PROPUESTA DE ACTUALIZACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN DE LA EMPRESA CASO DE ESTUDIO, EN LA SEDE MEDELLÍN DE LA ISO 27001:2005 A LA ISO 27001:2013

WILBER ARNULFO GAVIRIA ÁLVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2017

PROPUESTA DE ACTUALIZACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN EMPRESA CASO DE ESTUDIO, EN LA SEDE MEDELLÍN DE LA ISO 27001:2005 A LA ISO 27001:2013

WILBER ARNULFO GAVIRIA ÁLVAREZ

Monografía para optar el título de
Especialista en Seguridad Informática

Asesor

Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLÍN
2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Medellín, septiembre 27 de 2017

A mi familia, Mi madre: María Lillyam del Socorro Álvarez Barrera Q.E.P.D, a mi esposa Viviana Ortiz, a mis hijos: Wilber Stiven, y Yeison Alejandro, por sacrificar su tiempo y espacio para permitirme dedicarme a las labores que demandó este proyecto, por su apoyo incondicional en la realización y alcance de uno de los objetivos de mi vida.

Wilber Gaviria

AGRADECIMIENTOS

Wilber Gaviria expresa sus agradecimientos al:

Esp. Ingeniero de Sistemas. Freddy Enrique Acosta, de la Universidad Nacional Abierta y a Distancia, por su valioso acompañamiento, apoyo y asesoría permanente en el desarrollo de este proyecto.

CONTENIDO

pág.

INTRODUCCIÓN……...15
1. DEFINICIÓN DEL PROBLEMA. 17
1.1 PLANTEAMIENTO DEL PROBLEMA.....17
1.2 FORMULACIÓN DEL PROBLEMA 17
1.3 OBJETIVOS 18
1.3.1 Objetivo General 18
1.3.2 Objetivos Específicos.....18
1.4 JUSTIFICACIÓN.....18
1.5 ALCANCE Y LIMITACIONES 19
1.5.1 Alcance 19
1.5.2 Limitaciones 19
1.6 DISEÑO METODOLÓGICO 20
1.6.1 Población y Muestra.....20
1.6.1.1 Población 20
1.6.1.2 Muestra 21
1.6.1.3 Técnicas e instrumentos de recolección de información…..……21
1.6.2 Paradigma de investigación……..……21
1.6.2.1 Descriptiva……..21
2. MARCO DE REFERENCIA.....22
2.1 MARCO TEÓRICO 22
2.2 MARCO CONCEPTUAL.....28
2.2.1 Políticas de seguridad de la información.....28
2.2.2 Pilares de la seguridad de la información.....28
2.2.3 Declaración de aplicabilidad.....29
2.3 MARCO LEGAL.....29
2.3.1 Ley 527 del 18 de agosto de 1999. 29
2.3.2 Ley 962 de julio 8 de 2005. 29

2.3.3 Ley estatutaria 1266 del 31 de diciembre de 2008. 29
2.3.4 Ley 1273 del 5 de enero de 2009. 30
2.3.5 Ley 1341 del 30 de julio de 2009. 30
2.3.6 Ley estatutaria 1581 de octubre 17 de 2012. 30
2.3.7 Ley 1712 de marzo 6 de 2014. 30
2.3.8 Decreto 1151 de abril 14 de 2008. 31
2.3.9 Decreto número 1377 del 27 de junio de 2013. 31
2.3.10 Decreto número 103 del 20 de enero de 2015. 31
2.3.11 Resolución 2258 del 23 de diciembre de 2009. 31
3. ESTADO ACTUAL DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA EMPRESA CASO DE ESTUDIO, BASADAS EN LA NORMA ISO 27001:2005, IMPLEMENTADAS EN LA SEDE MEDELLÍN. 32
3.1 POLÍTICAS 32
3.1.1 Seguridad física y ambiental 32
3.1.2 Seguridad física y del entorno 33
3.1.3 Seguridad de los equipos 33
3.1.4 Suministro de energía 33
3.1.5 Seguridad del cableado 33
3.1.6 Mantenimiento de los equipos. 34
3.1.7 Destrucción o reutilización segura de equipos 35
3.1.8 Concienciación a los usuarios 35
3.1.9 Normas de escritorios y pantallas limpias 36
3.1.10 Gestión de las comunicaciones y operaciones 36
3.1.11 Procedimiento manejo de incidentes 36
3.1.12 Gestión de la prestación de servicios por terceras partes 36
3.1.13 Protección contra código malicioso 37
3.1.14 Controles de las redes 39
3.1.15 Acceso a internet 40
3.1.16 Uso de utilitarios del sistema 40

3.2 CONTROLES 40
4. COMPARATIVO DE LA NORMA ISO 27001:2005 CON ISO 27001:2013. 46
5. IDENTIFICACIÓN DE LOS CONTROLES QUE SERÁN PROPUESTOS PARA SU APLICACIÓN EN LA SEDE MEDELLÍN DE LA EMPRESA CASO DE ESTUDIO, ESTABLECIDOS EN EL ANEXO A DE LA NORMA ISO 27001:2013. 53
6. PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LA NORMA ISO 27001:2013, PARA LA SEDE MEDELLÍN. 72
6.1 Política de seguridad de la información 72
6.1.1 Política para dispositivos móviles 72
6.1.2 Política seguridad de los recursos humanos 73
6.1.3 Política de control de acceso 74
6.1.4 Política sobre el uso de controles criptográficos 75
6.1.5 Política de escritorio y pantalla limpia. 76
6.1.6 Política Protección contra código malicioso 77
6.1.7 Política y procedimiento de transferencia de información 78
6.1.8 Política de desarrollo seguro. 79
6.1.9 Política de seguridad de la información para las relaciones con proveedores 80
6.1.10 Política gestión de incidentes 81
6.1.11 Política gestión de continuidad del negocio 82
6.1.12 Política de gestión de activos 83
6.1.13 Política de gestión de contraseñas 84
6.1.14 Política de clasificación de la información 85
RECOMENDACIONES 87
CONCLUSIONES 88
7. BIBLIOGRAFÍA 89

LISTA DE CUADROS

pág.

Cuadro 1. Controles de seguridad de la información del sistema de gestión de seguridad de la Empresa caso de estudio implementadas en la sede Medellín...……41
Cuadro 2. Comparativo Anexo norma ISO 27001:2005-2013…..... 46
Cuadro 3. Comparativo de las cláusulas de seguridad de la información de la ISO 27001:2005-2013……..….47
Cuadro 4. Comparativos controles establecidos en la norma ISO 27001:2005 e ISO 27001:2013……..…….....47
Cuadro 5. Propuesta de controles de la seguridad de la información bajo la norma ISO 27001:2013……..……..…….……53

LISTA DE FIGURAS

pág.

Figura 1. Ciclo PHVA ……..27
Figura 2. Pilares de la seguridad de la información……28
Figura 3: Antivirus implementado para la seguridad en la plataforma tecnológica de la empresa caso de estudio…….38

GLOSARIO

Para dar claridad a los términos utilizados en el presente proyecto de grado, se enuncian las siguientes definiciones, las cuales son tomadas del "manual del sistema de gestión de seguridad de la información"[1] para la Empresa caso de estudio.

ACTIVO DE INFORMACIÓN: de acuerdo con la norma ISO 27001, un activo de información es "cualquier cosa que tenga valor para la organización y en consecuencia deba ser protegido". No obstante, este concepto es bastante amplio, y debe ser limitado por una serie de consideraciones: el impacto que para la empresa supone la pérdida de confidencialidad, integridad o disponibilidad de cada activo, el tipo de información que maneja en términos de su sensibilidad y criticidad y sus productores y consumidores. Los activos de información se traducen en dispositivos tecnológicos, archivos, bases de datos, documentación física, personas, sistemas de información, entre otros.

AUTENTICACIÓN: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CONFIDENCIALIDAD: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

DISPONIBILIDAD: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

DISPOSITIVOS DE ALMACENAMIENTO: materiales físicos donde se almacenan datos.

DOCUMENTOS DE ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: son documentos en los que los empleados de la Empresa caso de estudio o provistos por terceras partes aceptan acatar la Política de Seguridad de la Información y se acogen a las sanciones establecidas por el incumplimiento de dicha política.

HARDWARE: cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con el computador. Incluye elementos internos como el disco duro, CD-ROM, y también hace referencia al cableado, circuitos, gabinete, etc. E incluso a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

1 Manual del Sistema de Gestión de Seguridad de la Información de la empresa caso de estudio.

IP: es una dirección o etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol).

INCIDENTE DE SEGURIDAD: es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación, o inminente amenaza de violación de la Política de Seguridad de la Información.

INTEGRIDAD: es la protección de la exactitud y estado completo de los activos.

OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN (TI): Cumple la función de cubrir los requerimientos de seguridad de la información establecidos para la operación, administración, comunicación de los recursos de tecnología de la empresa caso de estudio. Así mismo debe efectuar las tareas de desarrollo y mantenimiento de sistemas de información, siguiendo una metodología de ciclo de vida de sistemas apropiada, la cual debe contemplar medidas de seguridad.

PERFILES DE USUARIO: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

SISTEMA DE INFORMACIÓN: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Empresa caso de estudio o de origen externo ya sea adquirido por la empresa como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SOFTWARE: es todo programa o aplicación programada para realizar tareas específicas.

SOFTWARE MALICIOSO: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

TIC: tecnologías de la información y las comunicaciones.

VULNERABILIDADES: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa (amenazas), las cuales se constituyen en fuentes de riesgo.

RESUMEN

En la presente propuesta de actualización de los controles y las políticas de seguridad de la información, se tomó como base el estado actual de lo ya dispuesto en la empresa caso de estudio bajo la norma ISO 27001:2005, lo que nos permitió determinar las fortalezas y debilidades que se tienen frente a los activos de información, realizando la comparación de estos con lo establecido en la norma ISO 27001:2013, información que nos ayuda a generar estrategias que minimizan las amenazas que puedan impactar las vulnerabilidades de la organización, dando a conocer los controles y políticas que deben ser implementadas, las cuales son producto del análisis de lo que posee implementado la empresa en mención, lo que aportara al fortalecimiento del sistema de seguridad de la información de la organización, como un proceso de mejora continua que requiere la actualización permanente.

Palabras Claves: seguridad, información, controles, políticas.

ABSTRACT

In the present proposal to update the information security policies and controls, the current status of the already established company case study under ISO 27001: 2005 was taken as a basis, which allowed us to determine the strengths and weaknesses that are faced with information assets, comparing these with ISO 27001: 2013, information that helps us to generate strategies that minimize the threats that can impact the vulnerabilities of the organization, giving know the controls and policies that must be implemented, which are the product of the analysis of what has the company implemented, which will contribute to the strengthening of the information security system of the organization, as a process of continuous improvement that requires the permanent update.

Keywords: security, information, controls, policies.

INTRODUCCIÓN

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Teniendo en cuenta lo que dice LOPEZ NEIRA y RUIZ SPOHR[2], los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

Cada día las organizaciones se enfrentan a demandas en la rentabilidad, la calidad y la seguridad que estimulan el desarrollo sostenible. La norma ISO 27001 ayuda a establecer un Sistema de Gestión de Seguridad de la Información eficiente que permite convertir estas presiones en una ventaja competitiva frente a otras organizaciones del mismo sector.

Las empresas para poder hacer frente a todos los retos a los que se enfrentan cada día, tienen que desarrollar procesos y estándares que midan y cumplan con dichos estándares que integran todos los principios de negocio en los Sistemas de Gestión. Algunas organizaciones utilizan el Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001[3].

Hoy en día la norma ISO 27001 se ha convertido en una herramienta muy importante en las organizaciones, lo que permitió para la empresa caso de estudio la implementación de su Sistema de Gestión de Seguridad de la Información, el cual se basa en sus inicios en la norma ISO/IEC 27001:2005.

El cambio de la norma ha obligado a la empresa a tener que realizar la mejora continua, es por esto que se ha planteado llevar el Sistema de Gestión de Seguridad de la Información a la norma ISO/IEC 27001:2013, mostrando con esto que la empresa está garantizando la confidencialidad, integridad y disponibilidad de la información de cada uno de sus clientes, y con esto aumentar la confianza en el manejo de la misma.

En esta monografía se muestra en primera medida el estado actual de la políticas de seguridad que se están implementadas hoy en día en la organización, donde se

[2] LOPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. Sistema de Gestión de la Seguridad de la Información. Madrid. 2005. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

3 ISOTools Excellence. (07 de Mayo de 2015). Sistema de Gestión de Seguridad de la Información. Blog especializado en sistemas de gestión de la seguridad informática [Blog]. Disponible en internet: http://www.pmg-ssi.com/

muestra que cada una de ellas busca es proteger los activos de la información como insumo fundamental para el cumplimiento de la misión y asegurar la supervivencia de la empresa, administrándola y protegiéndola a través de la aplicación efectiva de las mejores prácticas y controles, garantizando la gobernabilidad del país.

Continuo a esto se hace un paralelo entre de los dos escenarios donde se enlista cada una de las cláusulas de la norma ISO/IEC 27001:2005 frente a la norma ISO/IEC 27001:2013, lo que conllevo a realizar el comparativo entre la normas y de esta manera se determinan las modificaciones a realizar, posteriormente se aplica los controles del anexo A de la norma ISO/IEC 27001:2013 para de esta manera determinar las nuevas políticas de seguridad de la información, que se implementarán dentro de la empresa caso de estudio.

1. DEFINICIÓN DEL PROBLEMA.

1.1 PLANTEAMIENTO DEL PROBLEMA

Dada la actualización de la norma ISO 27001:2005, y a que los controles establecidos en la sede Medellín de la empresa caso de estudio, fueron basados en dicha norma, se requiere la actualización de estos, para garantizar la seguridad de la información, identificando los que no se encuentren ajustados a la norma ISO-27001:2013, así como aspectos de mejora en el sistema de gestión de la seguridad de la información, para la construcción de la declaración de aplicabilidad (controles del anexo A de la norma ISO 27001:2013.).

De la misma manera se requiere la realización de un nuevo Manual del Sistema de Gestión de Seguridad de la Información, donde se dé a conocer a todos los integrantes de la empresa dichos controles y su alcance, generando una unidad de criterio en lo referente a la política de seguridad de la información, el establecimiento normas, procedimientos y la asignación de responsabilidades con la seguridad de la información.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la actualización de los controles de la seguridad de la información de la norma ISO 27001:2005 a la ISO 27001:2013 aporta a la seguridad de la sede Medellín?

1.3 OBJETIVOS

1.3.1 Objetivo General

Proponer la actualización de políticas de seguridad de la información del sistema de gestión de la información de la empresa caso de estudio, en la sede Medellín de la ISO 27001:2005 a la ISO 27001:2013.

1.3.2 Objetivos Específicos

Revisar el estado actual de las políticas de seguridad de la información del sistema de gestión de seguridad de la empresa caso de estudio, basado en la norma ISO 27001:2005, implementadas en la sede Medellín.

Comparar los controles establecidos en la norma ISO 27001:2005 e ISO 27001:2013.

Identificar los controles de la norma ISO 27001:2013 que serán aplicados en la sede Medellín.

Plantear las políticas de seguridad de la información a establecer en la sede Medellín.

1.4 JUSTIFICACIÓN

La seguridad de la información es un factor importante dentro de la empresa caso de estudio, siendo esta una de las instituciones más grandes del país tanto en infraestructura como recurso humano, es de tener en cuenta que dentro de la parte misional de la empresa se hace necesario que todo los empleados tengan acceso a los diferentes aplicativos y bases de datos que se poseen, por la cual cada sede

requiere implementar y adecuar su plataforma tecnológica a fin de identificar y minimizar vulnerabilidades que puedan poner en riesgo el acceso a la información.

Por lo anterior la sede Medellín de la empresa caso de estudio, en su afán de mejora, el cuidado y uso de la información, se dio a la tarea de actualizar los controles adoptados en la norma ISO 27001:2005, a los establecidos en la norma ISO 27001:2013, los cuales mejoran el sistema de gestión de seguridad de la información, para una adecuada gestión del riesgo y fortalecimiento de la seguridad de la empresa ante posibles amenazas que afecten su continuidad.

Esto nos permite proteger los activos de la información, los cuales son insumo fundamental para el cumplimiento de la misión y asegurar el fortalecimiento permanente de la empresa, mediante la aplicación efectiva de mejores prácticas y controles, que contribuyan a alcanzar los estándares de calidad, seguridad y ciclo de vida de la información, en cumplimiento a los lineamientos establecidos por la empresa y la normatividad vigente.

1.5 ALCANCE Y LIMITACIONES

1.5.1 Alcance

La presente monografía se encuentra entre los proyectos de gestión de seguridad y lo que pretende es la actualización de políticas de seguridad de la información del sistema de gestión de la información de la empresa caso de estudio, en la sede Medellín de la ISO 27001:2005 a la ISO 27001:2013.

1.5.2 Limitaciones

Es conveniente resaltar que el desarrollo de la presente monografía no se abarcara los temas que se definen a continuación:

- No se realizará la implementación de los controles propuestos basados en la norma ISO 27001:2013, en la sede Medellín, ya que estos deben ser elevados a la sede central para su aprobación.
- La empresa caso de estudio no permite que se publique su nombre dentro del proyecto, al igual que se dé información relacionada con los sistemas de información, políticas, procedimientos y formatos establecidos en el manual de seguridad de su información, debido a que debe garantizar la integridad, confidencialidad y disponibilidad de su información.

1.6 DISEÑO METODOLÓGICO

1.6.1 Población y Muestra

1.6.1.1 Población

La población seleccionada es el personal y los activos informáticos de la empresa caso de estudio del departamento de Antioquia.

1.6.1.2 Muestra

La población a la cual va dirigido el proyecto, es la sede Medellín de la empresa caso de estudio, lo que redundara en la seguridad de la información de los clientes internos y externos.

La muestra es intencionada, ya que no se obtiene de un proceso de selección aleatoria, sino que los sujetos de la muestra son seleccionados en función de su accesibilidad o a criterio personal e intencional del investigador, teniendo en cuenta el cargo, el perfil y las funciones que tiene el empleado.

1.6.1.3 Técnicas e instrumentos de recolección de información.

Para la obtención de información se utilizó la técnica de entrevista, la cual se realizó al personal, la observación directa de los activos informáticos y la revisión documental la empresa con sede Medellín.

1.6.2 Paradigma de investigación

La investigación es cuantitativa y el método definido en esta monografía teniendo en cuenta los tipos de investigación planteados según Hurtado de Barrera[4] (2000), en su libro "Metodología de la investigación holística", es de tipo descriptiva, puesto que se conoce el estado actual de los controles de la seguridad de la información establecidos, a partir de los cuales se espera identificar y definir los que apliquen bajo la norma ISO/IEC 27001:2013, para su respectiva propuesta de actualización.

1.6.2.1 Descriptiva

La investigación descriptiva[5] tiene como objeto central lograr la descripción o caracterización del evento de estudio dentro de un contexto particular.

4 HURTADO DE BARRERA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. p. 20.
5 Ibid., p. 222.

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

2.1.1 Seguridad de la información

Es la protección de la información que hay en una entidad o que un individuo maneja. Esta información representa un activo valioso para la organización.

La información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad redes sistemas de información). Según la ISO/IEC 17799 [6], la información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

En ISO/IEC 17799 [7], la seguridad de la información se alcanza implementando un conjunto adecuado de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

[6] ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. s.l.: s.n., 2005. [citado el 19-04-16]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[7] Ibid. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

2.1.2. Sistema de gestión de la seguridad de la información

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta que sirve de ayuda a las diferentes empresas, para implementar políticas, procedimientos y controles de seguridad informática acordes con los objetivos del negocio.

Teniendo en cuenta el concepto establecido en la norma ISO 27001:2005[8], este es parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

2.1.3 Familia de las normas ISO/IEC 27000

Es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia, tiene algunas similitudes a la familia de las normas de gestión de la calidad ISO 9000. Cada una de las normas de la familia 27000[9], define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas.

2.1.3.1 Alcance de la norma ISO/IEC 27000. ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones etc.

[8] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá, D.C.: El Instituto 2006. Pág. 3.

[9] ISO 27000.ES, El portal de ISO 27001 en español, Op. Cit. Disponible en: http://www.iso27000.es/iso27000.html

Según VARGAS, y CASTRO MATTEI[10], no se debe centrar la atención solamente en los sistemas informáticos por mucho que tengan hoy en día una importancia más que relevante en el tratamiento de la información ya que de otra forma, se podría dejar sin proteger información que puede ser esencial para la actividad de la empresa.

A continuación, se exponen las Normas relacionadas con la ISO 27000:

- **ISO/IEC 27000.** Publicada 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español.

- **Norma ISO 27001: 2005:** Norma elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del sistema de gestión de la seguridad de la información (SGSI), adoptando el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), que se aplica para estructurar todos los procesos del SGSI[11].

[10]VARGAS, Ana Cecilia y CASTRO MATTEI, Alonso. Sistemas de gestión de seguridad de la información [en línea]. San José Costa Rica: Universidad de Costa Rica, s.f. [citado el 22-04-16]. Disponible en: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

[11] Ibid., Pág. I.

- **ISO/IEC 27001.** Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.

- **Norma ISO 27001: 2013**: Norma elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continúa de un sistema de gestión de la seguridad de la información.

Según ISO/IEC 27001[12], el sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

- **ISO/IEC 27002.** Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

Actualmente, la última edición de 2013 de este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013.

[12] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información. Requisitos. NTC-ISO/IEC 27001. Bogotá, D.C.: El Instituto 2013. Pág. I.

- **ISO/IEC 27003.** Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

- **ISO/IEC 27004.** Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

- **ISO/IEC 27005.** Publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información.

- **ISO/IEC 27006.** Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007) y revisada el 30 de Septiembre de 2015. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

- **ISO/IEC 27007.** Publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

- **ISO/IEC TR 27008**[13]**.** Publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida.

[13] ISO 27000.ES, El portal de ISO 27001 en español, Op. Cit. Disponible en: http://www.iso27000.es/iso27000.html

2.1.4. Ciclo PHVA

Según lo relatado por Bernal[14], es una herramienta para la mejora continua, que fue presentada por Edwards Deming desde el año 1950, la cual se basa en un ciclo de 4 pasos: Planificar, Hacer, Verificar y Actuar. En inglés se conoce como PDCA: Plan, Do, Check, Act. Figura 1.

Esta metodología es la más utilizada en la implementación de sistemas de gestión.
Planificar: implica identificar un objetivo o meta, y ponerlo en acción.
Hacer: en el que se pone en marcha la implementación de lo planeado,
Verificar: que es en el que se monitorean los resultados para probar la efectividad del plan, los problemas y acciones de mejora.
Actuar: el cual integra el aprendizaje obtenido en dicho ciclo, lo que nos permite realizar los ajustes necesarios como parte de la mejora continua.

Figura 1. Ciclo PHVA.

Fuente. http://toddleoutsourcing.es/wp-content/uploads/2014/04/sgsi_pdca.jpg

[14] BERNAL, Jorge Jimeno. (2013). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. Disponible en: http://www.pdcahome.com/5202/ciclo-pdca/

2.2 MARCO CONCEPTUAL

2.2.1 Políticas de seguridad de la información

La política de seguridad de la información es un conjunto de procedimientos establecidos en una organización, para regular y garantizar el uso de la información de manera segura al interior de la misma.

2.2.2 Pilares de la seguridad de la información

El Sistema de Gestión de Seguridad de la Información, busca garantizar la protección de la información, basado en tres pilares fundamentales: Ver Figura 2.

- Confidencialidad[15]**:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Integridad[16]**:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- Disponibilidad[17]**:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Figura 2. Pilares de la seguridad de la información.

Fuente. Propiedad del autor.

[15] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá, D.C.: El Instituto 2013. p. 2.
[16] Ibid., p. 3.
[17] Ibid., p. 2.

2.2.3 Declaración de aplicabilidad[18]

La llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

2.3 MARCO LEGAL

2.3.1 Ley 527 del 18 de agosto 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" [19].

2.3.2 Ley 962 de julio 8 de 2005.

"Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos" [20].

2.3.3 Ley estatutaria 1266 del 31 de diciembre de 2008.

"Por la cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información" [21].

[18] ISO 27000, (2013). Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf p.14Ibid., p. 14.
[19] CONGRESO DE LA REPUBLICA. Ley 527. (21, agosto, 1999). Bogotá, D.C., Colombia. Diario Oficial 43673 de agosto 21 de 1999. p. 1-19.
[20] CONGRESO DE LA REPUBLICA. Ley 962. (8, julio, 2005). Bogotá, D.C., Colombia. Diario Oficial. 46.023 de julio 8 de 2005. p.1-17.
[21] CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Bogotá, D.C., Colombia. Diario Oficial 47.219. de 31 de diciembre de 2008. p.1-17.

2.3.4 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"[22].

2.3.5 Ley 1341 del 30 de julio de 2009.

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones" [23].

2.3.6 Ley estatutaria 1581 de octubre 17 de 2012.

"Por la cual se dictan disposiciones generales para la protección de datos personales" [24].

2.3.7 Ley 1712 de marzo 6 de 2014.

"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" [25].

[22] CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Bogotá, D.C., Colombia. Diario Oficial. 47.223 de enero 5 de 2009. p. 5-6.
[23] CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio, 2009). Bogotá, D.C., Colombia. Diario Oficial. 47426 de julio 30 de 2009. p. 1-34.
[24] CONGRESO DE LA REPUBLICA. Ley 1581. (17, octubre, 2012). Bogotá, D.C., Colombia. Diario Oficial. 48.587 de octubre 17 de 2012. p. 1-15.
[25] CONGRESO DE LA REPUBLICA. Ley 1712. (06, marzo, 2014). Bogotá, D.C., Colombia. Diario Oficial. 49084 de marzo 6 de 2014. p. 1-14.

2.3.8 Decreto 1151 de abril 14 de 2008.

"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones" [26].

2.3.9 Decreto número 1377 del 27 de junio de 2013.

"Por el cual se reglamenta parcialmente la Ley 1581 de 2012" [27].

2.3.10 Decreto número 103 del 20 de enero de 2015.

"Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones"[28].

2.3.11 Resolución 2258 del 23 de diciembre de 2009.

"Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007" [29].

[26] CONGRESO DE LA REPUBLICA. Decreto 1151. (14, abril, 2008). Bogotá, D.C., Colombia. Diario Oficial. 46960 de abril 14 de 2008.p. 1-4.
[27] CONGRESO DE LA REPUBLICA. Decreto 1377. (27, junio, 2013). Bogotá, D.C., Colombia. Diario Oficial. 48834 de junio 27 de 2013. p. 1-11.
[28] CONGRESO DE LA REPUBLICA. Decreto 103. (20, enero, 2015). Bogotá, D.C., Colombia. Diario Oficial. 49400 de enero 20 de 2015. p.1-16.
[29] COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 2258. (23, diciembre, 2009). Bogotá, D.C., Colombia. Diario Oficial. 47572 de diciembre 23 de 2009. p. 1-6.

3. ESTADO ACTUAL DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA EMPRESA CASO DE ESTUDIO, BASADAS EN LA NORMA ISO 27001:2005, IMPLEMENTADAS EN LA SEDE MEDELLÍN.

La empresa caso de estudio mediante la implementación del “Sistema de Gestión de Seguridad de la Información”, busca proteger los activos de la información como insumo fundamental para el cumplimiento de la misión y asegurar la supervivencia de la empresa, administrándola y protegiéndola a través de la aplicación efectiva de las mejores prácticas y controles, teniendo en cuenta este precepto se identifican y se dan a conocer las políticas y controles de la seguridad de la información, establecidos por la misma, basados en la norma ISO 27001:2005, extraídos del manual de seguridad de la información de la empresa caso de estudio.

3.1 POLÍTICAS

Con el fin de salvaguardar los activos de información, la sede Medellín, adopto el Manual del Sistema de Gestión de Seguridad de la Información de la empresa caso de estudio, implementando las siguientes políticas, como una estrategia de seguridad basada en las mejores prácticas y controles, resguardando los activos de información de las amenazas que se ciernen sobre ellos, así:

3.1.1 Seguridad física y ambiental

Busca proteger los activos de información de las amenazas naturales y ambientales como inundaciones, terremotos, tormentas, tornados e incendios; de las amenazas por interrupción de servicios públicos; de las amenazas artificiales como acceso no autorizado (tanto internos como externos), explosiones, daños por empleados, vandalismo, fraude, robo, y finalmente de las amenazas por motivos políticos como huelgas, disturbios, desobediencia civil, ataques terroristas y bombardeos.

3.1.2 Seguridad física y del entorno

Implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de las instalaciones de la empresa caso de estudio, del mismo modo, controlar las amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones.

3.1.3 Seguridad de los equipos

Los equipos de cómputo son ubicados y protegidos para reducir la exposición a riesgos ocasionados por amenazas ambientales y de acceso no autorizado.

3.1.4 Suministro de energía

Los centros de procesamiento de datos están protegidos con respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía está de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía.

3.1.5 Seguridad del cableado

Para el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información para protegerlos contra intercepción o daño:

- Se cumple con el reglamento técnico de instalaciones eléctricas – RETIE, expedido por el Ministerio de Minas y Energía.
- Se cumple con los estándares ISO/IEC/11801, ANSI/EIA/TIA 568A o 568B o con la reglamentación vigente expedida al respecto.
- Las instalaciones de cableado estructurado están protegidas contra la influencia o daño causado por agentes externos.
- Los elementos metálicos que forman parte de los cableados estructurados están conectados al sistema de tierras del edificio.

- Los equipos se albergan en sitios acondicionados a temperaturas entre 16 y 22 grados centígrados.
- Los centros de cableado cuentan con rack para alojar los equipos y terminaciones de los cableados cumpliendo las normas técnicas y asegurados con chapas o cerraduras de seguridad, cuyas llaves sean administradas por personal técnico capacitado.
- Las instalaciones se realizan siguiendo la arquitectura de los edificios, debidamente protegidos con canaleta en caso de instalación interior, o con tubo metálico en caso de instalación tipo intemperie.

3.1.6 Mantenimiento de los equipos.

El mantenimiento a la plataforma tecnológica posibilita su disponibilidad e integridad, teniendo en cuenta los siguientes controles:

- Mantenimiento preventivo a los equipos de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.
- Uso de un sistema de información que permite llevar el control del detalle de la frecuencia de mantenimiento de los equipos.
- Sólo el personal de mantenimiento autorizado puede llevar a cabo reparaciones en los equipos.
- El responsable técnico de los equipos registra de todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- El responsable técnico de los equipos registra el retiro los equipos de las instalaciones de la empresa caso de estudio para su mantenimiento.
- En las especificaciones técnicas para contratos de mantenimiento o garantía se contempla el suministro de nuevos discos sin realizar la entrega del disco dañado.
- Seguridad de los equipos fuera de las instalaciones: El uso de equipos institucionales, fuera de las instalaciones, está restringido a equipos

portátiles y móviles, y su uso está regulado por el procedimiento de uso de dispositivos móviles.

La seguridad para estos equipos es equivalente a la suministrada dentro de las instalaciones empresa y controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso de estos, así:

- Los equipos móviles institucionales, no pueden conectarse a redes inalámbricas públicas o no conocidas.
- El software instalado en los dispositivos móviles está totalmente licenciado y avalado por la Oficina de Tecnologías de la Información (TI).
- El acceso a los equipos móviles se realiza mediante el uso de usuario y contraseña.
- La información almacenada en los equipos de cómputo portátiles está cifrada.

3.1.7 Destrucción o reutilización segura de equipos

Se realiza borrado seguro de la información o destrucción física del dispositivo de almacenamiento, antes de la reutilización o devolución de cualquier equipo de cómputo.

El borrado seguro y destrucción de dispositivos de almacenamiento, está regulado por el procedimiento de destrucción o reutilización segura de equipos.

3.1.8 Concienciación a los usuarios

Garantizar que los empleados, así como el personal externo vinculado a la empresa, cuenten con el nivel deseado de conocimiento para la correcta gestión de los activos de información, para lo cual se realizaran charlas y actividades pedagógicas para la enseñanza del Manual del Sistema de Gestión de Seguridad de la Información de la Empresa caso de estudio promoviendo la concienciación en seguridad de la información, la protección, uso y procesamiento de la misma.

3.1.9 Normas de escritorios y pantallas limpias

Estas normas tienen como fin reducir los riesgos de acceso no autorizado, pérdida y daño de la información. Entre las que se encuentran las siguientes:

- Almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.
- Guardar bajo llave la información clasificada en nivel 3 o superior (preferiblemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso.
- Bloquear la sesión de los computadores personales cuando no se está usando. El protector de pantalla se activa en forma automática después de cinco (5) minutos de inactividad.
- Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
- Bloquear las fotocopiadoras fuera del horario normal de trabajo.
- Retirar inmediatamente la información sensible, una vez impresa.
- Los escritorios de los equipos de cómputo no deben tener accesos directos a archivos.

3.1.10 Gestión de las comunicaciones y operaciones

El proceso de Direccionamiento Tecnológico de la Empresa caso de estudio, es el encargado de la operación y administración de la plataforma tecnológica como soporte a los procesos de la empresa, asigna funciones específicas a sus empleados quienes deben garantizar la adecuada operación y administración de dicha plataforma. Así mismo, vela por la eficiencia de los controles implantados en los procesos y procedimientos asociados con el objeto de garantizar la confidencialidad, la integridad y la disponibilidad de la información.

3.1.11 Procedimiento manejo de incidentes

El manejo de incidentes se realiza acorde con el procedimiento “Atención a Incidentes”, el cual garantiza una respuesta rápida, eficaz y sistemática a los incidentes relativos a la seguridad de la información.

Los incidentes que así lo requieran cuentan con la asesoría de la Policía Judicial, para el manejo de la evidencia digital y posible judicialización.

3.1.12 Gestión de la prestación de servicios por terceras partes

La tercerización de la plataforma tecnológica de la empresa caso de estudio, está supeditada a los controles establecidos en el contrato, para la entrega del servicio a estos, se debe asegurar que tengan implementado, operen y mantengan los controles de seguridad, definidos en el servicio y niveles de entrega incluidos en el contrato.

3.1.13 Protección contra código malicioso

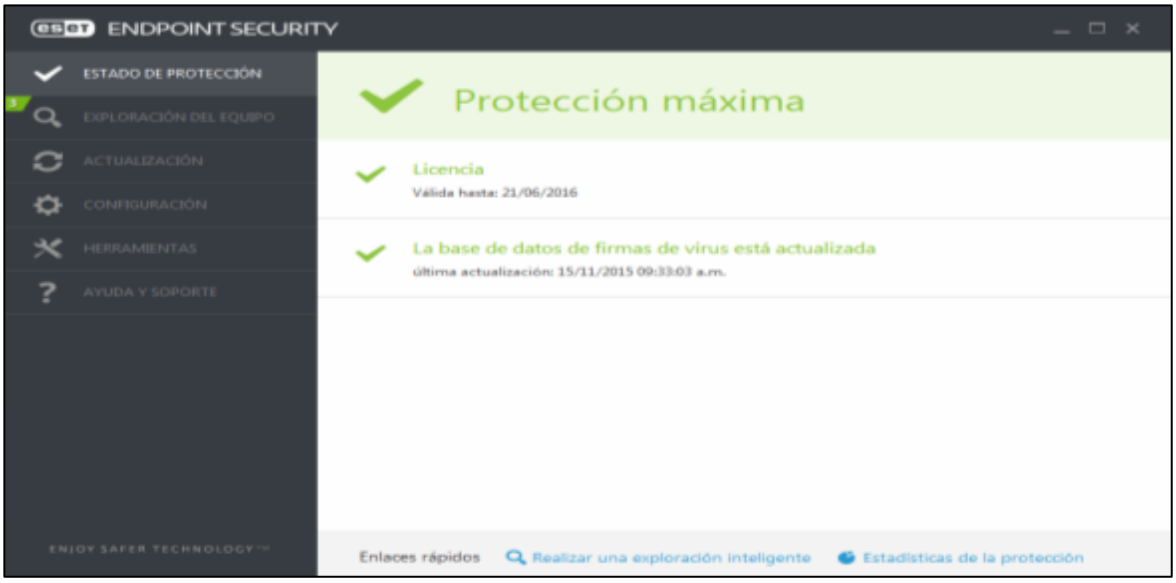
El proceso de Direccionamiento Tecnológico de la empresa caso de estudio, implementa controles para prevenir y detectar código malicioso, lo cual se basa en software, concienciación de usuarios y gestión del cambio.

Los controles implementados contemplan las siguientes directrices:

- No permite el uso de software no autorizado por la Oficina de Tecnologías de la información (TI).
- No permite el intercambio de información a través de archivos planos.
- No compartir carpetas en los equipos de cómputo.
- Instala y actualiza software de detección y reparación de virus, IPS de host, antispyware examinado computadores y medios informáticos, como medida preventiva y rutinaria.
- Mantiene los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.

- Revisa periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verifica antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientiza al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

Figura 3: Antivirus implementado para la seguridad en la plataforma tecnológica de la empresa caso de estudio.



Fuente. Propiedad del autor.

El responsable del ciclo de vida de la información, junto con los propietarios de los activos de información determina los requerimientos de respaldo, según el nivel de criticidad de la información y control de registros.

El procedimiento de resguardo de la información incluye actividades de prueba de recuperación de la información. Las instalaciones de resguardo garantizan las condiciones de seguridad y ambientales necesarias para la conservación de los respaldos.

El procedimiento de respaldo contempla las siguientes directrices:

- Un esquema de rótulo de las copias de respaldo, para permitir su fácil identificación.
- Destrucción de las copias de respaldo, cuando se venza la vida útil de los medios de almacenamiento, de acuerdo con el procedimiento de destrucción o reutilización segura de equipos.
- Almacenamiento de las copias de respaldo en un lugar fuera de las instalaciones del lugar de origen de la información, con un registro exacto y completo de cada una de ellas, así como los procedimientos de restauración.
- Almacenamiento de al menos 3 ciclos de información de copias de respaldo para la información.
- La información respaldada en el sitio alterno considera los niveles de clasificación
- Almacenamiento de las copias de respaldo en condiciones de seguridad y ambientales adecuadas, consistentes a las aplicadas al sitio principal.
- Pruebas periódicas de la restauración de los medios de respaldo, según lo estipulado en el Plan de Continuidad del Negocio.

3.1.14 Controles de las redes

El proceso de Direccionamiento Tecnológico define los controles de seguridad de la red de datos Institucional, para lo cual usa como referencia el estándar ISO/IEC 18028 Tecnología de la información-Técnicas de seguridad – la seguridad de TI de la Red.

Estos controles contemplan salvaguardas especiales para:

- Los equipos activos de las redes LAN, de las sedes de Policía a nivel nacional.
- Mantener la disponibilidad de los servicios de red e infraestructura tecnológica conectada a ella.
- Transmisión de información a través de redes públicas.

- Acceso a la red institucional, desde otras redes.
- Intercambio de información interinstitucional con el sector público y privado.
- Garantizar la trazabilidad de las conexiones a la red institucional.
- Supervisión del cumplimiento de los controles implementados.

3.1.15 Acceso a internet

La empresa caso de estudio, provee a través de un Prestador de Servicios de Internet, el servicio de internet comercial, el cual es administrado por el proceso de direccionamiento tecnológico y es el único servicio de internet autorizado. Este servicio se ajustará al artículo 26 relación con terceros.

- El acceso a internet requiere de la autenticación de los usuarios, mediante el uso de usuario y contraseña.
- El uso de internet está regulado por los términos de uso adecuado del internet.

3.1.16 Uso de utilitarios del sistema

El uso de utilitarios licenciados del sistema está restringido a usuarios administradores. Se estableció una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema.
Ningún usuario final, tiene privilegios de usuario administrador

3.2 CONTROLES

Controles implementados actualmente en la empresa caso de estudio de acuerdo al Manual del Sistema de Gestión de Seguridad de la Información.

Cuadro 1. Controles de seguridad de la información del sistema de gestión de seguridad de la empresa caso de estudio implementadas en la sede Medellín.

ISO 27001:2005	
ID. CONTROL	**NOMBRE CONTROL**
A.5	**POLÍTICA DE SEGURIDAD**
A.5.1	**Política de seguridad de la información**
A.5.1.1	Documento de Política de seguridad de la información
A.5.1.2	Revisión de la política de seguridad de la información
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
A.6.1	**Organización Interna**
A.6.1.1	Compromiso de la dirección con la seguridad de la información
A.6.1.2	Coordinación de la seguridad de la información
A.6.1.3	Asignación de responsabilidades para la seguridad de la información
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información
A.6.1.5	Acuerdos sobre confidencialidad
A.6.1.6	Contacto con las autoridades
A.6.1.7	Contacto con grupos de interés especiales
A.6.1.8	Revisión independiente de la seguridad de la información
A.6.2	**Partes Externas**
A.6.2.1	Identificación de los riesgos relacionados con las partes externas
A.6.2.2	Consideraciones de la seguridad cuando se trata de clientes
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes
A.7	**GESTIÓN DE ACTIVOS**
A.7.1	**Responsabilidad por los activos**
A.7.1.1	Inventarios de Activos
A.7.1.2	Propiedad de los Activos
A.7.1.3	Uso aceptable de los activos
A.7.2	**Clasificación de la información**
A.7.2.1	Directrices de clasificación
A.7.2.2	Etiquetado y manejo de la información
A.8	**SEGURIDAD DE LOS RECURSOS HUMANOS**
A.8.1	**Antes de la contratación laboral**
A.8.1.1	Roles y Responsabilidades
A.8.1.2	Selección
A.8.1.3	Términos y condiciones laborales
A.8.2	**Durante la vigencia de la contratación laboral**
A.8.2.1	Responsabilidades de la dirección
A.8.2.2	Educación, formación y concienciación sobre la seguridad de la información
A.8.2.3	Proceso Disciplinario
A.8.3	**Terminación o cambio del contrato laboral**
A.8.3.1	Responsabilidades en la terminación

ISO 27001:2005	
ID. CONTROL	**NOMBRE CONTROL**
A.8.3.2	Devolución de activos
A.8.3.3	Retiro de los derechos de acceso
A.9	**SEGURIDAD FÍSICA Y DEL ENTORNO**
A.9.1	**Áreas Seguras**
A.9.1.1	Perímetro de seguridad física
A.9.1.2	Controles de acceso físico
A.9.1.3	Seguridad de las oficinas, recintos e instalaciones
A.9.1.4	Protección contra amenazas externas y ambientales
A.9.1.5	Trabajo en áreas seguras
A.9.1.6	Áreas de carga, despacho y acceso público
A.9.2	**Seguridad de los equipos**
A.9.2.1	Ubicación y protección de los equipos
A.9.2.2	Servicios de suministro
A.9.2.3	Seguridad del cableado
A.9.2.4	Mantenimiento de los equipos
A.9.2.5	Seguridad de los equipos fuera de las instalaciones
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos
A.9.2.7	Retiro de equipos
A.10	**GESTIÓN DE COMUNICACIÓN Y OPERACIONES**
A.10.1	Procedimientos operacionales y responsabilidades
A.10.1.1	Documentación de los procedimientos de operación
A.10.1.2	Gestión del Cambio
A.10.1.3	Distribución de funciones
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación
A.10.2	Gestión de la prestación del servicio por terceras partes
A.10.2.1	Prestación del servicio
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes
A.10.2.3	Gestión de los cambios en los servicios por terceras partes
A.10.3	**Planificación y aceptación del sistema**
A.10.3.1	**Gestión de la capacidad**
A.10.3.2	Aceptación del sistema
A.10.4	Protección contra códigos maliciosos y móviles
A.10.4.1	Controles contra códigos maliciosos
A.10.4.2	Controles contra códigos móviles
A.10.5	Respaldo
A.10.5.1	Respaldo de la Información
A.10.6	**Gestión de la seguridad de las redes**
A.10.6.1	Controles de las redes
A.10.6.2	Seguridad de los servicios de la red
A.10.7	**Manejo de los medios**
A.10.7.1	Gestión de los medios removibles.

ISO 27001:2005	
ID. CONTROL	**NOMBRE CONTROL**
A.10.7.2	La eliminación de los medios
A.10.7.3	procedimientos para el manejo de la información
A.10.7.4	Seguridad de la documentación del sistema
A.10.8	**Intercambio de información**
A.10.8.1	Políticas y procedimientos para el intercambio de información
A.10.8.2	Acuerdos para el intercambio
A.10.8.3	Medios físicos en tránsito
A.10.8.4	Mensajería electrónica
A.10.8.5	Sistemas de información del negocio
A.10.9	**Servicios de comercio electrónico**
A.10.9.1	Comercio electrónico
A.10.9.2	Transacciones en línea
A.10.9.3	Información disponible al público
A.10.10	**Monitoreo**
A.10.10.1	Registro de auditorias
A.10.10.2	Monitoreo del uso del sistema
A.10.10.3	Protección de la información de registro
A.10.10.4	Registros del administrador y del operador
A.10.10.5	Registro de fallas
A.10.10.6	Sincronización de relojes
A.11	**CONTROL DE ACCESO**
A.11.1	**Requisito del negocio para el control de acceso**
A.11.1.1	Política de control de acceso
A.11.2	**Gestión de acceso de los usuarios**
A.11.2.1	Registro de usuarios
A.11.2.2	Gestión de Privilegios
A.11.2.3	Gestión de contraseñas para usuarios
A.11.2.4	Revisión de los derechos de acceso de los usuarios
A.11.3	**Responsabilidades de los usuarios**
A.11.3.1	Uso de contraseñas
A.11.3.2	Equipo de usuario desatendido
A.11.3.3	Política de escritorio despejado y pantalla despejada
A.11.4	**Control de acceso a las redes**
A.11.4.1	Política de uso de los servicios de red
A.11.4.2	Autenticación de usuarios para conexiones externas
A.11.4.3	Identificación de los equipos en las redes
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto
A.11.4.5	Separación de redes
A.11.4.6	Control de la conexión a las redes
A.11.4.7	Control de enrutamiento en la red
A.11.5	**Control de acceso al sistema operativo**

ISO 27001:2005	
ID. CONTROL	**NOMBRE CONTROL**
A.11.5.1	Procedimientos de ingreso seguros
A.11.5.2	Identificación y autenticación de usuarios
A.11.5.3	Sistema de gestión de contraseñas
A.11.5.4	Uso de las utilidades del sistema
A.11.5.5	Tiempo de inactividad de la sesión
A.11.5.6	Limitación del tiempo de conexión
A.11.6	**Control de acceso a las aplicaciones y a la información**
A.11.6.1	Restricción de acceso a la información
A.11.6.2	Aislamiento de sistemas sensibles
A.11.7	Computación móvil y trabajo remoto
A.11.7.1	Computación y comunicaciones móviles
A.11.7.2	Trabajo remoto
A.12	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**
A.12.1	**Requisitos de seguridad de los sistemas de información**
A.12.1.1	Análisis y especificación de los requisitos de seguridad
A.12.2	**Procesamiento correcto en las aplicaciones**
A.12.2.1	Validación de los datos de entrada
12.2.2	Control de procesamiento interno
12.2.3	Integridad del mensaje
12.2.4	Validación de los datos de salida
A.12.3	**Controles criptográficos**
A.12.3.1	Política sobre el uso de controles criptográficos
12.3.2	Gestión de claves
A.12.4	**Seguridad de los archivos del sistema**
A.12.4.1	Control del Software Operativo
A.12.4.2	Protección de los datos de prueba del sistema
A.12.4.3	Control de acceso al código fuente de los programas
A.12.5	**Seguridad en los procesos de desarrollo y soporte**
A.12.5.1	Procedimientos de control de cambios
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo
A.12.5.3	Restricciones en los cambios a los paquetes de software
A.12.5.4	Fuga de información
A.12.5.5	Desarrollo de software contratado externamente
A.12.6	Gestión de la Vulnerabilidad Técnica
A.12.6.1	Control de vulnerabilidades técnicas
A.13.1	Reporte sobre los eventos y las debilidades de la seguridad de la información
A.13.1.1	Reporte sobre los eventos de seguridad de la información
A.13.1.2	Reporte sobre las debilidades de la seguridad
A.13.2	**Gestión de incidentes y las mejoras en la seguridad de la información**
A.13.2.1	Responsabilidades y procedimientos

ISO 27001:2005	
ID. CONTROL	**NOMBRE CONTROL**
A.13	**GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN**
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información
A.13.2.3	Recolección de evidencia
A.14	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
A.14.1	**Aspectos de seguridad de la información, de la gestión de la continuidad del negocio**
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
A.14.1.2	Continuidad del negocio y evaluación de riesgos
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información
A.14.1.4	Estructura para la planificación de la continuidad del negocio
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
A.15	**CUMPLIMIENTO**
A.15.1	**Cumplimiento de los requisitos legales**
A.15.1.1	Identificación de la legislación aplicable
A.15.1.2	Derechos de propiedad intelectual (DPI)
A.15.1.3	Protección de los registros de la organización
A.15.1.4	Protección de los datos y privacidad de la información personal
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información
A.15.1.6	Reglamentación de los controles criptográficos
A.15.2	**Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico**
A.15.2.1	Cumplimiento con las políticas y normas de seguridad
A.15.2.2	Verificación del cumplimiento técnico
A.15.3	Consideraciones de auditoría de los sistemas de información
A.15.3.1	Controles de auditoría de los sistemas de información
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información

Fuente: Propiedad del autor.

4. COMPARATIVO DE LA NORMA ISO 27001:2005 CON ISO 27001:2013.

Con la actualización de la norma ISO 27001:2005 a la ISO 27001:2013, se realizaron cambios a los controles y dominios de seguridad de la información en el Anexo A, donde podemos identificar que, aunque aumentaron el número de dominios de seguridad de 11 a 14, esto se debió a más a la reestructuración del estándar que a un cambio de fondo de la norma, ya que podemos observar que el dominio A.10 Administración de Comunicaciones y Operaciones de la versión 2005, ahora se separó en dos dominios, así como también se creó un dominio específico para Criptografía y otro para la Relación con proveedores. Cuadro 2.

Cuadro 2. Comparativo Anexo norma ISO 27001:2005-2013.

Anexo A ISO 27001:2005	Anexo A ISO 27001:2013
A.5 Política de Seguridad	A.5 Políticas de Seguridad
A.6 Organización de seguridad de la información	A.6 Organización de la seguridad de la información
A.8 Seguridad en recursos humanos	A.7 Seguridad de los recursos humanos
A.7 Administración de activos	A.8 Gestión de activos
A.11 Control de acceso	A.9 Control de acceso
	A.10 Criptografía
A.9 Seguridad física y ambiental	A.11 Seguridad física y del entorno
A.10 Administración de comunicaciones y operaciones	A.12 Seguridad de las operaciones
	A.13 Seguridad de las comunicaciones
A.12 Adquisición, desarrollo y mantenimiento de sistemas	A.14 Adquisición, desarrollo y mantenimiento de sistemas
	A.15 Relación con los proveedores
A.13 Administración de incidentes de seguridad de la información	A.16 Gestión de incidentes de seguridad de la información
A.14 Administración de continuidad del negocio.	A.17Aspectos de seguridad de la información de la Gestión de continuidad del negocio.
A.15 Cumplimiento	A.18 Cumplimiento

Fuente: Propiedad del autor

Igualmente se establecieron cambios en las cláusulas de la norma ISO 27001:2013, observando que pasaron de 9 a 11, evidenciando que, aunque algunas cambiaron de nombre, estas poseen gran contenido de la anterior norma, creándose adicionalmente nuevas clausulas como se aprecia a continuación. Ver Cuadro 3.

Cuadro 3. Comparativo de las cláusulas de seguridad de la información de la ISO 27001:2005-2013.

Cláusulas ISO 27001:2005	Cláusulas ISO 27001:2013
0. Introducción	0.Introducción
1. Objeto	1.Objeto
2. Referencias normativas	2.Referencias normativas
3. Términos y definiciones	3.Contexto de la organización
4. Sistema de Gestión de Seguridad de la Información	4.Liderazgo
5. Responsabilidad de la dirección	5.Politica
6. Auditoria interna	6.Planificación
7. Revisión por la dirección	7.Soporte
8. Mejora	8.Operación
	9.Evaluación de desempeño
	10.Mejora

Fuente: Propiedad del autor.

Derivado de dicha reestructura el número de controles disminuyó pasando de 133 a 114, lo cual se puede apreciar en el listado comparativo de los nuevos dominios de seguridad de la información, que se presenta a continuación: Cuadro 4.

Cuadro 4. Comparativos controles establecidos en la norma ISO 27001:2005 e ISO 27001:2013.

ISO 27001:20105		ISO 27001:2013	
ID. CONTROL	**CONTROL**	**ID. CONTROL**	**CONTROL**
A.5	**POLÍTICA DE SEGURIDAD**	**A.5**	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**
A.5.1	Política de seguridad de la información	A.5.1	Orientación de la dirección para la gestión de la seguridad de la información
A.5.1.1	Documento de Política de seguridad de la información	A.5.1.1	Políticas para la seguridad de la información
A.5.1.2	Revisión de la política de seguridad de la información	A.5.1.2	Revisión de las políticas para la seguridad de la información
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**A.6**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
A.6.1	Organización Interna	A.6.1	Organización Interna
A.6.1.1	Compromiso de la dirección con la seguridad de la información	A.6.1.1	Roles y responsabilidades para la seguridad de la información
A.6.1.2	Coordinación de la seguridad de la información	A.6.1.2	Separación de deberes
A.6.1.3	Asignación de responsabilidades para la seguridad de la información	A.6.1.3	Contacto con las autoridades
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información	A.6.1.4	Contacto con grupos de interés especial

ISO 27001:20105		ISO 27001:2013	
CONTROL	**ID. CONTROL**	**CONTROL**	**ID. CONTROL**
A.6.1.5	Acuerdos sobre confidencialidad	A.6.1.5	Seguridad de la información en la gestión de proyectos
A.6.1.6	Contacto con las autoridades	A.6.2	Dispositivos móviles y teletrabajo
A.6.1.7	Contacto con grupos de interés especiales	A.6.2.1	Política para dispositivos móviles
A.6.1.8	Revisión independiente de la seguridad de la información	A.6.2.2	Teletrabajo
A.6.2	Partes Externas	**A.15**	**RELACIÓN CON LOS PROVEEDORES**
A.6.2.1	Identificación de los riesgos relacionados con las partes externas	A.15.1	Seguridad de la información en las relaciones con los proveedores
A.6.2.2	Consideraciones de la seguridad cuando se trata de clientes	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores
		A.15.1.3	Cadena de suministro de tecnología de información y comunicación
		A.15.2	Gestión de la prestación de servicios de proveedores
		A.15.2.1	Seguimiento y revisión de los servicios de los proveedores
		A.15.2.2	Gestión de cambios en los servicios de los proveedores
A.7	**GESTIÓN DE ACTIVOS**	**A.8**	**GESTIÓN DE ACTIVOS**
A.7.1	Responsabilidad por los activos	A.8.1	Responsabilidad por los activos
A.7.1.1	Inventarios de Activos	A.8.1.1	Inventarios de Activos
A.7.1.2	Propiedad de los Activos	A.8.1.2	Propiedad de Activos
A.7.1.3	Uso aceptable de los activos	A.8.1.3	Uso aceptable de los activos
A.7.2	Clasificación de la información	A.8.1.4	Devolución de los activos
A.7.2.1	Directrices de clasificación	A.8.2	Clasificación de la información
A.7.2.2	Etiquetado y manejo de la información	A.8.2.1	Clasificación de la información
		A.8.2.2	Etiquetado de la información
		A.8.2.3	Manejo de activos
		A.8.3	Manejo de medios
		A.8.3.1	Gestión de medios removibles
		A.8.3.2	Disposición de medios
		A.8.3.3	Transferencia de medios físicos
A.8	**SEGURIDAD DE LOS RECURSOS HUMANOS**	**A.7**	**SEGURIDAD DE LOS RECURSOS HUMANOS**
A.8.1	Antes de la contratación laboral	A.7.1	Antes de asumir el empleo
A.8.1.1	Roles y Responsabilidades	A.7.1.1	Selección
A.8.1.2	Selección	A.7.1.2	Términos y condiciones del empleo
A.8.1.3	Términos y condiciones laborales	A.7.2	Durante la ejecución del empleo
A.8.2	Durante la vigencia de la contratación laboral	A.7.2.1	Responsabilidades de la dirección
A.8.2.1	Responsabilidades de la dirección	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información
A.8.2.2	Educación, formación y concienciación sobre la seguridad de la información	A.7.2.3	Proceso disciplinario
A.8.2.3	Proceso Disciplinario	A.7.3	Terminación y cambio de empleo
A.8.3	Terminación o cambio del contrato laboral	A.7.3.1	Terminación o cambio de empleo de responsabilidades de empleo
A.8.3.1	Responsabilidades en la terminación		
A.8.3.2	Devolución de activos		
A.8.3.3	Retiro de los derechos de acceso		

ISO 27001:20105		ISO 27001:2013	
CONTROL	**ID. CONTROL**	**CONTROL**	**ID. CONTROL**
A.9	**SEGURIDAD FÍSICA Y DEL ENTORNO**	**A.11**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
A.9.1	Áreas Seguras	A.11.1	Áreas seguras
A.9.1.1	Perímetro de seguridad física	A.11.1.1	Perímetro de seguridad física
A.9.1.2	Controles de acceso físico	A.11.1.2	Controles de acceso físicos
A.9.1.3	Seguridad de las oficinas, recintos e instalaciones	A.11.1.3	Seguridad de oficinas, recintos e instalaciones
A.9.1.4	Protección contra amenazas externas y ambientales	A.11.1.4	Protección contra amenazas externas y ambientales
A.9.1.5	Trabajo en áreas seguras	A.11.1.5	Trabajo en áreas seguras
A.9.1.6	Áreas de carga, despacho y acceso público	A.11.1.6	Áreas de despacho y carga
A.9.2	Seguridad de los equipos	A.11.2	Equipos
A.9.2.1	Ubicación y protección de los equipos	A.11.2.1	Ubicación y protección de los equipos
A.9.2.2	Servicios de suministro	A.11.2.2	Servicios de suministro
A.9.2.3	Seguridad del cableado	A.11.2.3	Seguridad del cableado
A.9.2.4	Mantenimiento de los equipos	A.11.2.4	Mantenimiento de equipos
A.9.2.5	Seguridad de los equipos fuera de las instalaciones	A.11.2.5	Retiro de activos
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones
A.9.2.7	Retiro de equipos	A.11.2.7	Disposición segura o reutilización de equipos
		A.11.2.8	Equipos de usuario desatendido
		A.11.2.9	Política de escritorio limpio y pantalla limpia
A.10	**GESTIÓN DE COMUNICACIÓN Y OPERACIONES**	**A.12**	**SEGURIDAD DE LAS OPERACIONES**
A.10.1	Procedimientos operacionales y responsabilidades	A.12.1	Procedimientos operacionales y responsabilidades
A.10.1.1	Documentación de los procedimientos de operación	A.12.1.1	Procedimientos de operación documentados
A.10.1.2	Gestión del Cambio	A.12.1.2	Gestión de cambios
A.10.1.3	Distribución de funciones	A.12.1.3	Gestión de capacidad
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
A.10.2	Gestión de la prestación del servicio por terceras partes	A.12.2	Protección contra códigos maliciosos
A.10.2.1	Prestación del servicio	A.12.2.1	Controles contra códigos maliciosos
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	A.12.3	Copias de respaldo
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	A.12.3.1	Respaldo de la información
A.10.3	Planificación y aceptación del sistema	A.12.4	Registro y seguimiento
A.10.3.1	Gestión de la capacidad	A.12.4.1	Registro de eventos
A.10.3.2	Aceptación del sistema	A.12.4.2	Protección de la información de registro
A.10.4	Protección contra códigos maliciosos y móviles	A.12.4.3	Registros del administrador y del operador
A.10.4.1	Controles contra códigos maliciosos	A.12.4.4	Sincronización de reglas
A.10.4.2	Controles contra códigos móviles	A.12.5	Control de software operacional
A.10.5	Respaldo	A.12.5.1	Instalación de software en sistemas operativos
A.10.5.1	Respaldo de la Información	A.12.6	Gestión de la vulnerabilidad técnica
A.10.6	Gestión de la seguridad de las redes	A.12.6.1	Gestión de las vulnerabilidades técnicas
A.10.6.1	Controles de las redes	A.12.6.2	Restricciones sobre la instalación del software
A.10.6.2	Seguridad de los servicios de la red	A.12.7	Consideraciones sobre auditorias de sistemas de información

ISO 27001:20105		ISO 27001:2013	
CONTROL	**ID. CONTROL**	**CONTROL**	**ID. CONTROL**
A.10.7	Manejo de los medios	A.12.7.1	Controles de auditorías de sistemas de información
A.10.7.1	Gestión de los medios removibles		
A.10.7.2	La eliminación de los medios	**A.13**	**SEGURIDAD DE LAS COMUNICACIONES**
A.10.7.3	Procedimientos para el manejo de la información	A.13.1	Gestión de la seguridad en las redes
A.10.7.4	Seguridad de la documentación del sistema	A.13.1.1	Controles de las redes
A.10.8	Intercambio de información	A.13.1.2	Seguridad en los servicios de red
A.10.8.1	Políticas y procedimientos para el intercambio de información	A.13.1.3	Separación en las redes
A.10.8.2	Acuerdos para el intercambio	A.13.2	Transferencia de información
A.10.8.3	Medios físicos en tránsito	A.13.2.1	Políticas y procedimientos de transferencia de información
A.10.8.4	Mensajería electrónica	A.13.2.2	Acuerdos sobre transferencia de información
A.10.8.5	Sistemas de información del negocio	A.13.2.3	Mensajería electrónica
A.10.9	Servicios de comercio electrónico	A.13.2.4	Acuerdos de confidencialidad o de no divulgación
A.10.9.1	Comercio electrónico		
A.10.9.2	Transacciones en línea		
A.10.9.3	Información disponible al público		
A.10.10	Monitoreo		
A.10.10.1	Registro de auditorias		
A.10.10.2	Monitoreo del uso del sistema		
A.10.10.3	Protección de la información de registro		
A.10.10.4	Registros del administrador y del operador		
A.10.10.5	Registro de fallas		
A.10.10.6	Sincronización de relojes		
A.11	**CONTROL DE ACCESO**	**A.9**	**CONTROL DE ACCESO**
A.11.1	Requisito del negocio para el control de acceso	A.9.1	Requisitos del negocio para control de acceso
A.11.1.1	Política de control de acceso	A.9.1.1	Política de control de acceso
A.11.2	Gestión de acceso de los usuarios	A.9.1.2	Acceso a redes y a servicios en red
A.11.2.1	Registro de usuarios	A.9.2	Gestión de acceso a usuarios
A.11.2.2	Gestión de Privilegios	A.9.2.1	Registro y cancelación del registro de usuarios
A.11.2.3	Gestión de contraseñas para usuarios	A.9.2.2	Suministro de acceso a usuarios
A.11.2.4	Revisión de los derechos de acceso de los usuarios	A.9.2.3	Gestión de derechos de acceso privilegiado
A.11.3	Responsabilidades de los usuarios	A.9.2.4	Gestión de información de autenticación secreta de usuarios
A.11.3.1	Uso de contraseñas	A.9.2.5	Revisión de los derechos de acceso de los usuarios
A.11.3.2	Equipo de usuario desatendido	A.9.2.6	Retiro o ajuste de los derechos de acceso
A.11.3.3	Política de escritorio despejado y pantalla despejada	A.9.3	Responsabilidad de los usuarios
A.11.4	Control de acceso a las redes	A.9.3.1	Uso de información de autenticación secreta
A.11.4.1	Política de uso de los servicios de red	A.9.4	Control de acceso a sistemas y aplicaciones
A.11.4.2	Autenticación de usuarios para conexiones externas	A.9.4.1	Restricción de acceso a la información
A.11.4.3	Identificación de los equipos en las redes	A.9.4.2	Procedimiento de ingreso seguro
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	A.9.4.3	Sistema de Gestión de contraseñas
A.11.4.5	Separación de redes	A.9.4.4	Uso de programas utilitarios privilegiados

ISO 27001:20105		ISO 27001:2013	
CONTROL	**ID. CONTROL**	**CONTROL**	**ID. CONTROL**
A.11.4.6	Control de la conexión a las redes	A.9.4.5	Control de acceso a códigos fuente de programas
A.11.4.7	Control de enrutamiento en la red		
A.11.5	Control de acceso al sistema operativo		
A.11.5.1	Procedimientos de ingreso seguros		
A.11.5.2	Identificación y autenticación de usuarios		
A.11.5.3	Sistema de gestión de contraseñas		
A.11.5.4	Uso de las utilidades del sistema		
A.11.5.5	Tiempo de inactividad de la sesión		
A.11.5.6	Limitación del tiempo de conexión		
A.11.6	Control de acceso a las aplicaciones y a la información.		
A.11.6.1	Restricción de acceso a la información		
A.11.6.2	Aislamiento de sistemas sensibles		
A.11.7	Computación móvil y trabajo remoto		
A.11.7.1	Computación y comunicaciones móviles		
A.11.7.2	Trabajo remoto		
A.12	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	**A.14**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
A.12.1	Requisitos de seguridad de los sistemas de información	A.14.1	Requisitos de seguridad de los sistemas de información
A.12.1.1	Análisis y especificación de los requisitos de seguridad	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información
A.12.2	Procesamiento correcto en las aplicaciones	A.14.1.2	Seguridad de servicios de las aplicaciones en las redes publicas
A.12.2.1	Validación de los datos de entrada	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones
12.2.2	Control de procesamiento interno	A.14.2	Seguridad en los procesos de desarrollo y de soporte
12.2.3	Integridad del mensaje	A.14.2.1	Política de desarrollo seguro
12.2.4	Validación de los datos de salida	A.14.2.2	Procedimientos de control de cambios en sistemas
A.12.3	**Controles criptográficos**	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
A.12.3.1	Política sobre el uso de controles criptográficos	A.14.2.4	Restricciones en los cambios a los paquetes de software
12.3.2	Gestión de claves	A.14.2.5	Principios de construcción de los sistemas seguros
A.12.4	Seguridad de los archivos del sistema	A.14.2.6	Ambiente de desarrollo seguro
A.12.4.1	Control del Software Operativo	A.14.2.7	Desarrollo contratado externamente
A.12.4.2	Protección de los datos de prueba del sistema	A.14.2.8	Pruebas de seguridad de sistemas
A.12.4.3	Control de acceso al código fuente de los programas	A.14.2.9	Prueba de aceptación de sistemas
A.12.5	Seguridad en los procesos de desarrollo y soporte	A.14.3	Datos de prueba
A.12.5.1	Procedimientos de control de cambios	A.14.3.1	Protección de datos de prueba
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo		
A.12.5.3	Restricciones en los cambios a los paquetes de software	**A.10**	**CRIPTOGRAFÍA**
A.12.5.4	Fuga de información	A.10.1	Controles criptográficos
A.12.5.5	Desarrollo de software contratado externamente	A.10.1.1	Política sobre uso de controles criptográficos
A.12.6	Gestión de la Vulnerabilidad Técnica	A.10.1.2	Gestión de llaves
A.12.6.1	Control de vulnerabilidades técnicas		
A.13	**GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN**	**A.16**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN**

ISO 27001:20105		ISO 27001:2013	
CONTROL	**ID. CONTROL**	**CONTROL**	**ID. CONTROL**
A.13.1	Reporte sobre los eventos y las debilidades de la seguridad de la información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información
A.13.1.1	Reporte sobre los eventos de seguridad de la información	A.16.1.1	Responsabilidades y procedimientos
A.13.1.2	Reporte sobre las debilidades de la seguridad	A.16.1.2	Reporte de eventos de seguridad de la información
A.13.2	Gestión de incidentes y las mejoras en la seguridad de la información	A.16.1.3	Reporte de debilidades de seguridad de la información
A.13.2.1	Responsabilidades y procedimientos	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	A.16.1.5	Respuesta de incidentes de seguridad de la información
A.13.2.3	Recolección de evidencia	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información
		A.16.1.7	Recolección de evidencia
A.14	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**A.17**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
A.14.1	Aspectos de seguridad de la información, de la gestión de la continuidad del negocio	A.17.1	Continuidad de la seguridad de la información
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	A.17.1.1	Planificación de la continuidad de la seguridad de la información
A.14.1.2	Continuidad del negocio y evaluación de riesgos	A.17.1.2	Implementación de la continuidad de la seguridad de la información
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.14.1.4	Estructura para la planificación de la continuidad del negocio	A.17.2	Redundancias
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información
A.15	**CUMPLIMIENTO**	**A.18**	**CUMPLIMIENTO**
A.15.1	Cumplimiento de los requisitos legales	A.18.1	Cumplimiento de requisitos legales y contractuales
A.15.1.1	Identificación de la legislación aplicable	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
A.15.1.2	Derechos de propiedad intelectual (DPI)	A.18.1.2	Derechos de propiedad intelectual
A.15.1.3	Protección de los registros de la organización	A.18.1.3	Protección de registros
A.15.1.4	Protección de los datos y privacidad de la información personal	A.18.1.4	Privacidad y protección de información de datos personales
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	A.18.1.5	Reglamentación de controles criptográficos
A.15.1.6	Reglamentación de los controles criptográficos	A.18.2	Revisiones de seguridad de la información
A.15.2	Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico	A.18.2.1	Revisión independiente de la seguridad de la información
A.15.2.1	Cumplimiento con las políticas y normas de seguridad	A.18.2.2	Cumplimiento con las políticas y normas de seguridad
A.15.2.2	Verificación del cumplimiento técnico	A.18.2.3	Revisión del cumplimiento técnico
A.15.3	Consideraciones de auditoría de los sistemas de información		
A.15.3.1	Controles de auditoría de los sistemas de información		
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información		

Fuente: Propiedad del autor.

5. IDENTIFICACIÓN DE LOS CONTROLES QUE SERÁN PROPUESTOS PARA SU APLICACIÓN EN LA SEDE MEDELLÍN DE LA EMPRESA CASO DE ESTUDIO, ESTABLECIDOS EN EL ANEXO A DE LA NORMA ISO 27001:2013.

Una vez comparados los controles adoptados por la empresa caso de estudio basados en la norma ISO 27001:2005, y los establecidos por la norma ISO 27001:2013 se procede a realizar la propuesta de los controles y políticas de la seguridad de la información que deben ser implementados en la sede Medellín, para garantizar la seguridad de la información que allí se maneja, los cuales se relacionan a continuación, así: Cuadro 5.

Cuadro 5. Propuesta de controles de la seguridad de la información bajo la norma ISO 27001:2013.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE SI	APLICABLE NO	PROPUESTA
A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información.**				
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	X		Redactar y documentar las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables, como una estrategia de seguridad basada en las mejores prácticas y controles, con el fin de resguardar los activos de información de las amenazas que se ciernen sobre ellos. Documento se debe poner a disposición de los empleados y público en general.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	X		Las políticas de seguridad de la información se revisarán y evaluarán periódicamente y/o cuando sea necesario. La revisión es llevada a cabo por la Oficina de Tecnologías de la información (TI) de la empresa, líder del Proceso Tecnológico, se documentan los cambios y las justificaciones de los mismos.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**				
A.6.1	**Organización Interna**				
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	X		Los roles y responsabilidades de quienes deben apoyar y cumplir la política de seguridad de la información están definidos en cada una de las áreas de la empresa. (Comités, Grupos, Direcciones, oficinas asesoras).

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	X		El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín mantiene los contactos actualizados para incidentes de seguridad.
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín mantienen contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín es el encargado de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos de TI.
A.6.2	**Dispositivos móviles y teletrabajo**				
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	X		Se documenta una política de seguridad apropiada para los dispositivos móviles. Los dispositivos móviles son configurados bajo las condiciones de seguridad aplicables antes de realizar cualquier conexión a la red institucional, La seguridad para estos equipos es equivalente a la suministrada dentro de las instalaciones y controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso de estos.
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		X	La creación de políticas de uso y protección para las conexiones remotas, son usadas con el fin de evitar filtraciones y daño en la integridad de la información durante la conexión. Sin embargo, en el caso concreto de la sede Medellín, no están autorizadas las conexiones remotas para el trabajo de los empleados desde el exterior de las instalaciones.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				
A.7.1	**Antes de asumir el empleo**				

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	X		El personal es seleccionado cuidadosamente por la Dirección de incorporación en base a su perfil y la idoneidad del trabajo a realizar, acorde con lo establecido en el proceso seleccionar el Talento Humano para la Empresa caso de estudio.
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	X		Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información, las cuales quedan plasmadas en un acta de aceptación que hace parte integral del contrato.
A.7.2	**Durante la ejecución del empleo**				
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	X		La Dirección General de la Empresa caso de estudio comprende la importancia de la seguridad de la información y apoya la mejora continua del SGSI.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	X		La oficina de Tecnologías de la información (TI) (CSIRT) y el Promotor de la seguridad de la información de la sede Medellín realizan permanentemente campañas y talleres de formación y educación en la seguridad de la información de forma periódica al personal de la empresa.
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	X		Los empleados son sometidos a medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso, en caso de incumplimiento con las políticas de seguridad de la información de forma deliberada.
A.7.3	**Terminación y cambio de empleo**				
A.7.3.1	Terminación o cambio de empleo de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín vela que el empleado que termine contrato o cambie de responsabilidades, se le sean reasignados los permisos y condiciones de seguridad de la información.
A.8	**GESTIÓN DE ACTIVOS**				
A.8.1	**Responsabilidad por los activos**				

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.8.1.1	Inventarios de Activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín junto a los empleados, realizan el inventario de activos y se documentan con su clasificación y responsable.
A.8.1.2	Propiedad de Activos	Los activos mantenidos en el inventario deben tener un propietario	X		Los activos inventariados tienen asignados los empleados responsables.
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	X		Los empleados se comprometen a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de información generales.
A.8.1.4	Devolución de los activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	X		Se mantienen registros de la devolución de los activos entregados a los empleados, los cuales son necesarios para firmar paz y salvo con la empresa.
A.8.2	**Clasificación de la información**				
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X		Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo con los niveles de seguridad establecidos
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		Cada uno de los activos inventariados están etiquetados con la clasificación de la información asociada, de acuerdo con las Cuadros de retención documental que aplique para cada unidad de Policía.
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín junto a los empleados realizan y documentan los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
A.8.3	**Manejo de medios**				
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	X		Existe una política para la gestión de los medios removibles tales como memorias USB, discos duros externos, entre otros utilizados en la unidad, se clasifican y protegen de acuerdo con su tipo.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.8.3.2	Disposición de medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	X		Los medios removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros. Se cuenta con un procedimiento que tiene como objetivo Realizar el borrado seguro y la baja de bienes inservibles, en desuso u obsoletos de la Empresa caso de estudio, con el fin reasignar o destruir los equipos que cumplieron su ciclo de vida.
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	X		El transporte de información en medios físicos (digital o impresa) contempla mecanismos que no permiten su uso no autorizado mediante el uso de herramientas criptografías que evitan un acceso no autorizado o fuga de la información contenida en ellos en caso de pérdida, preservando así la confidencialidad, integridad y disponibilidad de la misma.
A.9	**CONTROL DE ACCESO**				
A.9.1	**Requisitos del negocio para control de acceso**				
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	X		La política de control de acceso está documentada en las Políticas de la Seguridad de Información, mediante el modelo de Administración de identidades y Control de acceso (IAM), implantado mediante el Sistema de Identificación Digital.
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	X		Las redes están segmentadas y el acceso a ellas está protegido a personas no autorizadas, el acceso a redes desde y hacia afuera de la Empresa caso de estudio cumple con los lineamientos del Control de acceso a la red y adicionalmente se utilizan métodos de autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.
A.9.2	**Gestión de acceso a usuarios**				
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	X		La oficina de Tecnologías de la información (TI) a través del Sistema de Identificación Digital, integrado al Sistema Para la Administración del Talento Humano administrar el ciclo de vida de los usuarios, desde la creación automática de las cuentas, roles y permisos necesarios hasta su inoperancia.
A.9.2.2	Suministro de acceso a usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	X		La oficina de Tecnologías de la información (TI) a través de usuarios administradores contempla el registro de usuarios, gestión de privilegios y gestión de contraseñas.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	X		A los empleados se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo. Estos privilegios son documentados y los empleados son agrupados bajo Perfiles de Usuario.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	X		La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso, en todos y cada uno de los sistemas de información de la empresa.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín junto a los empleados encargados verifican que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación se realiza de forma periódica y cualquier novedad es debidamente documentada e informada al administrador del sistema de información.
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín verifican y eliminan los permisos asignados al personal que sea retirado o reasignado al cumplimiento de otras funciones.
A.9.3	**Responsabilidad de los usuarios**				
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	X		La información de autenticación del empleado en los sistemas y acceso a información es confidencial. Se realiza la entrega de los formatos establecidos para tal fin, cada vez que se hace la entrega de un usuario a un empleado de su dependencia
A.9.4	**Control de acceso a sistemas y aplicaciones**				
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	X		Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del empleado en la empresa.
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	X		El acceso a los sistemas operativos y sistemas de información están protegidos mediante un inicio seguro de sesión. Se emplean mecanismos seguros de cifrado de información
A.9.4.3	Sistema de Gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	X		Se implementan mecanismos de recuperación de contraseñas de forma automática y se garantiza que la nueva contraseña del empleado cumpla con los requisitos de seguridad expuestos en la Política de Seguridad de contraseñas. Las contraseñas se administran de forma automática mediante el OID y estas están configuradas para que cumplan con lo que se enuncia en la guía establecida para tal fin.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	X		El uso de utilitarios licenciados del sistema está restringido a usuarios administradores. Se estableció una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema. La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín verifican que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados.
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.		X	La oficina de Tecnologías de la información (TI) a través del grupo de desarrollo, verifica que los códigos fuentes de los programas se almacenan de forma confidencial garantizando su integridad, actividad que no hace parte de la misionalidad de la sede Medellín de la empresa caso de estudio.
A.10	**CRIPTOGRAFÍA**				
A.10.1	**Controles criptográficos**				
A.10.1.1	Política sobre uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	X		Existe una política de seguridad que documenta el uso de los controles criptográficos, la escogencia y justificación de los algoritmos de cifrado y su aplicación en los servicios que la requieran.
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	X		Existe una política de seguridad que documenta el proceso y ciclo de vida de las llaves criptográficas, la utilización de firmas y certificados digitales para el intercambio de información con entidades ajenas a la Empresa caso de estudio.
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**				
A.11.1	**Áreas seguras**				
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	X		La Empresa caso de estudio realiza el mayor esfuerzo en implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro, en todas sus instalaciones, para el control de las amenazas físicas externas e internas y las condiciones medioambientales. El perímetro físico de la sede Medellín de la empresa caso de estudio, es controlado con lectores biométricos, tarjetas de acceso, monitoreado a través de un CCTV, contando adicionalmente con personal de seguridad en la infraestructura que contiene el hardware de las operaciones críticas.
A.11.1.2	Controles de acceso físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	X		El acceso físico a la infraestructura que contiene el hardware de las operaciones críticas está controlado por medio de lectores biométricos y tarjetas de proximidad que permiten el acceso a sólo el personal autorizado y registran la fecha y hora de acceso.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	X		Para la seguridad de oficinas e instalaciones, se cuenta con personal de seguridad y cámaras de seguridad que monitorean permanentemente el ingreso y salida de personal a las mismas.
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X		La Empresa caso de estudio, cuenta con un Plan de Continuidad del Negocio que le permite recuperarse de incidentes que amenacen la prestación del servicio de policía; para lo cual el comité del Sistema de Seguridad de la Información elaboró el plan de continuidad del negocio y la Oficina de Tecnologías de la información (TI), elaboró el plan de recuperación de desastres en materia tecnológica
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	X		Se cuenta con áreas seguras que buscan proteger los activos de información de las amenazas naturales y ambientales; de las amenazas por interrupción de servicios públicos; de las amenazas artificiales como acceso no autorizado (tanto internos como externos), explosiones, daños por empleados, vandalismo, fraude, robo, y finalmente de las amenazas por motivos políticos como huelgas, disturbios, desobediencia civil, ataques terroristas y bombardeos.
A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	X		Existe un área diseñada y estructurada para el cargue y descargue, que impide el acceso al interior de las instalaciones, oficinas e infraestructura que contiene el hardware de las operaciones críticas.
A.11.2	**Equipos**				
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	X		Los equipos de cómputo son ubicados y protegidos para reducir la exposición a riesgos ocasionados por amenazas ambientales y de acceso no autorizado, y existen políticas de seguridad de la información documentadas para su uso.
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	X		Los centros de procesamiento de datos están protegidos con respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía está de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.
A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	X		El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente con canaleta en caso de instalación interior, o con tubo metálico en caso de instalación tipo intemperie.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X		El mantenimiento preventivo de los equipos se realiza de acuerdo con los intervalos de servicio y especificaciones recomendadas por el proveedor. La generación de contratos para la realización de los mantenimientos preventivos de los equipos contribuye con objetivo de evitar daños o suspensión de los servicios de los mismos.
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	X		El jefe logístico en concordancia con el promotor de la seguridad de la información documenta el retiro de los activos.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	X		Está restringido a equipos portátiles y móviles, la seguridad para estos equipos es equivalente a la suministrada dentro de las instalaciones empresa y controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso de estos.
A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	X		Se realiza borrado seguro de la información o destrucción física del dispositivo de almacenamiento, antes de la reutilización o devolución de cualquier equipo de cómputo, dicho procedimiento se encuentra estipulado en el procedimiento “Borrado seguro de información”.
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	X		Existe un plan de capacitación y campaña de concientización a los empleados sobre la seguridad de la información y los riesgos a los que están expuestos los activos. Los usuarios deberán cerrar la sesión cuando hayan terminado, de igual forma los equipos de cómputo cuentan con un mecanismo de bloqueo automático como el de protector de pantalla después de 5 minutos de inactividad.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	X		La oficina de Tecnologías de la información (TI), el Promotor de la seguridad de la información, los empleados de la sede Medellín, garantizan que la información confidencial física es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.
A.12	**SEGURIDAD DE LAS OPERACIONES**				
A.12.1	**Procedimientos operacionales y responsabilidades**				
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados documentan los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín, verifica que los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín, realizan un monitoreo continuo a los recursos y la adquisición de los nuevos y se proyecta de acuerdo con las necesidades críticas de la empresa.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación.	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.		X	Los ambientes de desarrollo, pruebas y producción, en lo posible estarán separados preferiblemente en forma física o virtualizados. La transferencia de software del ambiente de pruebas al ambiente de producción será documentada, para lo cual se aplican los siguientes controles: 1. Ejecutar el software de desarrollo y producción en diferentes ambientes. 2. Las actividades de desarrollo y pruebas deberán realizarse en ambientes separados. 3. Los datos de producción no deberán usarse en ambientes de desarrollo o pruebas. 4. No usar compiladores, editores y otros utilitarios que no sean necesarios para el funcionamiento de los ambientes de producción. Dicho control no aplica a la sede Medellín, ya que en él no se desarrolla software.
A.12.2	**Protección contra códigos maliciosos**				
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X		Existe un plan de capacitación y campaña de concientización a los empleados sobre la seguridad de la información y los riesgos a los que están expuestos los activos, especialmente sobre el software de código malicioso. La oficina de Tecnologías de la información (TI), el Promotor de la seguridad de la información de la sede Medellín y los empleados, verifican que los equipos estén protegidos con antivirus y existe una política documentada de actualización de todo el software utilizado, antivirus y sistema operativo, implementando controles para prevenir y detectar código malicioso, lo cual se basa en software, concienciación de usuarios y gestión del cambio.
A.12.3	**Copias de respaldo**				
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y empleados pertinentes realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A.12.4	**Registro y seguimiento**				

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y empleados pertinentes revisan periódicamente los registros de los usuarios y las actividades relativas a la seguridad de la información. El proceso es auditado y documentado, Los registros de auditoría de los sistemas de información están consolidados en ambientes separados a los transaccionales.
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	X		Se implementan controles de seguridad que garanticen la protección de la información de los registros, salvaguardándolos de acceso o modificaciones, que alteren su integridad. Estos registros poseen copias de respaldo.
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	X		Las acciones y registros de los administradores son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	X		Para garantizar la exactitud de los registros de auditoría, la Empresa caso de estudio, dispone de un servicio de protocolo de tiempo de red NTP que esta sincronizado a su vez con la hora legal colombiana
A.12.5	**Control de software operacional**				
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X		Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y software, que cumple con las políticas de seguridad de la información, solo usuarios administradores pueden realizar la instalación de software.
A.12.6	**Gestión de la vulnerabilidad técnica**				
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X		Existe una metodología de análisis y evaluación de riesgos sistemática y documentada, a cargo del Área de Administración de la Información, el cual realiza el análisis de la explotación de vulnerabilidades conocidas, que podrían poner en riesgo la plataforma tecnológica institucional y su información, por tanto, estas son adecuadamente gestionadas y remediadas.
A.12.6.2	Restricciones sobre la instalación del software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X		La instalación de software es realizada sólo por el personal autorizado y con software probado y licenciado, el procedimiento de instalación es documentado y ningún usuario final, tiene privilegios de usuario administrador.
A.12.7	**Consideraciones sobre auditorias de sistemas de información.**				

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes acuerdan sobre las fechas de auditorías internas para los sistemas de información. El procedimiento es documentado y se coordinan las actividades previas con el fin de no afectar la disponibilidad del servicio.
A.13	**SEGURIDAD DE LAS COMUNICACIONES**				
A.13.1	Gestión de la seguridad en las redes				
A.13.1.1	Controles de las redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X		La oficina de Tecnologías de la información (TI) a través del proceso de Direccionamiento Tecnológico implementan controles de seguridad de la red de datos de la empresa, para lo cual usa como referencia el estándar ISO/IEC 18028 Tecnología de la información-Técnicas de seguridad – la seguridad de TI de la Red, garantizando la confidencialidad e integridad de la información que se transmite a través de las redes.
A.13.1.2	Seguridad en los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	X		El acceso a la red de los proveedores de servicio de red es monitoreado y controlado, están documentados los procedimientos de Chequeo del tráfico de la red, Monitoreo de los puertos en la red, y Auditoría, trazabilidad y respaldo de archivos de log's.
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X		La Empresa caso de estudio utiliza dispositivos de seguridad "firewalls", para controlar el acceso de una red a otra, la segmentación se realiza en equipos de enrutamiento mediante la configuración de control de acceso y configuraciones de VLAN´s, en los equipos de conmutación.
A.13.2	**Transferencia de información**				
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	X		Las políticas y procedimientos para la transferencia de la información están debidamente documentados y se aplican los mecanismos de seguridad necesarios para garantizar la confidencialidad e integridad de la información.
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	X		Existen documentos y acuerdos para la transferencia de información que garanticen su confidencialidad e integridad, la entrega de información se realiza bajo el deber de reserva, así mismo se documentan los controles.
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X		La mensajería electrónica en la Empresa caso de estudio, está asociada a los servicios de correo electrónico de sus dominios y a la plataforma de comunicaciones unificada, está regulada por los términos de uso adecuado.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	X		En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información. La Empresa caso de estudio estableció un compromiso de confidencialidad mediante el formato establecida para tal fin", el cual debe ser suscrito por todos los empleados o personal que tienen un vínculo laboral o contractual con la empresa, el cual es parte de su hoja de vida, junto con el acta de posesión y/o contrato.
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**				
A.14.1	**Requisitos de seguridad de los sistemas de información**				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X		Existe una política documentada que establece los requisitos relativos a la seguridad de la información, para la adquisición de productos se contemplan características de seguridad y realiza un proceso formal de pruebas, que hace parte del proceso de evaluación de las ofertas.
A.14.1.2	Seguridad de servicios de las aplicaciones en las redes publicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X		La oficina de Tecnologías de la información (TI) y el administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	X		La oficina de Tecnologías de la información (TI) y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.2	**Seguridad en los procesos de desarrollo y de soporte**				
A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	X		La oficina de Tecnologías de la información (TI) a través del proceso de Direccionamiento Tecnológico velará porque los sistemas de información adquiridos, desarrollados por terceras partes o al interior de la empresa, cumplan con el ciclo de vida de desarrollo y con los requerimientos de funcionalidad y seguridad esperados y se acojan a las metodologías para la definición de requerimientos de software y para la realización de pruebas al software desarrollado. Así mismo, asegurará que todo sistema de información adquirido, desarrollado por terceros o al interior de la empresa, cuente con el nivel de soporte requerido por la empresa.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	X		Se encuentra documentado un procedimiento de control de cambios, en el cual todo cambio es evaluado previamente tanto en los aspectos técnicos como de seguridad.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	X		Existe una documentación sobre la implementación de las nuevas aplicaciones, se realizan revisiones con el fin de evitar fallas que afecten la disponibilidad de los mismos. La oficina de Tecnologías de la información (TI), el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes realizan las pruebas bajo simulaciones críticas.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	X		Se encuentra documentado un procedimiento de control de cambios, en el cual las modificaciones de paquetes de software suministrados por un proveedor se analizan, se evalúan se guarda una copia del software a modificar, documentando los cambios realizados.
A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	X		Al establecer principios para la construcción de sistemas seguros en el Grupo Regional, y al aplicarlos a cualquier actividad de implementación de sistemas de información, se contribuye efectivamente a mejorar los estándares de seguridad dentro del proceso de construcción.
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		X	Siendo los sistemas de información parte importante del proceso de soporte a los procesos misionales de la Empresa caso de estudio, se busca brindar seguridad a los aplicativos institucionales desde el momento mismo del levantamiento de requerimientos y que las necesidades de seguridad, hagan parte integral de las decisiones arquitecturales del software a construir y/o adquirir. El procedimiento 1DT-PR-0017 Desarrollar Sistemas de Información, realiza levantamiento de anti requerimientos y casos de abuso, los cuales son expuestos por el Grupo de Seguridad de la Información, actividad que no realiza directamente la sede Medellín de la empresa caso de estudio.
A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.		X	La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes evalúan el software desarrollado externamente y prueban que cumpla con los requisitos de seguridad establecidos en las políticas de seguridad de la información, dicha actividad no se realiza la sede Medellín de la empresa caso de estudio, sino en el nivel central a través de la oficina de Tecnologías de la información (TI).

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	X		La oficina de Tecnologías de la información (TI) a través del proceso de Direccionamiento Tecnológico de la Empresa caso de estudio, realiza pruebas a los sistemas antes de su salida a producción.
A.14.3	**Datos de prueba**				
A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.		X	Existe una política documentada donde se establece que las pruebas de los sistemas de información se realizan en ambientes separados al de producción, dicha actividad no se realiza la sede Medellín de la empresa caso de estudio, sino en el nivel central a través de la oficina de Tecnologías de la información (TI).
A.15	**RELACIÓN CON LOS PROVEEDORES**				
A.15.1	**Seguridad de la información en las relaciones con los proveedores**				
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	X		Existe una política de seguridad de la información relacionada con los proveedores, en la cual deben diligenciar y firmar los acuerdos de confidencialidad y acuerdos de intercambios de información con personal externo, sedes y dependencias
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	X		Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados, los cuales son formalizados en cada uno de los contratos establecidos.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	X		Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados. Dentro de los pliegos de contratación se deja una cláusula de firma de confidencialidad, estudios de confiabilidad, y acuerdos de nivel de servicio como acuerdos de soporte, servicio y garantías.
A.15.2	**Gestión de la prestación de servicios de proveedores**				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	X		Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados, de igual forma se asigna un supervisor por cada contrato, el cual es el encargado de hacer seguimiento y cumplimiento de las obligaciones de los proveedores que suministran algún servicio o bien a la empresa.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.		X	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados, así mismos se da aplicación al procedimiento de gestión de cambios, en el cual un comité realiza el concepto para aprobar o denegar cambios dentro de la plataforma tecnológica de la empresa o servicios de sistemas de información, actividad que es desarrollara por el nivel central a través de la oficina de Tecnologías de la información (TI).
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**				
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**				
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	X		El Líder del Proceso de Desarrollo Tecnológico, La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	X		Los empleados están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados. Se establecen los procedimientos a seguir. La empresa caso de estudio cuanta con un procedimiento de atención de incidentes y una guía para la atención de eventos e incidentes informáticos, las responsabilidades en materia de incidentes están a cargo del CSIRT, por sus siglas en inglés Computer Security Incident.
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X		Existen los formatos documentados disponibles para que los empleados reporten las debilidades de la seguridad de la información, los acanales para reportar debilidades de seguridad de la información, son el correo electrónico, buzón de subgerencias, comunicados oficiales y skype empresarial. Estos reportes son evaluados de forma inmediata por La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.16.1.5	Respuesta de incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	X		El Líder del Proceso de Desarrollo Tecnológico, La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes, en caso de tener incidentes de la seguridad de la información. El Equipo de Respuesta a Incidentes de Seguridad Informática "CSIRT" a cargo de la Oficina de Tecnologías de la información (TI), está compuesto por un equipo de expertos en seguridad de la información, quienes velan por la prevención, atención e investigación de incidentes que afecten la seguridad de la información. La atención de incidentes está documentada mediante el procedimiento "Atención a Incidentes".
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	X		Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	X		Existen formatos y documentos para recolectar la evidencia y emitirlos a las autoridades competentes, llámese Fiscalía General de la Nación o entes disciplinarios.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**				
A.17.1	**Continuidad de la seguridad de la información**				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	X		El Líder del Proceso de Desarrollo Tecnológico, La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y los empleados pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	X		La Empresa caso de estudio, cuenta con un Plan de Continuidad del Negocio alineado con la Norma Internacional "BS 25999", el cual es liderado por el Grupo de Continuidad de la Información de la Oficina de Tecnologías de la información (TI), que le permite recuperarse ante incidentes que amenacen la prestación del servicio de policía; para ello se cuenta con un plan de continuidad del negocio (BIA) en el que se determinan los procesos esenciales para la continuidad de las operaciones y un plan de recuperación ante desastres (DRP) en materia tecnológica.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.		X	La Empresa caso de estudio tiene definidos intervalos de tiempo para la respectiva revisión y prueba de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información, actividad que desarrolla la oficina de Tecnologías de la información (TI) del nivel central con sus sedes desconcentradas.
A.17.2	**Redundancias**				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	X		En el Plan de Continuidad del Negocio se establece la instalación e infraestructura disponible para el procesamiento de información.
A.18	**CUMPLIMIENTO**				
A.18.1	**Cumplimiento de requisitos legales y contractuales**				
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización	X		Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	X		La Empresa caso de estudio posee procedimientos para la protección de propiedad intelectual, los cuales tienen como objetivo evitar incumplimientos de carácter legal ante el uso de material o software patentado. Todos los servidores públicos y terceros que hacen uso de la plataforma tecnológica institucional solo pueden utilizar software autorizado por la Oficina de Tecnologías de la información (TI).
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.		X	Los registros están protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados, estos se clasifican según las Cuadros de retención documental y su tiempo de retención se realizará de acuerdo con estas; con el fin de cumplir requisitos legales o normativos y/o respaldar actividades esenciales de la Empresa.
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	X		Los datos personales son almacenados y protegidos de acuerdo con las conformidades de la ley y regulaciones. Mediante control de acceso por usuario, y procedimiento de control de registro establecido para tal fin.

ID. CONTROL	REFERENCIA DEL CONTROL	CONTROL	APLICABLE		PROPUESTA
			SI	NO	
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.18.2	**Revisiones de seguridad de la información**				
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		X	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información. El Área de Control Interno o un organismo auditor externo, realiza revisiones independientes sobre el cumplimiento de la Política de Seguridad de la Información.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	X		Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información con el fin de verificar el nivel de cumplimiento, controles y políticas de seguridad de la información. La Empresa caso de estudio, a través de su plan anual de auditorías, garantiza el cumplimiento de la política de seguridad de la información, buscando el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X		La oficina de Tecnologías de la información (TI) y el Promotor de la seguridad de la información de la sede Medellín, verificará los sistemas de información, equipos de procesamiento, bases de datos y demás recursos tecnológicos, para que cumplan con los requisitos de seguridad esperados teniendo en cuenta las solicitudes internas.

Fuente: Propiedad del autor.

6. PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LA NORMA ISO 27001:2013, PARA LA SEDE MEDELLÍN.

Las presentes políticas se seguridad de la información son producto del mejoramiento de las ya existentes y relacionadas en el Manual de seguridad de la información de la empresa caso de estudio.

6.1 Política de seguridad de la información

Los miembros de la empresa caso de estudio se comprometen a salvaguardar sus activos de información con el fin de protegerlos de las amenazas que se ciernen sobre ellos, a través de la implementación de un Sistema de Gestión de Seguridad de la Información que permita la adecuada gestión del riesgo, la generación de estrategias de seguridad basada en las mejores prácticas y controles, el cumplimiento de los requisitos legales, la oportuna gestión de los incidentes, y el compromiso Institucional de mejora continua.

6.1.1 Política para dispositivos móviles

El uso de equipos institucionales, fuera de las instalaciones de la empresa, está restringido a equipos portátiles y móviles, se aprueba el uso de los dispositivos móviles autorizados por la empresa por parte de los empleados de la entidad, siempre y cuando no pongan en riesgo la Seguridad de la Información.

Objetivo: garantizar la seguridad de la información en los equipos fuera de las instalaciones de la empresa.

Aplicabilidad: dirigida a todo el personal de la empresa.

Directrices

La seguridad para estos equipos será equivalente a la suministrada dentro de las instalaciones de la empresa, con controles adicionales que permitan mitigar los riesgos que por sí mismo conlleva el uso de estos, así:

- Es responsabilidad del empleado garantizar el adecuado uso del medio móvil asignado, conectándolo siempre a redes confiables, que no sean de acceso público para evitar que se propague cualquier amenaza pertinente a estos dispositivos (virus, troyanos, malware).
- No será permitido almacenar en dispositivos móviles personales, información de la empresa caso de estudio que no esté clasificada como pública.
- El software instalado en los dispositivos móviles debe estar totalmente licenciado y autorizado por la Oficina de Tecnologías de la información (TI).
- La información almacenada en los equipos de cómputo portátiles deberá mantenerse cifrada o monitoreada por medio de las herramientas que la Empresa caso de estudio designe para tal fin.
- El trabajo remoto solo será autorizado por el responsable de la sede Medellín de la cual dependa el empleado que solicite el permiso. Dicha autorización solo se otorgará por la Oficina de Tecnologías de la información (TI) una vez se verifique las condiciones de seguridad del ambiente de trabajo.
- El acceso a los equipos móviles se realiza mediante el uso de usuario y contraseña.
- Los empleados autorizados podrán acceder a la red de la Empresa caso de estudio únicamente por medio de túneles SSL o VPN y utilizando los equipos de cómputo institucionales asignados para realizar sus funciones o equipos externos previamente autorizados con su debida justificación.

6.1.2 Política seguridad de los recursos humanos

El recurso humano es el activo más valioso de la empresa caso de estudio, por esto la importancia de contar con personal idóneo para desempeñar las funciones para

las cuales han sido contratados; así mismo se requiere de su compromiso y conocimiento con respecto a la seguridad de la información.

Objetivo: asegurar que el personal contratado cumpla con las políticas de seguridad de la información.

Aplicabilidad: dirigida al Grupo Talento Humano de la empresa.

Directrices

- El procedimiento para confirmar la veracidad de la información suministrada por el personal que se postula como candidato a ingresar a la empresa caso de estudio antes de su vinculación definitiva, se debe realizar acorde con lo establecido en el proceso Seleccionar el Talento Humano de la empresa.
- Todos los empleados, personal de prestación de servicios o cualquier otro tipo de vinculación con la empresa, deben diligenciar los formatos Declaración de Confidencialidad y Compromiso con la Seguridad de la Información.
- El personal externo o contratista diligenciará el formato Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Contratistas o Terceros y este hará parte integral del contrato o acuerdo de cooperación que debe reposar junto con las hojas de vida en las oficinas de Talento Humano de cada sede.

6.1.3 Política de control de acceso

Se establece como control a los recursos tecnológicos, el modelo de Administración de identidades y Control de acceso (IAM), implantado mediante el Sistema de Identificación Digital, que de manera integrada al Sistema de Talento Humano le permite administrar el ciclo de vida de los usuarios, desde la creación automática de las cuentas, roles y permisos necesarios hasta su inoperancia; a partir de las novedades reportadas por los grupos de talento humano; lo anterior para que el empleado tenga acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, autorización y auditoría.

Objetivo: definir los respectivos controles para el acceso a la información.

Aplicabilidad: dirigido a personal de desarrollo tecnológico.

Directrices

- Todos los desarrollos de Sistemas de Información para uso de la empresa deben estar integrados al SID (Sistema de Identificación Digital).
- La Identificación Digital o usuario empresarial es entregado al empleado una vez ingresa a la empresa y es registrado en el Sistema de Talento Humano, e ingresa por primera vez a la plataforma y acepta términos de uso que allí encuentra.
- El control de acceso a la información a través de los diferentes sistemas de información que posee la empresa se realiza a través de roles que administran los privilegios de los usuarios dentro del sistema de información.
- El control de acceso a información física o digital se realiza teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

6.1.4 Política sobre el uso de controles criptográficos

Se utilizan sistemas y técnicas criptográficas para la protección de la información, previo análisis de riesgos sobre los activos de información con mayor nivel de clasificación, con el fin de procurar una adecuada protección de su confidencialidad e integridad.

Objetivo: Aplicar controles criptográficos para mantener la integridad y confidencialidad de la información.

Aplicabilidad: dirigida a todo el personal de la empresa.

Directrices

El uso de controles criptográficos contempla los siguientes aspectos, así:
1. Se utilizarán controles criptográficos en los siguientes casos:

- Protección de contraseñas de acceso a sistemas y demás servicios que requieran autenticación.
- Transmisión de información sensible al interior de la empresa caso de estudio y fuera de ella.
- Transmisión de información de voz a través de los radios de comunicación.
- Servicios institucionales que recopilen información de terceros.
- Uso de correo electrónico institucional, vía web.
- Mensajería instantánea institucional.
- Firma digital de documentos y correos electrónicos.

2. Se genera el servicio de certificado digital cerrado, para proveer integridad, autenticidad y no-repudio a la información digital Institucional.

3. Los protocolos que se establezcan respecto a la administración de claves de cifrado, recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves de cifrado.

4. El Grupo de Seguridad de la Información del proceso de Direccionamiento Tecnológico es el encargado de administrar e implementar los controles criptográficos; a excepción de los Centros de Protección de Datos, quienes cumplirán estas funciones, al interior de cada una de las sedes.

6.1.5 Política de escritorio y pantalla limpia.

Esta política tiene como fin reducir los riesgos de acceso no autorizado, pérdida y/o daño de la información.

Objetivo: minimizar riesgos en la exposición de la información en escritorios y equipos de cómputo.

Aplicabilidad: dirigida a todo el personal de la empresa.

Directrices

- Almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.
- Bloquear la sesión de los computadores personales cuando no se está usando. El protector de pantalla se encuentra configurado, para que se active en forma automática después de cinco (5) minutos de inactividad.
- Proteger los puntos de recepción y envío de correo postal, las impresoras, fotocopiadoras y máquinas de fax no atendidas.
- Retirar inmediatamente la información sensible, una vez impresa.
- Los escritorios de los equipos de cómputo no deben tener accesos directos a archivos.

6.1.6 Política Protección contra código malicioso

Esta política tiene como fin prevenir la infección por parte de programas maliciosos (virus, gusanos, troyanos, etc.) de los equipos de la empresa, impidiendo de esta manera el acceso no autorizado, la pérdida y/o daño de la información.

Objetivo: Proteger los equipos de cómputo de infección por parte de programas maliciosos que pongan en riesgo la operación de la empresa.

Aplicabilidad: dirigida al grupo de seguridad de la información y direccionamiento tecnológico.

Directrices

- No se permite el uso de software no autorizado por la Oficina de Tecnologías de la información (TI).
- No se permite el intercambio de información a través de archivos planos.
- No compartir carpetas en los equipos de cómputo.

- Instalar y actualizar software de detección y reparación de virus, IPS de host, antispyware examinando computadores y medios informáticos, como medida preventiva y rutinaria.
- Mantener los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientizar y capacitar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

6.1.7 Política y procedimiento de transferencia de información

Para el intercambio de información se utiliza el formato acuerdo para la revelación de información confidencial bajo deber de reserva, así mismo se documentan los controles adicionales que contemplen cada uno de ellos.

Objetivo: proteger la información de la empresa del uso indebido de la misma por parte de los empleados.

Aplicabilidad: dirigido a personal de desarrollo tecnológico.

Directrices

- Sistemas informáticos, redes, computación y comunicaciones móviles, correo electrónico, comunicaciones de voz, servicio de correo tradicional, fax e impresoras.
- Uso de modelos de control de acceso.

- Implementación de webservices con autenticación.

6.1.8 Política de desarrollo seguro.

Los sistemas de información son soporte importante de los procesos de la empresa caso de estudio, en los cuales se busca brindar seguridad desde el momento del levantamiento de requerimientos, por lo tanto, las necesidades de seguridad, hace parte integral de las decisiones de arquitectura del software a construir y/o adquirir. El procedimiento Desarrollar Sistemas de Información, realiza levantamiento de anti requerimientos y casos de abuso, los cuales son expuestos por el Grupo de Seguridad de la Información.

Objetivo: establecer las medidas de seguridad necesarias para el desarrollo de software.

Aplicabilidad: dirigido a personal de desarrollo tecnológico.

Directrices

Las sedes en las cuales se desarrolle software deberán en lo posible separar las funciones de desarrollo, pruebas y producción; de no ser posible la separación de funciones por razones presupuestales, de personal o capacitación, se implementarán controles adicionales como:

- Todos los sistemas deben contar un módulo de auditoría, que permita almacenar los registros de transacciones realizadas desde la interfaz de usuario final o desde cualquier otra herramienta.
- Todos los equipos de procesamiento y comunicaciones deben tener activos los archivos de log’s y se envían a un syslog.
- Se debe asegurar la independencia entre el inicio de una actividad y su autorización, para evitar la posibilidad de fraude.

- Documentar de manera formal la razón por la cual no es posible segregar funciones.

6.1.9 Política de seguridad de la información para las relaciones con proveedores

La empresa caso de estudio establece los mecanismos de control en sus relaciones con personal externo que le proveen bienes o servicios. Los empleados responsables de la realización y/o firma de contratos, acuerdos o convenios con personal externo deben garantizar el cumplimiento de las políticas de seguridad de la información por parte de estos.

Objetivo: supervisar los servicios contratados con personal externo para que den cumplimiento a las políticas de seguridad de la información establecidas.

Aplicabilidad: personal externo, contratistas y proveedores.

Directrices

- Todos los contratos deben tener claramente definidos los acuerdos de niveles de servicios y ser contemplados como un numeral de las especificaciones técnicas.
- Diligenciar y firmar el formato declaración de confidencialidad y compromiso con la seguridad de la información contratistas o terceros y acuerdo para la revelación de información confidencial bajo deber de reserva.
- De acuerdo con el objeto del contrato y al acceso a la información por parte del personal externo estos deben someterse a un estudio de confiabilidad y de ser necesario estudio de credibilidad y confianza.
- Antes de permitir el acceso o la entrega de información a un tercero, se debe realizar una evaluación del riesgo, por parte del propietario del activo de información, con el fin de establecer la viabilidad de permitir el acceso a la información, para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

- El acceso a la información deberá ajustarse a los parámetros establecidos en el procedimiento entrega de Información bajo deber de reserva, proceso de gestión documental y sus procedimientos asociados.
- En las oficinas de Talento Humano se debe definir una persona responsable de supervisar el personal externo, contratista o terceros que realicen labores en las instalaciones de la sede Medellín, verificando que se encuentren debidamente diligenciados los documentos como compromiso con la seguridad de la información y exista la documentación requerida en los pliegos de condiciones del contrato (hoja de vida, estudios de seguridad, certificaciones solicitadas en las especificaciones técnicas, etc), este empleado será el encargo de coordinar con el supervisor del contrato, la firma por parte de los terceros del acta correspondiente a las medidas, controles o políticas de seguridad que se tienen en la organización.

6.1.10 Política gestión de incidentes

La empresa caso de estudio creó el CSIRT, por sus siglas en inglés Computer Security Incident Response Team, Equipo de Repuesta a Incidentes de Seguridad Informática el cual, está compuesto por un equipo de expertos en Seguridad de la Información, quienes velan por la prevención, atención e investigación de incidentes que afecten los activos de información.

Objetivo: Dar respuesta de manera oportuna a los incidentes de seguridad que se presenten.

Aplicabilidad: dirigido al grupo de Repuesta a Incidentes de Seguridad Informática y personal de la empresa en general.

Directrices

- Los incidentes deben ser documentados de acuerdo con el procedimiento Atención a Incidentes.

- Las diferentes sedes de la empresa a nacional deben reportar los incidentes generados y efectuar el respectivo análisis.
- Estos eventos deben ser registrados por el analista de seguridad de cada sede en el Sistema de Información para la Gestión de incidentes en TIC.
- Los incidentes que así lo requieran cuentan con la asesoría de Policía Judicial, para el manejo de la evidencia digital y su posible judicialización.

6.1.11 Política gestión de continuidad del negocio

La empresa caso de estudio establece un plan integral que identifica el impacto de posibles incidentes que amenazan de manera grave el desarrollo de las actividades de la empresa y genera un plan de respuesta efectivo para garantizar su recuperación.

Objetivo: Identificar las amenazas que pueden ocasionar interrupciones de los procesos o actividades que afecten el servicio de la empresa.

Aplicabilidad: Grupo Seguridad de la Información y Direccionamiento Tecnológico.

Directrices

- Evaluar y aprobar los riesgos para determinar el impacto de dichas interrupciones.
- Determinar los controles preventivos.
- Desarrollar un plan para establecer el enfoque integral con el que se abordará la continuidad de las actividades de la Institución.
- Elaborar los planes de actividades necesarios para garantizar la continuidad de los procesos de la empresa, mientras se restablecen los servicios en el sitio principal.

6.1.12 Política de gestión de activos

La empresa caso de estudio identifica y elabora un inventario de los activos de información aplicando el procedimiento Identificación y protección de los activos de la información", proceso de gestión documental y sus procedimientos asociados y designar un empleado, responsable de consolidar y administrar los activos de información.

Objetivo: Establecer responsabilidades en el manejo y uso de los activos de información.

Aplicabilidad: Grupo Seguridad de la Información y Direccionamiento Tecnológico.

Directrices

- Cada sede de la empresa debe nombrar un empleado, el cual es responsable de realizar el inventario de activos, su clasificación y recomendar ante el Comité de Seguridad de la Información el tratamiento de los mismos de acuerdo con los requerimientos establecidos.

- Para efectuar el inventario se debe aplicar la Guía identificación y valoración de activos de información, en la cual se describe la metodología que permite identificar, valorar y clasificar los activos de información, servicios, medios de procesamiento que soportan la gestión de los procesos y establecer su nivel de clasificación de acuerdo con las escalas contenidas en la misma.

- El inventario debe actualizarse como mínimo una vez al año y ser avalado por el Comité de Seguridad de la Información interno de cada sede.

- Gestionar con el responsable designado la identificación, valoración y clasificación de sus activos de información dentro del inventario, manteniendo información detallada para cada activo sobre su valoración y clasificación en

confidencialidad, integridad, disponibilidad. Igualmente deberá hacer el tratamiento adecuado correspondiente a su clasificación y corrección de inconsistencias detectadas dentro de la matriz de riesgos.

- Todos los empleados, personal que tenga vínculo directo con la empresa, propietario o custodio de activos de información, debe informar a la Oficina de tecnologías de la información (TI), las falencias en el tratamiento de la información con el fin de adoptar las acciones pertinentes para su protección.

- Una vez realizado el inventario de activos se debe dar a conocer el responsable, y/o custodio de los mismos, esta actividad de notificación se puede realizar mediante acta en la cual se le indique cual es el activo, su clasificación, sus responsabilidades y los controles aplicados a ese activo.

6.1.13 Política de gestión de contraseñas

La identificación y autenticación de usuarios se encuentra definido en la guía estándar nomenclatura de usuarios, si es usuario empresarial se realiza a través del Sistema de Información SID (Sistema de Identificación Digital)

Objetivo: gestionar de manera segura el acceso de los empleados a los sistemas de información de la empresa caso de estudio.

Aplicabilidad: Grupo Seguridad de la Información y Direccionamiento Tecnológico.

Directrices

El sistema de gestión de contraseñas de la empresa caso de estudio, es administrado a través del SID, en donde se cumple con los siguientes controles, así:

- Permite que los usuarios seleccionen y cambien sus propias contraseñas.
- Exige que se escojan contraseñas de calidad.
- Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.

- Lleva un registro de las contraseñas usadas previamente, e impide su reúso.
- No visualizar contraseñas en la pantalla cuando se está ingresando.
- Almacena y transmite las contraseñas en forma protegida.

6.1.14 Política de clasificación de la información

La información de la empresa caso de estudio se clasifica según la sensibilidad e importancia de ésta.

Objetivo: clasificar la información producida por la empresa caso de estudio para su respectivo acceso y almacenamiento por parte de los empleados.

Aplicabilidad: Grupo Seguridad de la Información y personal de la empresa en general.

Directrices

La información se clasificará de la siguiente manera:

ULTRASECRETA: información pertinente a actividades o planes de la empresa interna o externa, cuya divulgación no autorizada podría conducir a un rompimiento de acuerdos, convenios, entre otros, que afecte los intereses de la empresa.

SECRETA: información pertinente a una actividad o planes de la empresa interna o externa, cuya divulgación no autorizada podría afectar las relaciones con otras empresas, lesionar el prestigio o poner en peligro la estabilidad la misma.

RESERVADA: información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la empresa, proporcionar ventajas a la amenaza actual o potencial, o causar pérdidas a esta.

CONFIDENCIAL: información que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a una sede o persona.

INTERNA: es aquella información dirigida a los empleados, cuya divulgación, uso, alteración o destrucción podría resultar en pérdidas recuperables para la empresa, pero implica asuntos de conveniencia, facilidad de la operación, credibilidad o reputación u otros asuntos relacionados con la privacidad.

PÚBLICA: información entregada o publicada sin restricciones, sin que esto conlleve un impacto negativo de ninguna índole para la empresa.

RECOMENDACIONES

Realizar la revisión y la respectiva aprobación por parte de la alta gerencia de las políticas y controles propuestos, para su respectiva publicación y difusión tanto en la sede central como a sus sucursales.

Actualizar la declaración de aplicabilidad con las políticas y controles propuestos, los cuales están basados en la norma ISO 27001:2013, realizando para ello la respectiva difusión de la misma, al igual que la elaboración del nuevo manual de seguridad de la información.

Aplicar lo más rápido posible las políticas y controles propuestos, con el fin de minimizar riesgos y fortalecer los controles de acceso, transporte y almacenamiento de los activos de información de la empresa.

Nombrar un oficial de seguridad de la información en cada una de las sedes, como responsable de hacer seguimiento al cumplimiento de las políticas y controles para el manejo de los activos de información de la empresa.

Establecer perfiles de acceso a cada uno de los usuarios teniendo en cuenta la clasificación de la información de la empresa caso de estudio, garantizando así la confidencialidad de la información.

CONCLUSIONES

Las nuevas políticas y controles que establece la norma ISO 27001:2013, con relación a la ISO 27001:2005, nos ayudó a realizar la propuesta de actualización de los controles y políticas en la empresa caso de estudio, para fortalecer la seguridad de la información de la misma.

Con la aplicación de los controles de la seguridad de la información teniendo en cuenta la norma ISO 27001:2013, se logra la actualización de los ya adoptados por la empresa basados en la norma ISO 27001:2005, lo que nos permite adaptarnos a la evolución de los nuevos riesgos, minimizando estos de forma permanentemente, realizando las adecuaciones pertinentes para mantener la certificación en dicha norma.

Con la actualización de las políticas de seguridad de la información, se logra aportar al mantenimiento de los controles de cada uno de los procesos en los que interactúa de forma directa o indirecta el empleado con los activos de información, lo que nos ayuda a establecer responsabilidades en el manejo y uso de cada uno de ellos para la continuidad de los servicios de la misma.

7. BIBLIOGRAFÍA

BERNAL, Jorge Jimeno. (2013). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. Disponible en: http://www.pdcahome.com/5202/ciclo-pdca/

BSI Group, (2013). Guía de Transición, Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013, Disponible en: https://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf

CONGRESO DE LA REPUBLICA. Ley 527. (21, agosto, 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. Diario Oficial. Bogotá, D.C., 1999. no .43673. p.1-19.

CONGRESO DE LA REPUBLICA. Ley 962. (8, julio, 2005). Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Diario Oficial. Bogotá, D.C., 2005. no. 46.023. p.1-17.

CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). 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. Diario Oficial. Bogotá, D.C., 2008. no. 47.219. p.1-17.

CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 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. Diario Oficial. Bogotá, D.C., 2009. no. 47.223. p.5-6.

CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47426. p.1-34.

CONGRESO DE LA REPUBLICA. Ley 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., no. 48.587. p.1-15

CONGRESO DE LA REPUBLICA. Ley 1712. (06, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., no. 49084. p.1-14.

CONGRESO DE LA REPUBLICA. Decreto 1151. (14, abril, 2008). Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., no. 46960. p.1-4.

CONGRESO DE LA REPUBLICA. Decreto 1377. (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial. Bogotá, D.C., no. 48834. p.1-11.

CONGRESO DE LA REPUBLICA. Decreto 103. (20, enero, 2015). Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., no. 49400. p.1-16.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución 2258. (23, diciembre, 2009). Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Diario Oficial. Bogotá, D.C., no. 47572. p.1-6.

ESTÁNDAR INTERNACIONAL ISO/IEC 17779. Tecnología de la información Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información [en línea]. s.l.: s.n., 2005. [citado el 19-04-16]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

HURTADO DE BECERRA, Jacqueline. Metodología de la investigación holística. Caracas Venezuela, Edit. Sypal. 2000. p.20.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Referencias documentales para fuentes de información electrónicas. NTC 4490. Bogotá, D.C.: El Instituto 1998. p. 27.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá, D.C.: El Instituto 2006. p.3-38.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Presentación de tesis, trabajos de grado y otros trabajos de investigación. NTC 1486. Bogotá, D.C.: El Instituto 2008. p.41.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Referencias bibliográficas. Contenido, forma y estructura. NTC 5613. Bogotá, D.C.: El Instituto 2008. p.38.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información. Requisitos. NTC-ISO/IEC 27001. Bogotá, D.C.: El Instituto 2013. p.26.

ISO 27000.ES, El portal de ISO 27001 en español, Op. Cit. Disponible en: http://www.iso27000.es/iso27000.html

ISOTools Excellence. (07 de Mayo de 2015). Sistema de Gestión de Seguridad de la Información. Blog especializado en sistemas de gestión de la seguridad informática [Blog]. Disponible en internet: http://www.pmg-ssi.com/

LOPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. Sistema de Gestión de la Seguridad de la Información. Madrid. 2005. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

VARGAS, Ana Cecilia y CASTRO MATTEI, Alonso. Sistemas de gestión de seguridad de la información [en línea]. San José Costa Rica: Universidad de Costa Rica, s.f. [citado el 22-04-16]. Disponible en: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf