RESUMEN – TRABAJO DE GRADO

AUTORES	ANA MELISSA RODRIGUEZ CHINCHILLA WILMER ALEXANDER ORTIZ CAYCEDO LEONAR EMIR OTALVAREZ OSORIO PEDRO ALFONSO ATUESTA VERA
FACULTAD	FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
DIRECTOR	ANDRES MAURICIO PUENTES VELASQUEZ
TÍTULO DE LA TESIS	DISENO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA-CESAR.

RESUMEN

(70 palabras aproximadamente)

La auditoría de sistemas es un proceso donde se hace una revisión, una evaluación y la presentación de un informe final para la empresa, busca la evaluación de una manera crítica una determinada realidad para posteriormente emitir una opinión sobre un aspecto determinado o sobre la totalidad del proceso auditado, con la auditoria de sistemas se busca evaluar los sistemas y procedimientos de una empresa, de manera que se pueda determinar si el diseño y aplicación de estos son correctos; teniendo en cuenta este concepto se desarrolla el presente trabajo con la intención generar un guía de políticas de seguridad de la información que permita identificar la manera adecuada para usar las tecnologías de la información al interior del Establecimiento Penitenciario y Carcelario de la Ciudad e Aguachica Cesar.

CARACTERÍSTICAS

PÁGINAS: 68	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DISENO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA-CESAR.

ANA MELISSA RODRIGUEZ CHINCHILLA
WILMER ALEXANDER ORTIZ CAYCEDO
LEONAR EMIR OTALVAREZ OSORIO
PEDRO ALFONSO ATUESTA VERA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
OCAÑA
2014

DISEÑO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA-CESAR.

ANA MELISSA RODRIGUEZ CHINCHILLA
WILMER ALEXANDER ORTIZ CAYCEDO
LEONAR EMIR OTALVAREZ OSORIO
PEDRO ALFONSO ATUESTA VERA

Trabajo de Grado presentado para optar al título de Especialista en Auditoria de Sistemas

Director del Proyecto
ANDRES MAURICIO PUENTES VELASQUEZ
Magister (c)
Esp. Practica Docente Universitaria
Ingeniero de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
OCAÑA
2014

DEDICATORIA

A Dios por ser el creador de todas las cosas.

Ana Melissa Rodriguez Chinchilla

Dedico este logro a mi madre Blanca Caicedo de Ortiz (Q.E.P.D), por ayudar a forjar mi camino, y asi poder estar donde estoy hoy en dia.

Wilmer Alexander Ortiz Caicedo

AGRADECIMEINTOS

Primeramente a Dios por ser quien me permitió realizar con éxito este proceso que ahora termino.

A mi mama por ser ese apoyo incondicional con el que se que siempre puedo contar, por sus regaños y llamados de atención siempre con las mejores intenciones, pero principalmente por su gran amor y oraciones.

A mi papa por ser la persona que me encamino en el amor por la Ingeniería de Sistemas.

A mi hermana por sus palabras de aliento en los momentos en los que sentí desfallecer.

A ti, esa persona especial que me brindo su apoyo en momentos difíciles.

A nuestro director Andres Mauricio Puentes Velasquez por su apoyo, paciencia y su amable colaboración..

Y finalmente a todas y cada una de las personas que me han apoyado para la culminación de esta etapa de mi vida.

Ana Melissa Rodriguez Chinchilla

Antes que nada agradezco a Dios, por sus bendiciones, por darme fortaleza y sabiduría, a las dos mujeres que más amo mi querida madre y a Egna Gómez por todo su apoyo en aquellos momentos difíciles, y a mi hombresito de 2 años que es la luz de mis ojos y que con el solo hecho de compartir con él pequeños momentos me alegra la vida y me da ánimos de continuar mis proyectos.
Al profesor Mauricio por sus orientaciones, su valioso apoyo y dedicación de tiempo en la asesoría del trabajo de grado, a la ingeniera Torcoroma y a todos los docentes que me dejaron sus valiosas enseñanzas para mi vida profesional, y por ultimo pero no menos importante a mis compañeros de grupo.
A todos gracias totales…

Pedro Alfonso Atuesta Vera

Inicialmente a Dios sobre todas las cosas.
A mis padres y hermanos.

Wilmer Alexander Ortiz Caicedo

A mi madre Carmen Elena Osorio, por su apoyo incondicional.
A mis hijos Alana Camila y Wilson Daniel, por ser el motor de mi vida.

Leonar Emir Otalvarez Osorio

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRAFICAS

Pág.

INTRODUCCION

La auditoría de sistemas es un proceso donde se hace una revisión, una evaluación y la presentación de un informe final para la empresa, busca la evaluación de una manera crítica una determinada realidad para posteriormente emitir una opinión sobre un aspecto determinado o sobre la totalidad del proceso auditado.

Con la auditoria de sistemas se busca evaluar los sistemas y procedimientos de una empresa, de manera que se pueda determinar si el diseño y aplicación de estos son correctos; teniendo en cuenta este concepto se desarrolla el presente trabajo con la intención generar un guía de políticas de seguridad de la información que permita identificar la manera adecuada para usar las tecnologías de la información al interior del Establecimiento Penitenciario y Carcelario de la Ciudad e Aguachica Cesar.

La política de seguridad de la información planteada, se divide en tres capítulos que conforman el cuerpo de la política; el primer capítulo denominado Organización de la Seguridad de la Información, contiene directrices con respecto a la conformación y funciones del comité de seguridad de la información además de la gestión de activos, el segundo capítulo comprende los enunciados y controles de la política como tal y se denominó Enunciados de la política finalmente el capítulo tres está compuesto por un glosario de términos que ayudaran al lector a comprender la política.

1. TITULO

DISEÑO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA-CESAR.

1.1 PLANTEAMIENTO DEL PROBLEMA

El EPMSC (Establecimiento penitenciarios de mediana seguridad carcelaria) de Aguachica Cesar descentralizado de la dirección general del INPEC, en cumplimiento a las leyes de Colombia recepciona, personas infractoras derivadas de conductas inapropiadas, para el estado colombiano. Basado en un sistema de información SISIPEC WEB, el cual permite ingresar las situaciones jurídicas de cada trasgresor y la aplicabilidad del proceso de reinserción a la sociedad, como está tipificado en la misión de la institución. De acuerdo a lo observado el establecimiento de Aguachica Cesar, la información no es manejada de forma segura, el acceso a la información no tiene una restricción en un alto grado, el acceso de personal no autorizado a la información no se encuentra restringido, la información no es destruida sino que por el contrario se conserva, la infraestructura del establecimiento no es acorde al nivel de seguridad que se debe manejar en un estamento de este peso.

Por otra parte, el acceso a la plataforma y por ende a la información lógica no es restringido, no se manejan cambios de claves periódicos, sino que se mantienen las mismas.

1.2 FORMULACION DEL PROBLEMA

¿Con el diseño de una guía de políticas de seguridad de la información se proporcionará una herramienta que optimice la seguridad en la gestión de la información en el establecimiento penitenciario y carcelario de Aguachica-Cesar?

1.3 OBJETIVOS

1.3.1 Objetivo general

Diseñar una guía de políticas de seguridad de la información para el establecimiento penitenciario y carcelario de Aguachica-cesar.

1.3.2. Objetivos específicos

Diagnosticar la seguridad física y lógica del establecimiento penitenciario y carcelario de Aguachica-Cesar

Definir la norma o estándar adecuado para el planteamiento de las políticas de seguridad de la información.

Plantear una política de seguridad para el manejo de la información en el establecimiento penitenciario y carcelario de Aguachica-Cesar.

1.4 JUSTIFICACION

En el establecimiento penitenciario y carcelario de la ciudad de Aguachica se cuenta con sistemas de información que apoyan los procesos de gestión tal como SISIPEC WEB, el cual gestiona la información jurídica de los internos, se hace necesario desarrollar una guía de políticas de seguridad de la información para este establecimiento debido a que en todas las organizaciones la información es el bien más importante, y el manejo inadecuado de esta ocasiona graves daños.

Al entrar en funcionamiento el aplicativo SISIPEC WEB en establecimiento penitenciario y carcelario de la ciudad de Aguachica Cesar, se comienza una nueva era en el uso de las TIC Debido a que los procesos se realizaban de forma manual, presentando altos niveles de pérdida de la información, con la implementación de este aplicativo se ha logrado una mayor agilidad en el manejo de la información de la situación jurídica de los internos y reportes de los diferentes cambios del estado procesal.

Con el fin de salvaguardar la información de las situación jurídica de la población reclusa, es importante aplicar controles a la alimentación y recepción de la información, puesto que en el momento que exista una pérdida de información se retrasarían las actuaciones judiciales, provocando caos de los beneficios administrativos y resocialización de los señores internos.
Con la creación de una guía de políticas de seguridad de la información, se dará solución a los problemas encontrados en el establecimiento, se manejará de una forma mas segura el acceso a la información física por parte de personal autorizado UNICAMENTE, en igual medida en la destrucción de forma segura de la información que ya no se requiera usar.

Por otra parte, restringir el acceso a las oficinas donde reposa la información, UNICAMENTE a personal autorizado, con su respectiva identificación.

En la parte de la información lógica, con la guía de políticas de seguridad de la información, implementar el cambio de claves de acceso de una forma periódica y validar claves con un alto grado de dificultad para ser robadas.

Con las soluciones planteadas anteriormente, se pretende que el establecimiento crezca en la parte de la seguridad en cuanto al manejo de la información y el acceso a la misma.

1.5 HIPOTESIS

Mediante el diseño de una guía de políticas de seguridad de la información, se busca dotar al establecimiento con una herramienta de apoyo que permita optimizar la gestión de la información al interior del establecimiento penitenciario y carcelario de la ciudad de Aguachica Cesar.

1.6 DELIMITACIONES

1.6.1 Conceptuales. Durante el proceso de investigación se llevará a cabo el estudio de normas y estándares inherentes a la seguridad de la información y desarrollo de políticas de seguridad.

1.6.2. Espaciales. Este estudio se realizara en la ciudad de Aguachica, en el establecimiento penitenciario y carcelario (INPEC)

1.6.7. Temporales. El proyecto tendrá un tiempo de desarrollo de un periodo de 4 meses a partir de la fecha de aprobación del anteproyecto, de acuerdo con las actividades planteadas en el cronograma.

2 MARCO REFERENCIAL

2.1 MARCO HISTORICO

El Instituto Nacional Penitenciario y Carcelario (INPEC), fue creado en diciembre de 1992, mediante el decreto 2160, fusionando la dirección general de prisiones y el fondo rotatorio del ministerio de justicia y la imprenta nacional, cuya naturaleza jurídica es de un establecimiento público de orden nacional adscrito al ministerio de justicia y derecho, cuyo fin es la reinserción social.

Bajo la ley 065 de 1993, se expide el código penitenciario y carcelario, marco normativo en el cual se basa el INPEC para la ejecución de las sanciones penales que no denigre la dignidad humana acorde a la carta magna de los comité de derechos humanos.

Hoy el INPEC tiene el control sobre 139 establecimientos penitenciarios y carcelarios, clasificados asi: una Colonia Agrícola (CA), cuatro Establecimientos Penitenciarios y Carcelarios de Alta y Mediana Seguridad (EPCAMS), dos Establecimientos Penitenciarios de Alta y Mediana Seguridad (EPAMS), doce Reclusiones de Mujeres (RM), diez Establecimientos Penitenciarios (EP), diecinueve Establecimientos Carcelarios (EC), ochenta y nueve Establecimientos Penitenciarios y Carcelarios (EPC), dos Establecimientos de Reclusión Especial (ERE). Existen establecimientos penitenciarios y carcelarios con pabellones destinados como Establecimientos de Reclusión Especial (ERE). El manejo del sistema carcelario en cuanto a políticas y estrategias de desarrollo de efectúa a través de seis regionales que abarcan el total de establecimientos en todo el país (INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

El establecimiento Penitenciario y Carcelario de Aguachica fue fundado en 1985, figurando como Director Fernando Olaya Moncada docente de profesión, contaba con 7 funcionarios incluido el Director del Establecimiento 5 Dragoneantes masculinos y 1 femenino y adicionalmente contaba con un médico de contratación, durante el periodo de 1985 a 1995 la población carcelaria fluctuaba entre 30 y 80 internos promedio, y a su vez contaba con un pabellón femenino.

En su evolución histórica, se presentaron épocas difíciles por la incursión de grupos al margen de la ley, en la cual destacamos tres que se podría decir son las más relevantes por su alto contenido de violencia.

Como la presentada el día 22 de Noviembre de 1994, siendo las 12: 30 A.m. incursiono un grupo Paramilitar fuertemente armado, en busca de 5 guerrilleros que se encontraban dentro del establecimiento sindicados por el delito de porte ilegal de armas y rebelión, uno de los cinco fue sacrificado cerca al baño, y los cuatro restantes fueron hallados en diferentes partes de Aguachica y por las actas de defunción y por las necropsias se logró establecer que eran los internos del establecimiento. (INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

2.1.1 Antecedentes. Las condiciones carcelarias en toda América Latina y el Caribe, donde las personas privadas de libertad se encuentran hacinadas, carecen de alimentación adecuada, servicios sanitarios y atención de salud- constituyen una de las mayores violaciones a los derechos humanos y configuran muchas veces un tratamiento cruel, inhumano y degradante.

La organización Amnistía Internacional, es su Informe Anual 2003, recientemente presentado, expresó que siguieron registrándose casos de tortura y malos tratos infligidos por las fuerzas de seguridad y los guardias penitenciarios en al menos 20 países de la región, entre ellos Argentina, Bahamas, Belice, Bolivia, Colombia, Guyana, Jamaica, Trinidad y Tobago y Venezuela. En países como Brasil, Ecuador y México, la tortura a los detenidos y presos siguió siendo una práctica generalizada.

Así mismo se recibieron informes de las duras condiciones penitenciarias en toda la región, por ejemplo en países como Belice, Bolivia, Brasil, Ecuador, Estados Unidos, Jamaica, Perú y Uruguay, y de casos de muertes bajo custodia en Brasil y Estados Unidos.

Los presos y presas, además de estar privados de libertad por haber cometido un delito, son despojados prácticamente de todos sus derechos básicos y sujetos a condiciones insalubres y con frecuencia decididamente violentas.

Las cárceles lejos de ser lugares donde los infractores e infractoras a la ley reparan el daño causado y se rehabilitan para insertarse en la sociedad, se han convertido en depósitos de seres humanos y escuelas del crimen.

Como sostiene Raúl Zaffaroni el proceso de prisionización produce en la persona recluida en una institución total, un proceso de deterioro casi irreversible. La prisión es una institución que se comporta como una verdadera máquina deteriorante y genera una patología cuya característica más saliente es la regresión. El preso es llevado a condiciones de vida que nada tienen que ver con las del adulto, se le priva de todo lo que usualmente hace el adulto. Por otra parte se le lesiona la autoestima en todas las formas imaginables: pérdida de privacidad y de su propio espacio, sometimiento a requisas degradantes, falta de asistencia médica, etc.

No es novedad que estamos presenciando la crisis de la pena privativa de libertad, y que la pena no cumple con los diferentes fines que se le ha venido otorgando, ya que la misma no intimida, no resocializa, no rehabilita, a lo sumo podemos concluir que la pena tiene un fin meramente retributivo.

Sin embargo, es inviable la eliminación total de la pena privativa de libertad –más allá de los seductores planteos realizados por las teorías abolicionistas- la que constituye "una amarga necesidad" y continúa siendo la “reina de las penas”.

El gran problema es que debido al aumento de la criminalidad en los últimos años, y ante el reclamo de los ciudadanos por una mayor seguridad en sus comunidades, la clase política y el Poder Judicial se han visto presionados para actuar duramente contra el crimen. Esto ha provocado que los tribunales impongan condenas privativas de libertad y penas muy elevadas, hasta para delitos relativamente menores y se resistan a la aplicación de sanciones alternativas a la prisión. (Noel Rodriguez, 2011)

Tabla N°1 Personas Presas en America Latina y el Caribe, Tasas Cada Cien Mil Habitantes, 1992-2002

	1992	1994	1995	1996	1997	1998	1999	2000	2001	2002
A. LATINA										
Argentina	63	68	74	97	96	99	106			
Bolivia					80	86	102	110	97	
Brasil	75	82	93		104		115	132	135	137
Colombia	92	96	97	119	128	127	137	145	156	
Costa Rica	103	107	118	129	156	158	164	154	178	176
Chile	155	150	155	163	172	181	205	214	216	212
Ecuador	74	81	84	94	80	78	69		61	59
El Salvador	101	109	124	138	157	136	112	119	141	158
Guatemala				62			74			70
Haití			21	37	44	47	51			
Honduras	110	138	158	163	150	155	172			174
México	102	98	102	109	117	128	143	153		
Nicaragua	83	97	104	116	110	136	146	129	123	137
Panamá	178	224	232	274	288	300	303	305	332	335
Paraguay				69	74	73	76			
Perú	77	83	88	96	100	104	108	107	103	103
Rep.Dom.	148	155	164	132	143	169	172			
Uruguay	96	100	99	101	106	119	121	128	146	166
Venezuela				102	112	106	98			
EL CARIBE										
Belice	310	343	293	349	462	448	459			
Dominica	387	354	392	427	456	421	420			
Guyana	174	169	183	188	206					
Jamaica	178	168	171	161	166	162	170			
St. Kitts N			295	268	268	288	338			
St. Lucía	210	263	263	269	269	216	243			
Sn. V Gr.	294	298	323	318	375	390	368			
Surinam	308	287	302	327	365	382	437			
T. Tobago	269	285	299	324	349	353	351			

(Carranza, 1999)

2.2 MARCO CONCEPTUAL

La Información. La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente.

Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

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. (ISO/IEC, 2005).

Sistema de Informacion. Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico. Sin embargo en la práctica se utiliza como sinónimo de "sistema de información computarizado".

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.

Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardad en la sesión o proceso anterior.

Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, graficadores, cintas magnéticas, diskettes, la voz, etc. (Vega Briceño, 2005)

Seguridad de la Informacion. La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan 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. (ISO/IEC, 2005).

Guia. Se define como el documento que describe en forma sistemática y metodológica, los objetivos, técnicas y procedimientos de las diferentes herramientas de control, para realizar los estudios, análisis y evaluaciones a las entidades o sujetos de control. (RAE, 2009)

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. (ISO/IEC, 2005)

Riesgo. Riesgo es una palabra antigua y de uso común en muchas lenguas. En su uso corriente denota incertidumbre asociada a un evento futuro o a un evento supuesto. Una descripción con sentido común del término riesgo debería incluir las circunstancias que amenacen con disminuir la seguridad, el bienestar social, la salud, el bienestar y la libertad de una entidad determinada. Esta descripción no apunta a definiciones técnicas o específicas del riesgo, pero ejemplifica el rango de aplicaciones que posee ese término y aclara que el concepto de riesgo está estrechamente ligado a valores humanos significativos. El riesgo puede consistir en la mera posibilidad de un hecho adverso, en la causa de un evento, en la magnitud de la consecuencia, en alguien o algo considerado como peligroso y también en la conceptualización de un procedimiento para la estimación de una cantidad. En un sentido genérico el riesgo incluye una variedad de aspectos, todos los cuales constituyen el concepto de riesgo. Es obvio el enfoque futuro de estas acepciones, aunque el riesgo puede también considerarse desde una perspectiva histórica cuando es interpretado desde el punto de vista de aquellos que están involucrados. (Diaz Ceballos, 2007)

Estándar ISO/IEC 27002. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

El Estándar Internacional nace bajo la coordinación de dos organizaciones:

ISO: International Organization for Standardization.

IEC: International Electrotechnical Commission.

El Estándar Internacional ISO/IEC 27002 va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

El Estándar Internacional ISO/IEC 27002 contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

Política de seguridad.
Aspectos organizativos de la seguridad de la información.
Gestión de activos.
Seguridad ligada a los recursos humanos.
Seguridad física y ambiental.
Gestión de comunicaciones y operaciones.
Control de acceso.
Adquisición, desarrollo y mantenimiento de los sistemas de información.
Gestión de incidentes en la seguridad de la información.
Gestión de la continuidad del negocio.
Cumplimiento. (EcuRed, 2010)

COBIT. (Control Objectives Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez. (CIBERTEC, 2007)

INPEC. El Instituto Nacional Penitenciario y Carcelario, es un Establecimiento Público del Orden Nacional adscrito al Ministerio del Interior y de Justicia, con personería jurídica, autonomía administrativa y patrimonio independiente. (INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

SISIPEC. Sistematización Integral del Sistema Penitenciario y Carcelario. Este sistema de información permite la organización sistemática de la información de los internos desde el momento de su ingreso al Establecimiento de Reclusión, hasta cuando salen en libertad. (INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

SISIPEC entre muchos otros beneficios permite:

- Establecer el número exacto de internos que ingresan al INPEC en tiempo real, dando oportunidad y veracidad a la información.

- Fácil y rápida ubicación del interno.

- Identificar plenamente la ocupación del personal en cada programa.

- Consultar la información los internos condenados o sindicados, en el momento que se requiera, con tiempo de respuesta eficaz para toda la información penal y penitenciaria del interno actualizada, precisa y completa.

- Seguridad en la información, sólo puede ser accesada mediante un usuario autorizado y contraseña, más toda la seguridad en infraestructura tecnológica necesaria.

- Oportuna atención al usuario externo como abogados, notificadores, autoridades, familiares de internos, etc.

- Controla la salida en libertad de los internos que tienen procesos requeridos por otra autoridad.

Políticas de Seguridad. Se define como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema. (Organización Internacional de Normalización., 1988), al tratarse de "términos generales", aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina política de aplicación específica. (Sead, Ahmed, Peter, Rafael, Jan, & Unto, 1993)

Seguridad Física. La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. (GOBIERNO DE ARAGON, 2007)

Seguridad Lógica. La seguridad lógica de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y la información contenida en él. El

activo más importante de un sistema informático es la información y, por tanto, la seguridad lógica se plantea como uno de los objetivos más importantes. (GOBIERNO DE ARAGON, 2007)

2.3 MARCO TEORICO

Las empresas, invierten una gran cantidad de dinero en el desarrollo de plataformas que den soporte a los usuarios, pero no piensan en los riesgos que se pueden producir, en como buscar la manera de minimizar esos riesgos.

La seguridad de la información se considera como la herramienta fundamental para implantar nuevas mejoras en las empresas, razón por la cual éstas deben realizar un esfuerzo cada día mayor para optimizar su nivel de seguridad en este aspecto. La organización debe mejorar continuamente la eficacia del Sistema de Gestión del Sistema de Información (SGSI), mediante el establecimiento de políticas y objetivos de seguridad de la información, tomando en cuenta los resultados de las auditorías, análisis de eventos, y acciones correctivas y preventivas de los mismos. De igual manera, deben establecer procedimientos argumentados para identificar documentos que ya no se requieran porque se actualizaron o porque se remplazaron por otros.[Piraquive, 2009].

La seguridad de la información de una empresa, es muy importante en las empresas, debido a que la información es el bien más preciado que tiene cualquier empresa, deben salvaguardarla de la mejor manera, buscado modelos, métodos, modelos para que hayan riesgos de hurto en un pequeñísimo porcentaje.

Es de vital importancia que las empresas cuenten con una política de seguridad, que se encarguen de identificar las funciones y deberes que se deben acatar para tener en buen resguardo la información, tanto física como digital.

No basta con tener a buen resguardo la información digital, también se debe tener salvaguardada la información física que a veces se descuida, se deja visible a terceros que pueden hacer daño con ella.

Con el desarrollo de una guía de políticas de seguridad en una empresa, y dándola a conocer o socializarla con todos los empleados de una empresa.

COBIT

Las empresas necesitan la certeza de que pueden confiar en los sistemas de información y en la información producida por los sistemas, y así obtener un retorno positivo de las inversiones en TI. COBIT permite que los ejecutivos de negocios entiendan mejor cómo dirigir y gestionar el uso de las TI en la empresa y el estándar de mejores prácticas que se espera de los proveedores de TI. COBIT proporciona las herramientas para dirigir y supervisar todas las actividades relacionadas con las TI.

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.

COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI.

El uso de las TI es una inversión importante que debe ser gestionado. COBIT ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida y proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales y sea probable que entreguen los beneficios esperados.

Existe una tremenda diferencia entre las empresas que realizan una buena gestión de TI y las que no lo hacen, o no pueden. COBIT permite el desarrollo de políticas claras y mejores prácticas para la administración de TI. El marco ayuda a aumentar el valor obtenido de TI. También ayuda a las organizaciones a gestionar los riesgos relacionados con TI y a asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Debido a que COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Una vez que se identifican e implementan los principios clave de COBIT para una empresa, los ejecutivos ganan confianza en que la utilización de las TI puede ser gestionada de forma eficaz.
Los ejecutivos de las empresas pueden esperar los siguientes resultados de la adopción de COBIT:
• Los gerentes y el staff de TI entenderán totalmente como es que el negocio y TI pueden trabajar en forma conjunta para la entrega exitosa de las iniciativas de TI.

• Los costos totales del ciclo de vida de TI serán más transparentes y predecibles.
• TI ofrecerá información más oportuna y de mayor calidad.
• TI entregará proyectos de mejor calidad y más exitosos.
• Los requisitos de seguridad y privacidad serán más claros y la implementación será monitoreada con mayor facilidad.
• Los riesgos de TI serán gestionados con mayor eficacia.
• Las auditorías serán más eficientes y exitosas.
• El cumplimiento de TI con los requisitos regulatorios serán una práctica normal de gestión. (ITGI, Board Briefing on IT Governance , 2003)

ITIL

Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

• Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
• Cumplir con la legislación.
• Asignarse y entregarse de forma eficaz y eficiente.
• Revisarse y mejorarse de forma continua.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse.

Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima. (ITGI, Board Briefing on IT Governance , 2003)

ISO/IEC 27002

El Estándar Internacional ISO/IEC 27002 nace bajo la coordinación de dos organizaciones:
ISO: International Organization for Standardization.

IEC: International Electrotechnical Commission.

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información, que es en esencia de lo que trata el Estándar Internacional ISO/IEC 27002 (antiguamente llamado ISO/IEC 17799, pero a partir de julio de 2007, adoptó un nuevo esquema de numeración y actualmente es ISO/IEC 27002).

El ISO/IEC 27002 se refiere a una serie de aspectos sobre la seguridad de de las tecnologías de información, entre los que se destacan los siguientes puntos:

Evaluación de los riesgos de de seguridad: se deben identificar, cuantificar y priorizar los riesgos.
Política de seguridad: deben haber políticas organizacionales claras y bien definidas que regulen el trabajo que se estará realizando en materia de seguridad de la información.

Aspectos organizativos de la seguridad de la información: cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna (empleados o personal de la organización) como de forma externa o con respecto a terceros (clientes, proveedores, etc.)

Gestión de activos: se debe tener un completo y actualizado inventario de los activos, su clasificación, quiénes son responsables por los activos, etc.

Seguridad ligada a los recursos humanos: especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

Seguridad física y ambiental: consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

Gestión de comunicaciones y operaciones: asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización. Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

Control de acceso: deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

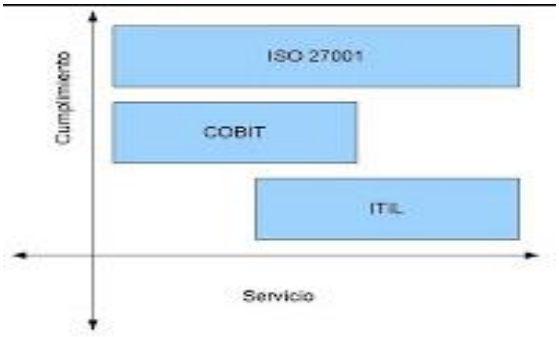
Adquisición, desarrollo y mantenimiento de los sistemas de información: consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

Gestión de incidentes en la seguridad de la información: los incidentes se pueden dar tarde o temprano, y la organización debe contar con registros y bitácoras para identificar a los causantes y responsables de los incidentes, recopilar evidencias, aprender de los errores para no volverlos a cometer, etc.

Gestión de la continuidad del negocio: se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios, etc.

Cumplimiento: debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías, etc. (ITGI, Board Briefing on IT Governance , 2003)

Grafica N°1 Comparativo



Fuente: Board Briefing on IT Governance , 2003

COBIT es un marco de control, ISO 27002 es una norma e ITIL es un marco de servicio.
Un marco de control es utilizado para hacer que las normas se cumplan y que los servicios fluyan de manera transparente y continua.

En la figura se puede observar se compara el cumplimiento y el servicio, mientras mayor es el cumplimiento se puede observar que se necesita el uso de normas como ISO 27002, para asegurar ese nivel de cumplimiento necesitamos implementar un marco de control como COBIT, ya que convive de manera natural con las normas ISO 27001 y 27002 y con un marco de servicios como ITIL.

ISO 27002 como norma o estándar se sitúa en el mayor nivel de cumplimiento, COBIT se situaría en un nivel medio de cumplimiento y por último se encuentra a ITIL, ya que como marco de servicio solo pretende habilitar el servicio y no garantizar su operación.

Para este trabajo de grado se trabajó en el estándar ISO 27002, porque el objetivo del proyecto de grado es diseñar una guía de políticas de la seguridad de la información, se descarta ITIL porque no se pretende habilitar o trabajar en un servicio determinado y COBIT solo es un conjunto de mejores prácticas que no está constituido como estándar como lo es ISO.

La norma ISO 27002 cubre las mejores prácticas para la seguridad de la información, los elementos necesarios para gestionar la seguridad, lineamientos para estructurar los planes de seguridad, los controles necesarios para implementar la seguridad en la organización y las acciones clave para minimizar los riesgos que pueden poner en peligro la seguridad de la información.

2.4. MARCO LEGAL

Ley 527 de 1999

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan disposiciones"

Ley 1273 de 2009

"Por medio del 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"

Bajo la ley 065 de 1993, se expide el código penitenciario y carcelario, marco normativo en el cual se basa el INPEC para la ejecución de las sanciones penales que no denigre la dignidad humana acorde a la carta magna de los comité de derechos humanos.

Norma Técnica Colombiana NTC-ISO/IEC 27000

- **Evaluación y tratamiento del riesgo Evaluación de los riesgos de seguridad**

La evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos. Puede ser necesario llevar a cabo el proceso de evaluación de los riesgos y la selección de controles varias veces para cubrir diferentes partes de la organización o sistemas individuales de información. Es recomendable que la evaluación de riesgos incluya el enfoque sistemático para estimar la magnitud de los riesgos (análisis del riesgo) y el proceso de comparación de los riesgos estimados frente a los criterios de riesgo para determinar la importancia de los riesgos (valoración del riesgo).

Es conveniente realizar periódicamente las evaluaciones de riesgos para abordar los cambios en los requisitos de seguridad y en la situación de riesgo, por ejemplo en activos,amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando se producen cambios significativos. Estas evaluaciones de riesgos se deberían efectuar de forma metódica que puedan producir resultados comparables y reproducibles. La evaluación de los riesgos de seguridad de la información debería tener un alcance definido claramente para que sea eficaz y debería incluir las relaciones con las evaluaciones de riesgos en otras áreas, según sea apropiado. El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil. En la norma ISO/lEC TR 13335-3 (Directrices para la seguridad de la tecnología de la información: técnicas para la gestión de la seguridad de la tecnología de la información) se discuten ejemplos de metodologías para la evaluación del riesgo. Tratamiento de los riesgos de seguridad. Antes de considerar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar si se pueden aceptar o no los riesgos. Los riesgos se pueden aceptar si, por ejemplo, según la evaluación se considera el riesgo bajo o que el costo del tratamiento no es efectivo en términos financieros para la organización. Tales decisiones se deberían registrar. Para cada uno de los riesgos identificados después de la evaluación de riesgos es necesario tomar una decisión para su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) Aplicación de los controles apropiados para reducir los riesgos.

b) Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política de la organización y sus criterios para la aceptación del riesgo.

c) Evitación de los riesgos al no permitir acciones que pudieran hacer que éstos se presentaran.

d) Transferencia de riesgos asociados a otras partes, por ejemplo aseguradores o proveedores.
Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se deberían seleccionar e implementar de modo que satisfagan los requisitos identificados por la evaluación de riesgos. Los controles deberían garantizar la reducción de los riesgos hasta un nivel aceptable teniendo en cuenta los siguientes elementos:

a) Requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales.

b) Objetivos de la organización.

c) Requisitos y restricciones operativos.

d) Costo de la implementación y la operación con relación a los riesgos que se reducen, y que permanezca proporcional a los requisitos y restricciones de la organización.

e) Necesidad de equilibrar la inversión en la implementación y operación de los controles frente a la probabilidad del daño que resultará debido a las fallas de seguridad.

Los controles se pueden seleccionar a partir de esta norma, de otros conjuntos de controles, o se pueden diseñar controles nuevos que satisfagan las necesidades específicas de la organización. Es necesario reconocer que es posible que algunos controles no se puedan aplicar a todos los sistemas y entornos de información, y pueden no ser viables para todas las organizaciones. A modo de ejemplo, el numeral 10.1.3 describe la forma en que se pueden segregar las funciones para evitar fraude y error. Es posible que las organizaciones pequeñas no puedan segregar todas las funciones y que sean necesarias otras formas de lograr el mismo objetivo de control. En otro ejemplo, el numeral 10.10 describe la forma en que se puede monitorear el uso del sistema y recolectar evidencia. Los controles descritos, como el registro de eventos, pueden entrar en conflicto con la legislación correspondiente, como por ejemplo en la protección de la privacidad para los clientes o en el sitio de trabajo. Los controles de seguridad de la información se deberían tener en cuenta en la especificación de los requisitos de sistemas y proyectos y en la fase de diseño. De lo contrario, se pueden originar costos adicionales y soluciones menos eficaces y, es posible, en el peor de los casos, la incapacidad de lograr una seguridad adecuada. Se debe recordar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización. 2.4.2.2 Capítulo 5: Política de seguridad de la información Objetivo: brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. Las directivas deberían establecer una dirección clara de la política según los objetivos del negocio y demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la política de seguridad de la información en toda la organización.
Documento de la política de seguridad de la información Control. La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes. Guía de implementación. El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.

b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.

c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.

d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización. Incluyendo los siguientes:

Cumplimiento de los requisitos legales, reglamentarios y contractuales. Requisitos de educación, formación y concientización sobre seguridad. Gestión de la continuidad del negocio. Consecuencias de las violaciones de la política de seguridad. Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información. Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios. Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

Información adicional. La política de seguridad de la información podría formar parte de un documento de política general. Si la política de seguridad de la información se distribuye fuera de la organización, es necesario tener cuidado de no divulgar información sensible.

3. DISEÑO METODOLOGICO

3.1 TIPO DE INVESTIGACION

La metodología representa la manera de organizar el proceso de la investigación, de controlar los resultados y de presentar las posibles soluciones al problema que nos lleva a la toma de decisiones. (Zorrilla A., Torres X., Cervo Amado, & Bervian, 1997)

Para el desarrollo de esta investigación se empleara la investigación de tipo descriptiva, ya que como menciona Tamayo y Tamayo: "La investigación descriptiva trabaja sobre realidades de hecho y su característica fundamental es la de presentarnos una interpretación correcta, además comprende la descripción, registro, análisis e interpretación de la naturaleza actual y la composición o procesos de los fenómenos" (Tamayo y Tamayo, 2003), con el fin de desarrolar el poryecto se llevaran a cabo las siguientes actividades, vinculadas cada una al cumplimiento de un objetivo asi:
*Objetivo 1:*Diagnosticar la seguridad física y lógica del establecimiento penitenciario y carcelario de Aguachica-Cesar

*Actividades:*Visitas al establecimiento penitenciario y carcelario de Agachica, diseño de instrumentos de recoleccion de la informacion y aplicar instrumentos de recoleccion de informacion
Obetivo 2: Definir la norma o estándar adecuado para el planteamiento de las políticas de seguridad de la información.

*Activdades:*Estudiar y analizar las etapas de la norma iso 27000 paracion entre iso 27000 y COBIT.
Objetivo 3: Crear una política de seguridad para el manejo de la información en el establecimiento penitenciario y carcelario de Aguachica-Cesar.

Actividades: Presentacion y revision del documento del anteproyecto de investigación

Definir cada uno de los controles y objetivos de control para cada uno de los dominios aplicados en la politica de seguridad de la información

3.2 POBLACION

Durante el desarrollo de este proyecto de investigación se contara con una población de estudio conformada por el personal administrativo del establecimiento.

3.3 MUESTRA

Teniendo en cuenta el número reducido de personas que conforman la población de estudio (10), se tomara a toda la población involucrada en el proceso como fuente para obtener la información necesaria.

3.4 TECNICAS DE RECOLECION DE LA INFORMACION

Fuentes Primarias:

Entrevistas al personal administrativo del Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica – Cesar.

Visita de observación y aplicación de instrumentos de recolección de la información en el Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica –Cesar.

Documentación institucional del Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica – Cesar.

Fuentes Secundarias:

Libros relacionados con la auditoria informática, seguridad informática y políticas de seguridad de la información.

Artículos científicos basados en la auditoria informática, seguridad informática y políticas de seguridad de la información.

Leyes, normas y estándares concernientes a las tecnologías de la información, técnicas de seguridad de información y políticas de seguridad e la información.

3.5 ANALISIS DE LA INFORMACION

Los instrumentos de recolección de la información elaborados para la documentación del proyecto tuvieron como base la norma ISO 27002; tomando como base la información recolectada mediante las fuentes anteriormente mencionadas se diseñaron las siguientes tablas que resumen el diagnostico o situaciones encontradas al interior del establecimiento:

Tabla N°2 Hallazgos

HALLAZGOS/OBERVACIONES	**RECOMENDACIONES**	**PROCESOS AFECTADOS**	**RIESGO**
Como resultado del proceso de auditoria en relación con la estructura organizacional del área de jurídica, se observa que no cuenta con el personal administrativo suficiente para preparar y rendir oportunamente la información institucional requerida, por lo cual es asignado el personal de custodia y vigilancia para la ejecución de labores de carácter administrativo, aspecto que podría afectar el desempeño del objeto misional del establecimiento en materia de seguridad. El establecimiento no cuenta con	Es importante que la administración del Establecimiento establezca acciones concretas tendientes a realizar un proceso de estudio, análisis y reestructuración sobre la asignación actual de los cargos y responsabilidades de todo el personal adscrito al Establecimiento, con el propósito de lograr una mejor distribución del recurso humano existente en el Establecimiento, para la	Administración de Recursos. Área: Administrativa y Financiera.	Incumplimiento de las políticas y procedimientos. Perdida de eficiencia en las operaciones. Déficit en la disponibilidad del personal de custodia y vigilancia. Concentración

el recurso humano competente para el desarrollo de los procesos misionales de Atención integral y Tratamiento penitenciario incumpliendo con lo establecido en la Ley 65 de 1993. Las responsabilidades y funciones del área de jurídica han sido asignadas al personal de custodia y vigilancia, sin considerar los perfiles y competencias requeridos para el cargo.	ejecución de los diferentes procesos misionales y de apoyo. Dicha reestructuración debe estar basada inicialmente en cubrir las necesidades prioritarias de cada dependencia para atender sus requerimientos y funciones, y considerando los perfiles asociados a las responsabilidades de cada uno de los procesos.		de funciones incompatibles.
Se observo que la información incluida en algunos expedientes de la población reclusa no se encuentran las cartillas biográficas (Impresas desde el SISIPEC WEB) de los internos, situación que podría ocasionar inconsistencias con el seguimiento de los procesos de cada interno. De otra parte se observo que según el reporte de internos se encuentran algunos sin el documento de identificación (plena identidad) y solo son relacionados por sus nombres Como resultado del proceso de auditoria al área jurídica, se identificaron diferencias registradas de acuerdo al parte diario de SISIPEC WEB en tiempo real y el parte diario de contada de internos.	Con el propósito de fortalecer el control interno de los expedientes de la Población Reclusa es importante revisar los procedimientos que actualmente están siendo aplicados por el establecimiento, para el manejo y archivos de la información que reposa en los expedientes de cada uno de los internos y tomar medidas de ajuste que correspondan a fin de dar cumplimiento a lo indicado en el artículo 56 de la Ley 65 de 1993 que establece: *"(…) En los centros de reclusión se llevara un registro de ingreso y egreso con los datos especiales de cada interno, fecha, hora de ingreso, estado físico, fotografía y reseña Dactiloscópica. Simultáneamente se*	Administración de Recursos. Área: Gestión Jurídica	Perdida o extravío de la información jurídica del personal interno. Posibles sanciones por parte de los entes de control.

	abrirá un prontuario para cada sindicado y una cartilla biográfica para cada condenado ” A su vez solicitar al establecimiento agilizar la gestión ante al resgistraduria, de la documentación de los internos requeridos. El asesor Jurídico debe oficiar los trámites correspondientes a los procesos que se le imputan al interno, para así poder definir su situación jurídica en el establecimiento. Con el propósito de fortalecer el control interno de los reportes de la población reclusa es importante revisar los procedimientos que actualmente están siendo aplicados por el establecimiento, para el manejo y archivo de la información. Implementar las herramientas de sistemas necesarias con el fin de solucionar oportunamente esta situación a fin de minimizar el riesgo de pérdida de información valiosa para el establecimiento		
El establecimiento no cuenta con el personal totalmente capacitado para el manejo de la información, SISIPEC WEB	Se recomienda implementar las capacitaciones del personal encargado del	Administración de Recursos Área:	Falta del control total del programa

El establecimiento presenta fallas en el manejo del sistema SISIPEC WEB, ya que la señal satelital llega débil al establecimiento y defectuosa.	manejo de la información Implementar las herramientas de sistemas necesarios con el fin de solucionar oportunamente esta situación a fin de minimizar el riesgo de pérdida de información valiosa para el establecimiento.	Sistemas	Riesgo de pérdida de la información Posible alteración de la información.
No cuenta con un sistema de seguridad apropiado como son: circuito cerrado de televisión, alarmas, o sensores de movimiento. El sistema utilizado en las puertas y ventanas del inmueble no son los más apropiados, debido a que las chapas de las diferentes oficinas son comunes, las cuales serian fácilmente violentadas con el fin sustraer elementos de cómputo o procesos que son llevados por las diferentes dependencias.	La división administrativa debe realizar los trámites pertinentes a fin de adquirir los elementos necesarios de seguridad, con el fin de controlar el ingreso de personal y elementos a las áreas administrativas	Custodia y Vigilancia – Seguridad Área: Comando custodia y vigilancia.	Vulnerabilidad de la seguridad del establecimiento. Posible pérdida o alteración de información. Accesos no autorizados.

Fuente: Autores del Proyecto.

Posteriormente, luego de analizar los hallazgos detectados se definió la siguiente que relaciona fuente de riesto, area de impacto y riesgo, de la siguiente manera:

Tabla N°3 Relación fuente del riesgo, área de impacto y riesgo.

Fuente del Riesgo	**Área de Impacto**	**Riesgo**
Situación Jurídica	Bienestar y convivencia	• Clasificación interna de los Reclusos • Motines y Mitines al interior del Establecimiento
Actualización SISIPEC WEB	Jurídica	• Seguridad de la Información • Seguridad del Establecimiento • Seguridad Personal de Internos
Fallas eléctricas	Establecimiento penitenciario	• Retraso en el proceso de ingreso de la información • Pérdida de la información
Eventos naturales	Establecimiento	• Pérdida de la información

	penitenciario	• Disminución en la calidad del servicio.
Organización del trabajo	Establecimiento penitenciario	• Personal subutilizado por asignación errónea de labores • Personal no capacitado para desempeñar roles.
Infraestructura	Establecimiento penitenciario	• Continuidad del servicio • Ataques terroristas

Fuente: Autores del Proyecto.

Con los anteriores aspectos definidos se plantean las politicas de seguridad de la informacion para el establecimiento.

4. PRESENTACION DE RESULTADOS

4.1 IDENTIFICACION DE LA ORGANIZACIÓN

El establecimiento Penitenciario y Carcelario de Aguachica fue fundado en 1985, figurando como Director Fernando Olaya Moncada docente de profesión, contaba con 7 funcionarios incluido el Director del Establecimiento 5 Dragoneantes masculinos y 1 femenino y adicionalmente contaba con un médico de contratación, durante el periodo de 1985 a 1995 la población carcelaria fluctuaba entre 30 y 80 internos promedio, y a su vez contaba con un pabellón femenino. En su evolución histórica, se presentaron épocas difíciles por la incursión de grupos al margen de la ley, en la cual destacamos tres que se podría decir son las más relevantes por su alto contenido de violencia.
Como la presentada el día 22 de Noviembre de 1994, siendo las 12: 30 A.m. incursiono un grupo Paramilitar fuertemente armado, en busca de 5 guerrilleros que se encontraban dentro del establecimiento sindicados por el delito de porte ilegal de armas y rebelión, uno de los cinco fue sacrificado cerca al baño, y los cuatro restantes fueron hallados en diferentes partes de Aguachica y por las actas de defunción y por las necropsias se logró establecer que eran los internos del establecimiento. (INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

Figura N°1 Establecimiento Penitenciario y Carcelario Aguachica Cesar

Fuente: Autores del Proyecto.

4.2 MISION

Contribuimos al desarrollo y resignificación de las potencialidades de las personas privadas de la libertad, a través de los servicios de tratamiento penitenciario, atención básica y seguridad, fundamentados en el respeto de los derechos humanos.

4.3 VISION

El INPEC será reconocido por su contribución a la justicia, mediante la prestación de los servicios de seguridad penitenciaria y carcelaria, atención básica, resocialización y rehabilitación de la población reclusa, soportado en una gestión efectiva, innovadora y transparente e integrada por un talento humano competente y comprometido con el país y la sociedad.

4.4 PRINCIPIOS

Respeto, fundamento de las relaciones interpersonales
Justicia, garante de la inviolabilidad de los derechos
Ética pública, soporte de las actuaciones de los servidores del INPEC

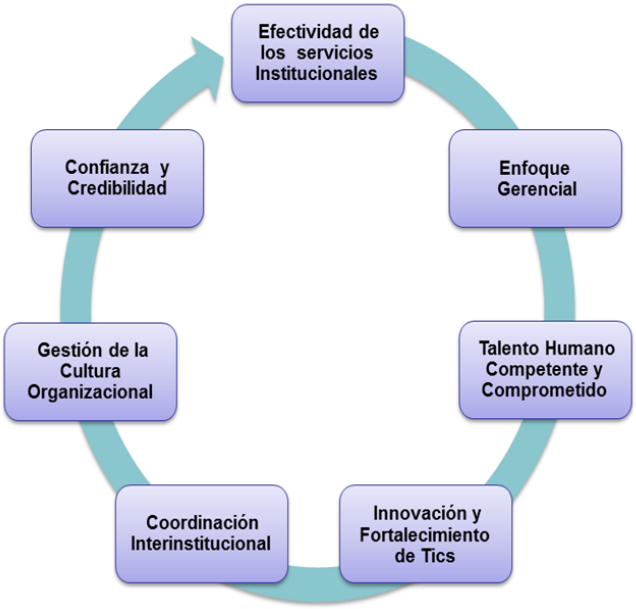
4.5 VALORES INSTITUCIONALES

Dignidad humana
Lealtad
Transparencia
Compromiso institucional
Solidaridad

4.6 LINEAMIENTOS ESTRATEGICOS

Con fundamento en los anteriores elementos, que precisan el SER y DEBER SER institucional y con el propósito de garantizar efectividad en el cumplimiento de la misión y avanzar con certeza hacia el alcance de la visión, el INPEC ha definido los siguientes lineamientos estratégicos, que orientan la gestión de los funcionarios que integran el instituto y en especial de quienes ejercen el liderazgo y dirección de los equipos de trabajo

Grafica N°2 Lineamientos Estrategicos



(INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

4.7 ESTRUCTURA ORGANICA

La estructura organica del establecimiento penitenciario y carcelario de la ciudad de Agiachica se encuentra definido de la siquiente manera:

Grafica N°3 Estructura Organica

Fuente: Autores del Proyecto.

4.8 ESTRUCTURA TECNOLOGICA

El establecimiento actualmente cuenta con 11 Equipos de cómputo, 7 impresoras, 1 Router, 1 Switch de red de 24 puertos y 1 Rack, además del cableado necesario para la infraestructura de red para desarrollar sus labores internas; los equipos que conforman la infraestructura tecnológica del establecimiento, se describen a continuación:

Tabla N°4. Especificaciones tecnicas "Computadores"

No	ESTÁNDAR	ORDEN	MARCA	CARACTERÍSTICAS
1	Equipo de escritorio	PCIA01	DELL	Pentium IV Socket mono núcleo 2.6 GHz, RAM DDR 256 MB, Monitor CRT 17" color Negro, Sistema operative windows XP Service Pack 3, Disco Duro de 160 GB.
2	Equipo de escritorio	PCIA02	HP	Pentium IV Socket mono núcleo 2.93 GHz, RAM DDR SDRAM 512 MB, Monitor CRT 17" color Negro, Sistema operative windows 7 profesional Service Pack 1, Disco Duro de 120 GB.
3	Equipo de escritorio	PCIA03	DELL	Pentium IV Socket mono núcleo 2.6 GHz, RAM DDR 256 MB, Monitor CRT 17" color Negro, Sistema operative windows XP Service Pack 3, Disco Duro de 160 GB.
4	Equipo de escritorio	PCIA04	DELL	Pentium IV Socket mono núcleo 2.6 GHz, RAM DDR 256 MB, Monitor CRT 17" color Negro, Sistema operative windows XP Service Pack 3, Disco Duro de 160 GB.
5	Equipo de escritorio	PCIA05	HP	Pentium IV Socket mono núcleo 2.93 GHz, RAM DDR SDRAM 512 MB, Monitor CRT 17" color Negro, Sistema operative windows 7 profesional Service Pack 1, Disco Duro de 120 GB.
6	Equipo de escritorio	PCIA06	DELL	Pentium IV Socket mono núcleo 2.6 GHz, RAM DDR 256 MB, Monitor CRT 17" color Negro, Sistema operative windows XP Service Pack 3, Disco Duro de 160 GB.
7	Equipo de escritorio	PCIA07	DELL	Pentium IV Socket mono núcleo 2.6 GHz, RAM DDR 256 MB, Monitor CRT 17" color Negro HP, Sistema operative windows XP Service Pack 3, Disco Duro de 160 GB.
8	Equipo de escritorio	PCIA08	HP	Pentium IV Socket mono núcleo 2.93 GHz, RAM DDR SDRAM 512 MB, Monitor CRT 17" color Negro, Sistema operative windows 7 profesional Service Pack 1, Disco Duro de 120 GB..
9	Equipo de escritorio	PCIA09	HP	Pentium IV Socket mono núcleo 2.93 GHz, RAM DDR SDRAM 512 MB, Monitor CRT 17" color Negro, Sistema operative windows 7 profesional Service Pack 1, Disco Duro de 120 GB..

10	Equipo de escritorio	PCIA10	HP	Pentium IV Socket mono núcleo 2.93 GHz, RAM DDR SDRAM 512 MB, Monitor CRT 17" color Negro, Sistema operative windows 7 profesional Service Pack 1, Disco Duro de 120 GB..
11	Equipo de escritorio	PCIA11	DELL	Pentium IV Socket mono núcleo 2.93 GHz, RAM DDR SDRAM 512 MB, Monitor CRT 17" color Negro, Sistema operative windows 7 profesional Service Pack 1, Disco Duro de 120 GB..

Fuente: Autores del Proyecto.

Tabla N°5 Especificaciones tecnicas "Impresoras"

NO	ESTÁNDAR	ORDEN	MARCA	CARACTERÍSTICAS
1	Impresora	IIAO1	HP	HP deskjet 3290
2	Impresora	IIAO2	HP	HP deskjet 3290
3	Impresora	IIAO3	HP	HP deskjet 3050 j610 series
4	Impresora	IIAO4	HP	HP deskjet 3050 j610 series
5	Impresora	IIAO5	HP	HP deskjet 3290
6	Impresora	IIAO6	HP	HP deskjet 3050 j610 series
7	Impresora	IIAO7	HP	HP deskjet 3050 j610 series

Fuente: Autores del Proyecto.

Tabla N°6 Especificaciones tecnicas "Equipos de comunicaciones"

NO	ESTÁNDAR	ORDEN	MARCA	CARACTERÍSTICAS
1	**Router**	**RIA01**	**Cisco**	**Router Wireless Cisco Linksys Wrt54g Con Dd-wrt**
2	**Switch**	**SIA01**	**Cat**	**Switch 24 Puertos Rj45 10/100/1000 Gigabit Cat 6 Rack Mmu.**

Fuente: Autores del Proyecto.

TIPO DE RED

Al interior del Establecimiento se cuenta con una Red LAN que permite la interconexión entre oficinas.

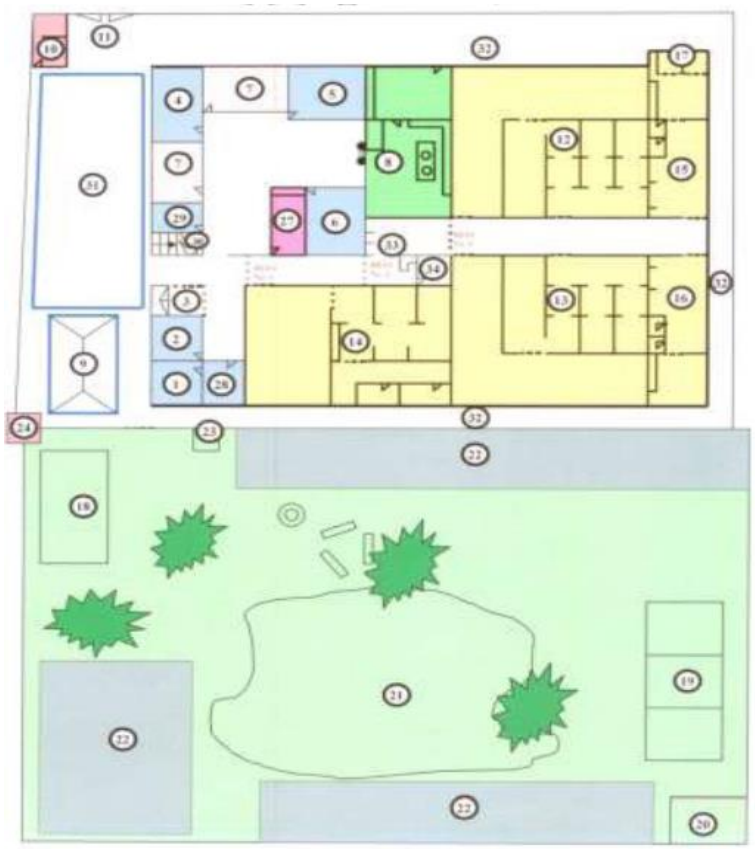
SISTEMAS OPERATIVOS

Los sistemas operativos que se encuentran instalados en los equipos del Establecimiento se describen a continuación:

4.9 ESTRUCTURA FISICA

La estructura física del establecimiento se describe en la siguiente imagen:

Figura N°2 Estructura física



(INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO, 2010)

5. DISEÑO DE UNA GUÍA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA-CESAR.

De acuerdo con los hallazgos encontrados en el Establecimiento, se propone una politica de seguridad de la informacion basado en dominios epsecificos de la ISO 27002, estos pemritieron estrucrutar la politica de acuerdo a las necesidades del establecimiento.

La guia de politicas, sera presentada a la direccion del estabecimiento para su debido analisis y aprobacion, de forma que esta pueda ser aplicada, la guia esta estructurad en capitulos que reunen grupos de controles.

El EPMSC a cargo del director Adalberto Nieves

Resuelve

La regulación de políticas de seguridad y el uso adecuado de la información en el establecimiento penitenciario y carcelario de Aguachica-Cesar.

LA DIRECCION DEL EPMSC-AGUACHICA,

CONSIDERA

1. INTRODUCCION

Que el EPMSC-Aguachica, en atención a la privacidad y complejidad de la información que se administra en el establecimiento, se hace necesario implementar políticas y prácticas de seguridad para optimizar el uso de los recursos tecnológicos que soportan la gestión de la entidad, orientados a optimizar el uso de estos recursos por parte de los usuarios y responsables de los mismos.

Que la Constitución Política en su Artículo 61 establece que el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

2. PROPOSITOS

Que las políticas y prácticas de seguridad de la información establecidas, son de obligatorio cumplimiento para los funcionarios y contratistas del establecimiento, ante su infracción se aplicaran los procedimientos sancionatorios administrativos, disciplinarios y penales que correspondan.

Que las buenas prácticas de seguridad tienen como propósito orientar a los usuarios frente a las responsabilidades que deben asumir en la seguridad, confidencialidad y salvaguarda de la información y recursos tecnológicos que se encuentren a su cargo.

RESUELVE

CAPITULO I

3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

El comité de seguridad de la información del EPMSC (establecimiento penitenciario de mediana seguridad carcelaria) de Aguachica, está integrado por:

- Un coordinador de seguridad de la información a nivel de establecimiento, el cual deberá acreditar estudios y/o experiencias de seguridad o en auditoria de sistemas, quien parametrizara directivas, instructivos, memorandos y comunicaciones en general referentes al establecimiento.
- El director del departamento de sistemas.
- Jefe de la oficina de talento humano o un delegado especializado.
- Jefe de la oficina de control interno o un delegado especializado.
- Jefe de la oficina de almacén general o un delegado especializado.

Los integrantes del comité velaran por el cumplimiento de los siguientes objetivos de seguridad:

1) Revisar y proponer al director del establecimiento, para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad que fueren convenientes y apropiadas.
2) Monitorear cambios significativos en los riesgos que afectan los recursos de la información frente a posibles amenazas sean internas o externas.
3) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios del EPMSC, sean pres existentes o nuevos.
4) Promover la difusión y cumplimiento de las políticas de seguridad establecidas.
5) Aprobar y revisar semestralmente el plan de continuidad.
6) Aprobar el plan anual de auditorías a realizar.

4. GESTION DE ACTIVOS

A partir de la dirección del EPMSC-Aguachica, las áreas del establecimiento, bajo la supervisión del comité de seguridad de la información, deben elaborar y mantener un inventario de los activos de la información que poseen, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen. La dependencia almacén general tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

CAPITULO II

5. ENUNCIADOS DE LA POLITICA

5.1. DOCUMENTO DE POLITICAS DE SEGURIDAD

El comité de seguridad de la información del Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica deberá diseñar un documento de politicas de la seguridad de la informacion el cual debe ser aprobado y publicado por la direccion del establecimiento a cada uno de los empleados y agentes externos relevantes del establecimiento.

5.2. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Los integrantes del establecimiento deben conocer la importancia del correcto uso de las herramientas tecnológicas y sus activos, como bases de datos, equipos de cómputo, comunicaciones, software, documentos reservados y clasificados, entre otros.

Ante los avances tecnológicos, se facilita el hurto de los datos protegidos, en dispositivos móviles fáciles de transportar u ocultar, lo que incrementa el riesgo de vulnerabilidad de la información, en consecuencia, la política de seguridad de la información establece una serie de medidas buenas prácticas para el control al acceso de la información, la administración y control de usuario, supervisión al uso y transmisión de la información

CONTROLES:

❖ El comité de seguridad desarrollara planes de capacitación de seguridad de la información, los cuales se realizaran periódicamente, mínimo semestralmente, la cual será direccionada a las regionales y establecimientos penitenciarios y carcelarios de orden nacional.
❖ El coordinador de seguridad realizara seguimiento a los miembros del establecimiento que se han retirado del mismo y eliminara el usuario correspondiente a dicho empleado.
❖ Los funcionarios y contratistas son responsables de la información entregada para el ejercicio de su función y deberá cumplir con los lineamientos dados por al Entidad, con el propósito de proteger y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
❖ Los funcionarios públicos y contratistas no deben suministrar información de la entidad a entes externos sin autorización.
❖ Los funcionarios de la entidad que utilicen recursos informáticos, tiene la responsabilidad de asegurad la integridad, confidencialidad, disponibilidad y confiabilidad de la información que administra, en especial si está protegida por reserva legal o ha sido clasificada como confidencial y/o critica.
❖ Todo funcionario de la institución debe abstenerse de ejecutar acciones tendientes a eludir o violar Las Políticas de Seguridad de la Información.

5.2 SEGUIRIDAD FISICA Y AMBIENTAL

La parte ambiental es de una importancia significativa en el establecimiento, por eso se pretende velar por la seguridad de la misma para la protección del ambiente que nos rodea. En base a lo anterior se crearan una serie de propuestas para impedir accesos no autorizados y evitar daños e interferencias a las sedes e información EPMSC -Aguachica.

CONTROLES

❖ Cada uno de los funcionarios debe velar que la información que esta consignada en documentos físicos debe ser protegidas en lugares que dificulten el acceso a personal no autorizado.
❖ La función de escritura en las unidades de DVD/CD, será deshabilitada, salvo autorización del Comité de Seguridad.
❖ Todos los funcionarios del establecimiento deben abstenerse de retirar equipos de computo que contienen información del mismo, sin autorización y conocimiento del comité de seguridad, a fin de verificar la actividad que se realizara y el tipo de información que contiene.
❖ Las impresoras adquiridas en el establecimiento deben ser aptas para trabajar e red (conectadas a un punto de red y no a un computador), su uso debe realizarse por minimo 5 personas por dependencia. Las impresoras de inyección de tinta (Color) son de uso restringido, con el fin de minimizar costos.
❖ El comité de seguridad se encargara de mantener seguros los servidores y estaciones de trabajo que contengan la información institucional mediante:

- Controles de acceso y seguridad física.
- Sistema de vigilancia (Cámaras, alarmas).
- Sistema de detección de incendios.
- Control de humedad temperatura.
- Bajo riesgo de inundación.
- Instalación de fuentes de potencia ininterrumpida (UPS)

❖ Ningún funcionario podrá destapar equipos o impresoras para realizar cualquier clase de mantenimiento o instalación de hardware o software, sin una previa autorización por parte del comité de seguridad.
❖ Todos los funcionarios del instituto, deben abstenerse de hacer uso de dispositivos de almacenamiento con puertos USB, tarjetas de memoria (SD, MMC, Micro SD, Mini SD Memory Stick, Compact flash1, Micro drive, entre otros) que se encuentran ubicados en los computadores o que pueden ser adaptados a los mismos.
❖ Ningún funcionario debe descuidar documentos que contengan información, ya que esto ocasionara la consulta, copia o pérdida de la información por parte de personas no autorizadas.
❖ El Comité de Seguridad garantizara que se disponga de pólizas de protección de equipos actualizados.

- ❖ Todos los funcionarios del establecimiento deben abstenerse de dejar portátiles, computadores de escritorio encendidos en horas no laborales, elevando con esto los niveles de riesgo frente a una posible pérdida o difusión no autorizada de la información.
- ❖ Es obligación de cada uno de los funcionarios destruir o desechar correctamente la documentación, evitando la posible reconstrucción de la misma.
- ❖ Los funcionarios deben tener especial cuidado con la seguridad de los inmuebles en cada uno de los puestos de trabajo, dejándolos bajo llave cuando se ausente de su puesto de trabajo.
- ❖ Los puertos USB, serán de uso restringido en los equipos de computo, su habilitación debe solicitarla el jefe de dependencia ante el Comité de Seguridad.
- ❖ El comité de seguridad, establecerá un plan de mantenimiento preventivo para los equipos y velara por el cumplimiento del mismo.
- ❖ Cada uno de los funcionarios debe velar que los documentos impresos que contengan información, deben ser guardados de forma segura, no deben ser abandonados en lugares públicos o de fácil acceso a personas ajenas a dicha información.

5.3 GESTION DE COMUNICACIONES Y OPERACIONES

Diseñados para garantizar la seguridad y el respaldo de la información.

CONTROLES

❖ El Coordinador de Seguridad Informática o su delegado, instalará antivirus en los servidores y estaciones de trabajo y configurados para actualizaciones diarias.
❖ Todo funcionario del establecimiento debe evitar el envío y transporte de información mediante equipos electrónicos y tecnológicos que a través de sistemas de interconexión inalámbrica permitan la transmisión y almacenamiento de datos, tales como agendas digitales, iPod, iPad, BlackBerry, PDA's, PALMS, equipos electrónicos que contengan sistemas infrarrojos, wireless o bluetooth y celulares inteligentes, entre otros.
❖ No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la ley 23 de 1982 y su modificación, la ley 44 de 1993 y la Decisión 351 de 1993.
❖ El Coordinador de Seguridad Informática monitoreará permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red.
❖ Todo funcionario debe abstenerse de hacer uso inadecuado de la red de datos (WANG y LAN) del establecimiento, para obtener, almacenar y difundir en los equipos de computo, material pornográfico, mp3, videos y películas comerciales, cadenas de correos no autorizados.
❖ Las instalaciones de software deben ser aprobadas por el Coordinador de Seguridad Informática y en el caso de encontrarse software ilegal en alguna dependencia, será reportado como incidente de seguridad y posteriormente investigado.
❖ Todo funcionario de la institución debe abstenerse de realizar actividades que puedan alterar el desempeño de los sistemas de información y por ende generar posibles pérdidas o daños de la misma, como la instalación de software no licenciado, esta conducta igualmente

genera riesgos, como el ingreso de virus, instalación de software espía, hurto o divulgación no autorizada de la información.

❖ El departamento de Sistemas contará con mínimo un cortafuegos (Firewall) que prevenga el acceso de intrusos al sistema.

❖ El Comité de Seguridad garantizará la seguridad de los servicios prestados de comercio electrónico y de las transacciones en línea.

❖ Todos los funcionarios de la institución deben realizar copias de seguridad de los datos del computador asignado, en forma mensual o en intervalos de tiempo acordes con la necesidad del usuario y de criticidad de la información.

❖ La administración de cambios (Creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, deberá ser solicitado mediante comunicación escrita o correo electrónico al Comité de Seguridad, por el usuario de la información y aprobado formalmente por el jefe inmediato.

❖ En lugares definidos como críticos por la información que se administra, el comité de seguridad debe restringir el ingreso de equipos de tecnología celular que cuenten con sistema de grabación y almacenamiento de datos o imágenes.

❖ El Coordinador de Seguridad Informática o su delegado, elaborará copias de seguridad semanales y las guardará en sitios bajo llave. Es recomendable que las copias de seguridad se almacenen también en un lugar externo al establecimiento para prevenir pérdida de datos en el caso de una destrucción del establecimiento.

❖ Todo funcionario del establecimiento debe abstenerse de efectuar la conexión de equipos de computo personales, a la red de datos del establecimiento.

❖ El Coordinador de Seguridad Informática revisará semanalmente las copias de seguridad y llevará un registro de dicho procedimiento.

❖ En las oficinas donde se encuentren dispositivos de red como switch, tomas reguladas, canaletas, puntos de red y otros, los funcionarios deben tener cuidado de no desconcertarlos, apagarlos, no colocar objetos pesados sobre las canaletas, se deben proteger de caída de fluidos, evitar como equipos como grabadoras, cargadores y otros.

❖ El Coordinador de Seguridad Informática documentará la configuración de los enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red.

❖ Todo equipo de TI debe ser revisado, registrado y aprobado por el Coordinador del Comité de Seguridad antes de conectarse a cualquier nodo de la red de comunicaciones, así mismo, desconectará aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

❖ Cuando el funcionario deje el sitio de trabajo, debe cerrar las aplicaciones que se están ejecutando.

5.4 CONTROL DE ACCESOS

El control para el acceso a la información del establecimiento estará dado bajo una serie de directrices que aseguran que la misma no corra ningún riesgo de pérdida.

CONTROLES

❖ El Departamento de sistemas elaborará, mantendrá y publicará los procedimientos de administración de cuentas de usuario para el uso de equipos de cómputo.
❖ A los funcionarios y contratistas que laboren en el establecimiento y que se les asigne un equipo de computo, el director del departamento de sistemas les asignara una cuenta con clave de acceso, la cual tiene definido el perfil de usuario para adicionar, modificar, borrar y consultar información.
❖ El Coordinador de Seguridad Informática o su delegado, configurará alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataque e intentos de intrusión.
❖ Cuando un funcionario se traslade o se retire del establecimiento, el jefe de dependencia debe informar al jefe de talento humano y este a su vez al departamento de sistemas, con por lo menos un día de antelación, para realizar el correspondiente backup y cambios o eliminación de usuarios.
❖ Las contraseña es personal, por lo tanto no debe ser compartida ni revelada, además deben serán cambiadas periódicamente (Mínimo cada dos meses) y suministradas al Jefe inmediato, cada vez que se haga el cambio.
❖ El uso del correo electrónico e Internet se prohíbe para fines que no sean institucionales dentro y hacia fuera de la institución.
❖ Cada funcionario debe establecer una contraseña distinta para los servicios utilizados (SISIPEC, correo, inicio se sesión, etc.)
❖ No está permitido el uso de seudónimos y envío de mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales, además que atenten contra la dignidad humana y las garantías fundamentales.
❖ Todo funcionario debe abstenerse del envío y recepción de datos del instituto a través de correos electrónicos personales, los cuales no poseen las características de seguridad requeridas.
❖ Las contraseñas deben tener mínimo seis caracteres, y deben ser de orden alfanumérico.
❖ Cada funcionario de la institución debe hacer un uso adecuado del correo, descargar los correos continuamente, archivar o eliminar los correos de las carpetas ya leídos y enviados, descargar la carpeta de mensajes eliminados mínimo de forma semanal.
❖ Los correos masivos institucionales que por necesidades específicas de un área requieran ser enviados a toda la institución, deben ser solicitados a través del departamento de Sistemas y autorizados por el mismo.
❖ La cuenta de correo no debe ser utilizada para enviar o reenviar correos como presentaciones, bromas, video clips, cadenas, pornografía, entre otros. Cuando sean recibidos este tipo de mensajes deberán eliminarse inmediatamente, para evitar la contaminación con posibles virus.
❖ Está prohibido a todos los funcionarios del establecimiento, usar como contraseña el nombre, apellido, numero de documento, nombre de los hijos o fechas que se relacionen con el usuario, ni ninguna palabra que aparezca en un diccionario de cualquier idioma.
❖ Ningún funcionario debe abrir archivos o ejecutar programas adjuntos a los correos si no se conoce el remitente o el asunto.

❖ El director del departamento de sistema se encargara de bloquear la recepción de archivos de audio y video, para evitar congestionar el servidor de correo, o el canal dedicado.

5.5 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La seguridad de la información depende en gran parte de los controles de seguridad inmersos en las aplicaciones que se manejan.

CONTROLES:

❖ Las aplicaciones contarán con el Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al Coordinador de Seguridad Informática, la revisión de incidentes en el manejo de las aplicaciones.
❖ El Coordinador de Seguridad Informática o su delegado actualizará diariamente el software del servidor Web con los parches publicados por el fabricante.
❖ Se debe llevar una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó.

5.6 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Una adecuada gestión de incidentes le permitirá al establecimiento responder a los incidentes de manera sistemática, eficiente y rápida; volver a la normalidad en poco tiempo, perder muy poca información; realizar continuamente mejoras en la gestión y tratamiento de incidentes; generar una base de conocimientos sobre incidentes; evitar en lo posible, incidentes repetitivos.

CONTROLES:

❖ El Coordinador de Seguridad Informática ante una incidencia, debe comunicarlo al Comité de Seguridad de la Información y diligenciará el correspondiente formato donde quede consignados los datos de reporte del incidente y de la persona que reportó:

REPORTE DE INCIDENTES		
No.	**HORA**	**FECHA**

DESCRIPCION DEL INCIDENTE	
EFECTOS PRODUCIDOS	
RESPONSABLE DEL ACTIVO AFECTADO	
CAUSAS DEL INCIDENTE (Se diligencia una vez se recupere la normalidad del proceso afectado)	
DATOS DEL REPORTANTE	
NOMBRE	**CARGO**
ESTABLECIMIENTO	**CORREO**

- Una vez verificada la incidencia, el Coordinador de Seguridad de la Información recolectará la información que le permitirá determinar el alcance del incidente, qué redes y que sistemas y aplicaciones fueron afectados, y que fue lo que generó el incidente, como ocurrió o está ocurriendo, también nos permite saber que originó el hecho, cómo ocurrió y las herramientas utilizadas, qué vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la empresa.

  Para determinar el alcance, el Coordinador de Seguridad de la Información puede hacerse las siguientes preguntas:

  - ¿Cuántos equipos fueron comprometidos?
  - ¿Cuántas redes se vieron envueltas?
  - ¿Hasta qué punto de la red logró penetrar el atacante?
  - ¿Qué nivel de privilegio logró el atacante?

- ¿Qué es lo que está en riesgo?
- ¿Cómo impacta en las actividades de la universidad el compromiso de los equipos?
- ¿Se encuentran en riesgo aplicaciones críticas?
- ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
- ¿Hay otros equipos con la misma vulnerabilidad?

❖ Determinado el alcance del incidente de seguridad, el Coordinador de Seguridad de la Información procederá a la contención, respuesta y puesta en marcha de las operaciones afectadas por el incidente.

La contención, evitará que el incidente siga produciendo daños. La erradicación eliminará la causa del incidente y todo rastro de los daños y la recuperación, consiste en volver el entorno afectado a su estado original.

Para llevar a cabo estas acciones, se tendrán que contar con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva.

Para contar con una buena estrategia tengamos en cuenta estos agentes:

- Daño potencial de recursos a causa del incidente
- Necesidad de preservación de evidencia
- Tiempo y recursos necesarios para poner en práctica la estrategia
- Efectividad de la estrategia total o parcialmente
- Duración de las medidas a tomar
- Criticidad de los sistemas afectados
- Características de los posibles atacantes
- Si el incidente es de conocimiento público
- Pérdida económica
- Posibles implicancias legales
- Relación costo-beneficio de la estrategia
- Experiencias anteriores

La recolección de información cuando se investigan las causas debe respetar los siguientes puntos:

1) **AUTENTICIDAD**: Quien haya recolectado la evidencia debe poder probar que es auténtica.
2) **CADENA DE CUSTODIA:** Registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
3) **VALIDACION**: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

CAPITULO III

6. GLOSARIO

AMENAZA: Evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

BITÁCORA: Libro donde se registran las observaciones de un evento

CA NALETAS: Una canaleta es un canal que contiene cables en una instalación. Las canaletas incluyen conductos comunes de electricidad, bandejas de cables especializadas o bastidores de escalera, sistemas de conductos incorporados en el piso, y canaletas de plástico o metal para montar sobre superficies.

CÓDIGO FUENTE: Conjunto de instrucciones para ejecutar un programa de computadora.

CONTRASEÑA: Conjunto de caracteres que permite el ingreso a un recurso informático.

CORTAFUEGOS: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

CRIPTOGRAFÍA: Ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar ("encriptar") la información y hacerla irreconocible a los usuarios no autorizados de un sistema informático, de modo que sólo los legítimos propietarios puedan recuperar ("desencriptar") la información original

INCIDENTE DE SEGURIDAD: Es cualquier evento que pueda o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

LOG DE AUDITORÍA: Término usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para una aplicación.

IMPACTO: Daño potencial sobre un sistema cuando una amenaza se presenta.

PLAN DE CONTINUIDAD DEL NEGOCIO: Estrategia planificada constituida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de

negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

PMI: Project Management Institute.

RIESGO: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

SERVIDOR: Computadora que ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes.

SWITCH: dispositivo inteligente utilizado en redes de área local

SISTEMA DE INFORMACIÓN: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

SISIPEC: Sistematización Integral del Sistema Penitenciario

TI: Tecnología de la Información y Comunicaciones.

UPS: Uninterrumpible Power Supply
VULNERABILIDAD: Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas para la organización.

WAN: es una red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel planetario.

7. HISTÓRICO DE REVISIONES, ACTUALIZACIONES Y APROBACIONES

Cada año la Política de Seguridad debe ser revisada y retroalimentada en los aspectos que sean necesarios mínimo cada año, y los cambios serán documentados en un Registro de Cambios de la Política de Seguridad Informática, se harán las modificaciones respectivas en el documento y posteriormente, se promulgará mediante Resolución.

El Comité de Seguridad de la Información divulgará la Política de Seguridad Informática a todos los funcionarios del Instituto Nacional Penitenciario y Carcelario INPEC.

REGISTRO DE CAMBIOS DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA					
AÑO	**ASPECTO A MODIFICAR**	**CONTROL ACTUAL**	**CONTROL MODIFICADO**	**PERSONA QUE RELAIZA LA MODIFICACION**	**CARGO**

6. CONCLUSIONES

El proceso de auditoría que se hizo en el establecimiento penitenciario de mediana seguridad carcelaria de Aguachica, permitió la identificación de falencias en cuanto al diseño y uso de los sistemas y procedimientos internos del establecimiento, tales como carencia de personal administrativo, inconsistencias en los expedientes de la población reclusa, falta de capacitación, desactualización de software antivirus, contraseñas de fácil reconocimiento, entr4e otros; debido a esto se propuso la creación de una guía de políticas de seguridad de la información para el establecimiento, todo esto con el ánimo de contribuir al mejoramiento de los procesos que se manejan en dicho lugar.

La creación de la guía de políticas de seguridad de la información se basó en el estándar ISO/IEC 27002, tomando los dominios pertinentes (9 dominios) que aplicaran para generar controles para el mejoramiento del manejo de la información.

Sabiendo que la información es el bien más preciado que una empresa puede tener, se debe tratar de reducir o mitigar los riesgos que puedan ocurrir en el manejo de los diferentes procesos que se manejen, es por esto que el establecimiento penitenciario de mínima seguridad carcelaria no es ajeno a estos posibles ataque informáticos que puedan poner en riesgo la información, y con la creación de las políticas de seguridad y su posterior aplicabilidad se reduce o mitiga el riesgo.

7. RECOMENDACIONES

Se recomienda la socialización de la guía de políticas de seguridad a cada uno de los empleados del establecimiento, para que sea conocida y aplicada en cada uno de los procesos que se manejan.
Con el mejoramiento de los procesos también se debe ir mejorando o complementando a guía de políticas de seguridad para que en un futuro no se encuentre obsoleta respecto a la forma de manejar la información en el establecimiento.

Tener claro que la información es el tesoro que se debe tener mejor guardado, y no ponerlo en riesgo aplicando las políticas existentes.

BIBLIOGRAFIA

Calvo Orra, A. (2006). ISO 27001. Dintel, 150-153.
Carranza, E. (1999). Justicia penal y sobrepoblación penitenciaria. Respuestas posibles. Costa Rica: Siglo Veintiuno Editores.

CIBERTEC. (2007). CIBERTEC. Recuperado el 29 de Julio de 2013, de http://www.cibertec.edu.pe/2/modulos/JER/JER_Interna.aspx?ARE=2&PFL=2&JER=3749#Top

Diaz Ceballos, A. M. (2007). La percepción del riesgo sobre los niveles de aceptabilidad del mismo. Gerencia de Riesgos y Seguros de la Fundación MAPFRE ESTUDIOS.

EcuRed. (13 de Diciembre de 2010). EcuRed, Conocimiento con Todos y para Todos. Recuperado el 29 de Julio de 2013, de http://www.ecured.cu/index.php?title=ISO/IEC_27002&action=history

GOBIERNO DE ARAGON. (2007). Plataforma E-ducativa Aragonesa. Recuperado el 29 de Julio de 2013, de http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio//1000/1063/html/11_seguridad_fsica_y_seguridad_lgica.html

Gonzalez R., M., & Becerra G., J. (2011). Ingenieria de Sistemas. Tachira: Ministerio del Poder Popular para la Educaicion Superior.

INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO. (2010). INPEC. Recuperado el 29 de Julio de 2013, de http://www.inpec.gov.co/portal/page/portal/Inpec

ISACA. (2007). COBIT 4.1 -IT governance framework. IT Governance Institute.

ISO/IEC. (15 de 10 de 2005). Estandar Internacional ISO/IEC 27001.

Montes, A. (2010). ColombiaLink. Recuperado el 30 de Julio de 2013, de http://www.colombialink.com/01_INDEX/index_historia/07_otros_hechos_historicos/0320_llegaron_computadores.html

Noel Rodriguez, M. (2011). PANORAMA DE LOS SISTEMAS PENITENCIARIOS EN AMERICA LATINA Y EL CARIBE. Obtenido de http://www.iidh.ed.cr/comunidades/seguridad/docs/seg_docpolicia/curso%20noel%20doct.htm#_msoanchor_1

Organización Internacional de Normalización. (1988). Sistemas de Procesamiento de la Información - OSI RM. . Informe Técnico 97 7498-2, ISO / TC, 1988. .

RAE. (2009). Real Academia Española. Recuperado el 29 de Julio de 2013, de http://lema.rae.es/drae/?val=guia

Sead, M., Ahmed, P., Peter, S., Rafael, C., Jan, H., & Unto, P. (1993). Seguridad en sistemas abiertos. John Wiley and Sons.

Susanto, H., Nabil Almunawar, M., & Chee Tuan, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences, 23-29.

Tamayo y Tamayo, M. (2003). El Proceso de la Investigacion Cientifica. Limusa S.A.

Vega Briceño, E. A. (Junio de 2005). GestioPolis. Recuperado el 29 de Julio de 2013, de http://www.gestiopolis.com/Canales4/mkt/simparalas.htm

Zorrilla A., S., Torres X., M., Cervo Amado, L., & Bervian, P. a. (1997). Metodologia de la Investigacion. Mc Graw- Hill.

ANEXOS

Anexo A. Lista de Chequeo, Seguridad Lógica aplicada en el Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica, Cesar.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS

INSTITUTO NACIONAL PENITENCIARIO Y CARCELAR
ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA- CESAR.

CHECK LIST DE RANGO SEGURIDAD LOGICA

EMPRESA: ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUCHICA CESAR.
AREA:

PREGUNTAS	E	S	A	I	D
¿Existe algun tipo de control para acceder a los equipos o a los programas?					
¿Las personas que laboran en esta dependecnia so concientes de ka importancia de proteger la infromacion que manejan?					
¿Las claves de acceso son unicas para cada usuario y para cada aplicacion?					
¿Si un empleado se retira temporal o definitivamente de sus labores, que hace el establecimiento con la informacion que ese empleado poseia?					
¿Se cuenta con una copia de las claves de acceso de los usuarios en un lugar seguro?					
¿Existe un acuerdo de confidencialidad entre el establecimiento y los empleados para la portecion de la informacion que ha sido encomendada?					
En caso de incumplimiento de dicho acuerdo ¿Que acciones emprende el establecimiento contra quien lo comete?					
¿Cuando se presenta rotacion de personal, se inhabilitan las claves de acceso de los usuarios que ya no utilizan el sistema?					
¿Se limita el uso del equipo a los usuarios autorizados unicamente?					
¿Se capacitan periodicamente a los usuarios en el adecuado manejo de los equipos y de los aplicativos?					
¿Es suficiente el plan de capacitacion establecido para los usuarios?					
¿Se limita el acceso a los programas y archivos mediante el uso de conteseñas o algun otro mecanismo para el ingreso a aplicaciones o programas?					
¿Se realizan copias de seguridad de la informacion que se genera al interior del establecimiento?					
¿Donde se almacenan estas copiaa de respaldo (caja fuerte, mueble con cerradura, otros)?					
¿Que medios utiliza para realizar las copias de seguridad de la informacion (CD, DVD, Memorias USB, Discos duros)?					
¿El establecimiento cuenta con programas utilitarios que permitan la recuperacion de archivos en caso de fallas de los equipos?					
¿En los equipos del establecimiento hay software para la detecciin de intrusos?					

¿Los equipos tienen isntalado software antivirus?					
¿Las bases de datos de estos antivirus se encuetran actualizadas?					

E: Excelete
S: Sobresaliente
A: Aceptable
I: Insuficiente
D: Deficiente

Anexo B. Lista de Chequeo, Seguridad Fisica aplicada en el Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica, Cesar.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS

INSTITUTO NACIONAL PENITENCIARIO Y CARCELAR
ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA- CESAR.

CHECK LIST DE RANGO SEGURIDAD FISICA

EMPRESA: ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUCHICA CESAR.
AREA:

PREGUNTAS	E	S	A	I	D
¿Que mecanismos utiliza el establecimiento para la proteccion fisica de los equipos de computo?					
¿En el establecimiento se realizar mantenimientos preventivos y correctivos a los equipos de computo?					
¿Con que frecuencia?					
¿El responsable del mantenimiento preventivo entrega reportes de las tareas ejecutadas?					
¿Existe un plan de mantenimiento preventivo de equipos contemplado dentro de las politicas del establecimiento?					
En caso de perdida del fluido electrico ¿Que mecanismos utiliza el establecimiento, para darle continuidad a sus actividades, especialmente aquellas que son soportadas por los sistemas informaticos?					
¿Existen prohibiciones formales para el consumo de alimentos o bebidas cerca de los equipos de computo al igual que las prohibiciones para fumar?					
¿Existe conexion de polo a tierra para las inatalaciones de los equipos de computo?					
¿En caso de presentarse un incendio, el establecimiento cuenta con algun mecanismo de alerta?					
¿El cableado de datos esta independiente de las conexiones electricas?					
¿Es establecimiento cuenta con un lugar escpecifico para el almacenamiento de las copias de seguridad de la informaicon?					
¿El establecimiento posee planos de la red de datos?					
¿Existe inventarion fisici de los equipos de computo y dispositivos de comunicacion que conforman la red de datos del establecimiento?					
¿El establecimiento posee un plan de contingenca que permita el normal desempeño de las actividades, aun cuando se presente algun inconveniente? -Inundaciones -Terremotos					

-Corte del fluido electrico -Daño a los equipos -Tormentas electricas					

E: Excelete
S: Sobresaliente
A: Aceptable
I: Insuficiente
D: Deficiente

Anexo C. Entrevista a Funcionario, Director del Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica, Cesar.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS

INSTITUTO NACIONAL PENITENCIARIO Y CARCELAR
ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA- CESAR.

ENTREVISTA PARA FUNCIONARIOS (Diferentes del Director)

EMPRESA: ESTABLECIMIENTO PENITENCIARIO YCARCELARIO DE AGUACHICA-CESAR.
OBJETIVO: Obtener una visión general del Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica- Cesar.
FECHA ENREVISTA: _____
ENTREVISTADO: _____
ROL ENTREVISTADO: Director del Establecimiento (e)

PREGUNTAS	SI	NO	NO SE	OBSERVACIONES
1. ¿El personal del establecimiento conoce cada una de sus responsabilidades y las sanciones que existen, con respecto a la seguridad de la información?				
2. ¿El personal adscrito al establecimiento firman acuerdos de confidencialidad?				
3. ¿Las diferentes áreas del establecimiento están debidamente identificadas?				
4. ¿Las diferentes áreas del establecimiento cuentan con controles de ingreso de personal?				
5. ¿El establecimiento cuenta con registros de los accesos, uso de aplicativos y servicios de red?				

6. ¿El establecimiento cuenta con controles criptográficos? (Certificados digitales o programas para la encriptación)				
7. ¿El establecimiento tiene determinados lineamientos para el control de acceso a sus aplicaciones?				
8. ¿Son aplicados los lineamientos de control de acceso?				
9. ¿Se cuenta con un listado actualizado de los accesos otorgados a los sistemas de información?				
10. ¿Las aplicaciones que se utilizan al interior del establecimiento cuentan con contraseña para permitir el acceso a los usuarios?				
11. En caso de un incidente ¿Se cuenta con un plan de respuesta?				
12. ¿Después de un incidente se realizan investigaciones?				

Anexo D. Entrevista a Funcionarios diferentes al Director

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS

INSTITUTO NACIONAL PENITENCIARIO Y CARCELAR
ESTABLECIMIENTO PENITENCIARIO Y CARCELARIO DE AGUACHICA- CESAR.

ENTREVISTA PARA FUNCIONARIOS (Diferentes del Director)

EMPRESA: ESTABLECIMIENTO PENITENCIARIO YCARCELARIO DE AGUACHICA-CESAR.
OBJETIVO: Obtener una visión general del Establecimiento Penitenciario y Carcelario de la Ciudad de Aguachica- Cesar.
FECHA ENREVISTA: _____
ENTREVISTADO: _____
ROL ENTREVISTADO:_____

PREGUNTAS	SI	NO	NO SE	OBSERVACIONES
1. ¿Accede usted a los equipos de cómputo del establecimiento, para desempeñar sus funciones?				
2. ¿Usa usted algún mecanismo para la seguridad de su información digital?				
3. ¿Usa usted algún mecanismo para la seguridad de su información física?				
4. ¿Respalda usted la información que maneja dentro de sus funciones?				
5. ¿Cuenta usted con controles contra software malicioso en su puesto de trabajo? (Antivirus, antispyware, entre otros)				

6.	¿Las aplicaciones a las que usted accede, cuentan con contraseña para permitir acceso a los usuarios?				
7.	¿Cuenta con controles de cambios para las aplicaciones, software y sistemas operativos, en su puesto de trabajo?				
8.	¿Conoce usted si existen lineamientos para el control de la seguridad de la información en el establecimiento?				
9.	¿Conoce usted si existe una guía formal de políticas de la información? (Si la respuesta es afirmativa responder, la pregunta 7, de lo contrario continuar con la pregunta 8)				
10.	¿La política de Seguridad de la información, se encuentra formalmente aprobada, establecida y publicada?				
11.	¿Sabe usted si existe un comité de seguridad de la información?				