia puede implementar políticas en donde se garanticen el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.
	• Registro y baja del usuario	Control que **aplica** dentro de la biblioteca, debido a que la institución cuenta con sistemas de automatizados que les permita realizar estas funciones.
	• Gestión de privilegios	Control que **aplica** dentro de la biblioteca, cuenta con sistemas de automatizados que les permita realizar estas funciones.
	• Gestión de información de autenticación secreta de usuarios.	Control que **aplica** dentro de la biblioteca, cuenta con sistemas automatizados que les permita realizar estas funciones.
	• Revisión de derechos de acceso de usuarios.	Control que **aplica** dentro de la biblioteca debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Responsabilidades del Usuario	Control que **aplica** dentro de la biblioteca debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Uso de información de autenticación secreta.	Control que **aplica** dentro de la biblioteca debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.
	• Control de Acceso de Sistemas y Aplicaciones.	Control que **aplica** dentro de la biblioteca, debido a que se encuentra establecida una política de seguridad de la información dentro de la institución que reglamente dicho control.

	• Restricción de acceso a la información.	Control que **aplica** dentro de la biblioteca, debido a que la alta gerencia restringe el acceso a la información sensible de la institución.
	• Procedimientos de conexión segura.	Control que **no aplica** dentro de la biblioteca, debido a que la institución no implementa procedimientos para establecer conexiones seguras en la red.
	• Sistema de gestión de contraseñas.	Control que **no aplica** dentro de la biblioteca debido a que la institución no cuenta con servidores de contraseñas que les brinde este servicio.
	• Uso de programas y utilidades privilegiadas.	Control que **no aplica** dentro de la biblioteca, debido dentro de la institución no se tiene estandarizado la utilización de un sistema de información automatizado.
	• Control de acceso al código fuente del programa.	Control que **aplica** dentro de la biblioteca debido a que los usuarios de la institución no tienen acceso a los códigos fuentes de las aplicaciones utilizadas dentro de la organización.
CIFRADO.		
Controles Criptográficos	• Política en el uso de controles criptográficos.	Control que **no aplica** dentro de la, debido a que en la institución no se aplican políticas de cifrado de la información.
	• Gestión de llaves.	Control que **no aplica** dentro de la, debido a que la institución no cuenta con servidores de contraseñas que les brinde este servicio.
SEGURIDAD FÍSICA Y AMBIENTAL.		
Áreas Seguras	• Perímetro de seguridad físico.	Control que **aplica** dentro de la, puesto que ya se realizó en encerramiento de las instalaciones, y en la institución cuentan con los mecanismos para la protección de las instalaciones física de la Organización.
	• Controles físicos de entrada.	Control que **aplica** dentro de la biblioteca, debido a que en la institución no cuentan con mecanismos de acceso de ingreso a las instalaciones de la Organización.
	• Seguridad de oficinas, habitaciones y facilidades.	Control que **aplica** dentro de la biblioteca, debido a que las instalaciones y oficinas cuentan con los requerimientos mínimos de seguridad en los recintos.
	• Protección contra amenazas externas y del ambiente.	Control que **no aplica** dentro de la biblioteca, puesto que la Organización no se cuenta con la infraestructura para la prevención de amenazas externas y desastres naturales.
	• Trabajo en áreas seguras.	Control que **aplica** dentro de la biblioteca, debido a que los funcionarios de la Organización realizan sus labores en áreas seguras.
	• Áreas de entrega y carga.	Control que **no aplica** dentro de biblioteca, debido a que la tipo de actividad económica realizada por la institución.

Equipo.	• Instalación y protección de equipo.	Control que **aplica** dentro de la biblioteca, puesto a que la alta gerencia contrata periódicamente personal capacitado para realizar estas funciones.
	• Servicios de soporte.	Control que **aplica** dentro de la biblioteca, puesto a que la alta gerencia contrata periódicamente personal capacitado para realizar estas funciones.
	• Seguridad en el cableado.	Control que **aplica** dentro de la biblioteca, debido a que el estado del cableado estructurado de la institución se encuentra en óptimas condiciones.
	• Mantenimiento de equipos.	Control que **aplica** dentro de la biblioteca, puesto a que la alta gerencia contrata periódicamente personal capacitado para realizar estas funciones.
	• Retiro de activos.	Control que **aplica** dentro de la biblioteca, cuando la alta gerencia logra la adquisición de nuevos activos para la institución.
	• Seguridad del equipo.	Control que **aplica** dentro de la biblioteca, debido a que la alta gerencia tiene personal a cargo de la vigilancia y aseguramiento de los equipos.
	• Eliminación segura o reúso del equipo.	Control que **aplica** dentro de la biblioteca, debido a que los usuarios no realizan eliminación segura de la información que albergan en sus equipos de cómputo.
	• Equipo de usuario desatendido.	Control que **aplica** dentro de la biblioteca, debido a que los funcionarios de la Organización no aplican ningún método para suspender o hibernar sus equipos, quedando estos desprotegidos a cualquier tipo de riesgo.
	• Política de escritorio limpio y pantalla limpia.	Control que **aplica** dentro de la biblioteca, debido a que el personal administrativo de la Organización no implementa la buena práctica de mantener el escritorio limpio sin ningún tipo de icono o archivos.
SEGURIDAD EN LAS OPERACIONES.		
Procedimientos Operacionales y Responsabilidades.	• Documentación de procedimientos operacionales.	Control que **no aplica** dentro de la biblioteca, debido a que en la institución no cuentan con manuales de procedimientos que le permitan realizar sus labores.
	• Gestión de cambios.	Control que **no aplica** dentro de la biblioteca, debido a que no se realizan e implementen adecuadamente todos los cambios necesarios en la infraestructura y servicios de TI
	• Gestión de la capacidad.	Control que **no aplica** dentro de la biblioteca, debido a que los servicios TI no están respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada.
	• Separación de los ambientes de desarrollo, pruebas y	Control que **no aplica** dentro de la biblioteca, debido a que la Organización no cuenta con ambientes de desarrollo y de operación.

	operación.	
Protección de Software Malicioso	• Controles contra software malicioso.	Control que **aplica** dentro de la biblioteca, debido que dentro de la Organización se pueden realizar controles y políticas para el uso de software contra código malicioso.
Copias de seguridad.	• Respaldo de información.	Control que **aplica** dentro de la biblioteca, debido a que la alta gerencia puede establecer políticas para el respaldo y resguardo de la información crítica de la institución.
Registro de actividad y supervisión.	• Registro de eventos.	Control que **aplica** dentro de la biblioteca, donde se llevara todos los registros de los eventos que realicen lo funcionarios en cada uno de los sistemas de información de la Organización.
	• Protección de registros de información.	Control que **aplica** dentro de la biblioteca, en donde se pueden llevar de forma segura los registros de la información sensible de la institución.
	• Registros de Administrador y Operador.	Control que **aplica** dentro de la biblioteca, en donde se deben registrar las actividades del administrador del sistema y de la operación del sistema.
	• Sincronización de relojes.	Control que **aplica** dentro de la biblioteca, en donde se deben sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.
Control de Software Operacional.	• Instalación de software en sistemas operacionales.	Control que **aplica** dentro de la biblioteca, en donde se debe realizar la instalación de software seguro y confiable en las dependencias que lo requiera para la realización de sus labores.
Gestión de Vulnerabilidades Técnicas.	• Gestión de Vulnerabilidades Técnicas.	Control que **aplica** dentro de la biblioteca, contribuyendo a reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.
	• Restricciones en la instalación de software.	Control que **aplica** dentro de la biblioteca, debido que la alta gerencia debe regular y restringir la instalación de software no seguro para garantizar la integridad, confidencialidad y disponibilidad de la información.
Consideraciones de Auditoria de Sistemas de información.	• Controles de Auditoría de Sistemas de Información.	Control que **aplica** dentro de la biblioteca, debido a que la institución cuenta con una oficina de auditoria interna que le permita hacer seguimiento a los sistemas de información
SEGURIDAD EN LAS TELECOMUNICACIONES.		
Gestión de Seguridad en Red.	• Controles de red.	Control que **aplica** dentro de la biblioteca, en el cual se deben mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.
	• Seguridad de los servicios en red.	Control que **aplica** dentro de la biblioteca, en los cuales la alta gerencia puede implementar herramientas que brinden la seguridad en la red de datos.

	• Segregación en redes	Control que **aplica** dentro de la biblioteca, en donde se debe segregar o dividir los grupos de usuarios, servicios y sistemas de información en las redes, lo cual garantiza la seguridad de la información en cada una de las redes de datos de la institución.
Transferencia de Información.	• Políticas y procedimientos para la transferencia de información.	Control que **aplica** dentro de la biblioteca en la alta gerencia por medio de la política de seguridad de la información establezca procedimiento para la transferencia segura de la información de la institución.
	• Acuerdos en la transferencia de información.	Control que **aplica** dentro de la biblioteca, en donde se deben establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.
	• Mensajería electrónica.	Control que **aplica** dentro de la biblioteca, en donde se proteja adecuadamente la información contenida en la mensajería electrónica. Con herramientas gratuitas que generan firmas codificadas según el formato PKCS#7 o CMS.
	• Acuerdos de confidencialidad o no-revelación	Control que **aplica** dentro de la biblioteca, en los cuales al momento de la contratación el personal administrativo acepte un acuerdo de confidencialidad en las labores en las que se desempeñara.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.		
Requerimientos de Seguridad de Sistemas de Información	• Análisis y especificación de requerimientos de seguridad.	Control que **aplica** dentro de la biblioteca, al momento de adquirir nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad, que garanticen la confidencialidad, integridad y disponibilidad de los datos.
	• Aseguramiento de servicios de aplicación en redes públicas.	Control que **aplica** dentro de la biblioteca, debido que la institución cuenta con aplicaciones en redes públicas.
	• Protección de transacciones de servicios de aplicación.	Control que **aplica** dentro de la biblioteca, debido que la institución cuenta con servicios de aplicación.
Seguridad en los Procesos de Desarrollo y Soporte.	• Política de desarrollo seguro.	Control que **aplica** dentro de la biblioteca. En donde se debe establecer una política por la alta gerencia para el desarrollo de software seguro y confiable.
	• Procedimientos de control de cambios.	Control que **aplica** dentro de la biblioteca, en donde se deberán controlar los cambios en los sistemas y en los recursos de tratamiento de la información.
	• Revisión técnica de aplicaciones después de cambios a la plataforma	Control que **aplica** dentro de la biblioteca, en donde se deberá revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de

	operativa.	la Organización.
	• Restricción de cambios a paquetes de software.	Control que **aplica** dentro de la biblioteca, Se deberá desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.
	• Procedimientos de desarrollo de sistemas.	Control que **aplica** dentro de la biblioteca, en donde se deberán documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.
	• Entorno de desarrollo seguro.	Control que **no aplica** dentro de la biblioteca, en donde el desarrollador no se encuentra en entorno de desarrollo seguro para la realización del software
	• Desarrollo tercerizado.	Control que **aplica** dentro de la biblioteca, debido a que la institución recurre a terceros para el desarrollo de software que le permite realizar los procesos propios de la institución como lo es el Academusoft, SIJADIT, entre otros.
	• Pruebas de seguridad del sistema.	Control que **aplica** dentro de la biblioteca, debido que al momento de adquirir u nuevo software este debe de estar sometido para determinar qué tan segura estará la información almacenada en él.
	• Pruebas de aceptación del sistema.	Control que **aplica** dentro de la biblioteca debido que, dentro de la institución a la hora de adquirir un nuevo software, se debe realizar este tipo de pruebas para determinar el nivel de aceptación que tendrá en la institución.
Datos de Prueba.	• Protección de datos de prueba.	Control que **no aplica** dentro de la biblioteca, debido a que la actividad económica de la Institución no es el desarrollo de software.
RELACIONES CON PROVEEDORES.		
Seguridad en Relaciones con el Proveedor.	• Política de Seguridad de la Información para relaciones con proveedores.	Control que **aplica** dentro de la biblioteca, debido a que la institución al contratar o recibir productos o servicios estos deben de garantizar que se le binde las características primordiales de la información.
	• Atención de tópicos de seguridad dentro de los acuerdos con proveedores.	Control que **aplica** dentro de la biblioteca, debido a que dentro de los contratos establecidos con los proveedores se deben establecer tópicos para la seguridad de la información.
	• Cadena de suministros de TIC.	Control que **aplica** dentro de la biblioteca, debido a las adquisiciones de equipos tecnológicos que realiza la institución con los proveedores.

	• Gestión de Entrega de Servicios de Proveedor.	Control que aplica dentro de la Organización, debido a que los funcionarios encargados de estas labores pueden verificar la adecuada entrega de los servicios
	• Monitoreo y revisión de servicios de proveedor	Control que **aplica** dentro de la biblioteca, debido a que la organización, debe monitorear periódicamente los productos servicios que los proveedores ofrecen.
	• Gestión de cambios a servicios de proveedor.	Control que **aplica** dentro de la biblioteca, puesto que la organización puede gestionar los cambios a los servicios que ofrecen los distintos productos o servicios que ofrecen los proveedores.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.		
Gestión de Incidentes de Seguridad de la Información y Mejoras.	• Responsabilidades y Procedimientos.	Control que **aplica** dentro de la biblioteca, debido a que la alta gerencia debe implementar y asegurar la operación correcta y segura de los recursos y el tratamiento de la información.
	• Reporte de eventos de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca, en el cual se debe llevar un reporte detallado de los eventos ocurridos que involucran la seguridad de la información.
	• Reporte de debilidades de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca, en donde se debe llevar un reporte especificado de los sucesos ocurridos en los cuales se vea comprometidos las características básicas de la información.
	• Valoración y decisión de eventos de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca, en donde la alta gerencia debe tomar medidas preventivas y correctivas sobre los sucesos que hayan comprometido la confidencialidad, integridad y disponibilidad de la información de la institución.
	• Respuesta a incidentes de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca, en donde la alta gerencia implanta planes de contingencia para mitigar el riesgo de pérdida de la información.
	• Aprendizaje de incidentes de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca, en donde los incidentes presentados relacionados con la seguridad de la información sirvan como mecanismos de defensa y acciones correctivas para que los incidentes relacionados con la seguridad de la información no se vuelvan a presentar.
	• Colección de evidencia.	Control que **aplica** dentro de la biblioteca, en donde se realiza la recolección de toda la información con los incidentes y riesgos que se han presentado con respecto a la seguridad de la información.
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.		
Seguridad de la Información en la Continuidad.	• Planeación de Seguridad de la Información en la continuidad.	Control que **aplica** dentro de la biblioteca, en el cual se debe desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del

		negocio.
	• Implementación de Seguridad de la Información en la continuidad.	Control que **aplica** dentro de la biblioteca, en el cual se aplican estándares y metodologías que le permitan a la Organización poder continuar con el sistema de gestión de la seguridad de la información.
	• Verificación, revisión y evaluación de Seguridad de la Información en la continuidad.	Control que **aplica** dentro de la biblioteca, debido que aquí es donde se evalúa los resultados que se obtienen median el ciclo PHVA que estipula la norma, el cual es dinámico en el cual se establecen parámetros para la continuidad del negocio.
CUMPLIMIENTO		
Cumplimiento de los requisitos legales y contractuales	• Identificación de legislación aplicable y requerimientos contractuales.	Control que **aplica** dentro de la biblioteca, en donde se analizan todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Empresa para cumplir con los requisitos, que deben ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización.
	• Derechos de propiedad intelectual (IPR)	Control que **no aplica** dentro de la biblioteca, debido a que dentro de esta no se registra propiedades intelectuales.
	• Protección de información documentada.	Control que **aplica** dentro de la biblioteca, debido a que la información vital de la organización debe ser respaldada.
	• Privacidad y protección de información personal identificable.	Control que **aplica** dentro de la biblioteca, debido a que en la política de Seguridad de la Información debe estar contemplado un capitulo dirigido a la privacidad de la información.
	• Regulación de controles criptográficos.	Control que **no aplica** dentro de la biblioteca, debido a que la institución no cuenta con la infraestructura tecnológica suficiente para implementar estas técnicas de cifrado de datos.
	• Regulación de controles criptográficos.	Control que **no aplica** dentro de la biblioteca, debido a que la institución no cuenta con la infraestructura tecnológica suficiente para implementar estas técnicas de cifrado de datos.
	Revisión independiente de Seguridad de la Información.	Control que **aplica** dentro de la biblioteca, debido después de la implementación de políticas de seguridad de la información, se realiza una análisis independiente muy minucioso de cada una de las partes que conforman el sistema de gestión de seguridad de la información en la organización.
	• Cumplimiento con políticas y	Control que **aplica** dentro de la biblioteca, aquí es donde se verifica por parte de la alta gerencia si se logró el cumplimento de la políticas y de los

	estándares de seguridad.	estándares de seguridad propuestos.
	• Inspección de cumplimiento técnico.	Control que **aplica** dentro de la biblioteca, en este ítem se verifica que el cumplimiento de la política cumpla con todas especificaciones técnicas.
Revisiones de la seguridad de la información.	• Revisión independiente de la seguridad de la información	Control que **aplica** dentro de la biblioteca, debido que se debe de hacer seguimiento y evaluación a la política de seguridad de la información.
	• Cumplimiento de las políticas y normas de seguridad.	Control que **aplica** dentro de la biblioteca, en este ítem se verifica que el cumplimiento de la política cumpla con todas especificaciones técnicas.
	• Comprobación del cumplimiento.	Control que **aplica** dentro de la biblioteca, en este ítem se verifica que el cumplimiento de la política cumpla con todas especificaciones técnicas.

Fuente: Autores del proyecto.