AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES

JULIO CESAR BURGOS CHAGUEZAC
NELSON ANDRÉS CORTES BERNAL

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA: INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES

JULIO CESAR BURGOS CHAGUEZAC
NELSON ANDRÉS CORTES BERNAL

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARCIAL
PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS

ASESOR
Ingeniero: MANUEL BOLAÑOS GONZALES

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA: INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva del autor.

Artículo 1ro del Acuerdo No. 324 de octubre 11 de 1966 emanado del Honorable Consejo Directivo de la Universidad de Nariño.

Nota de aceptación

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

San Juan de Pasto, 6 de Marzo de 2013

DEDICATORIA

A Dios: Por estar en todo momento acompañándonos en cada tarea de nuestra vida diaria, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo.

A mis Padres: Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, por los ejemplos de perseverancia y constancia que los caracterizan y que me han infundado siempre. Por el valor mostrado para salir adelante, por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, y por su amor, para mirar que el sueño de cada Padre se ha hecho realidad.

A mi gran Amor; Por siempre estar a mi lado, brindándome todo su amor, entrega, dedicación, por brindarme su inmenso amor, conocimiento y sobre todo tenerme mucha comprensión y paciencia durante este tiempo de mi vida y quien ha sido una pieza clave en mi desarrollo profesional. Mil gracias porque siempre estas a mi lado sin condiciones.

A mis familiares: A mis hermanos y hermanas por sus alegrías brindadas en momentos difíciles; a mis tíos y tías; a mi abuela quien aporto con su grano de arena para llegar a este punto; a todos aquellos que participaron directa o indirectamente en la elaboración de esta tesis.

A mis amigos: Al apoyo incondicional y la lucha del día a día de quien siempre me acompañado en las buenas y las malas.

Como dijo Thomas Chalmers: “La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar”.

Julio Cesar Burgos

DEDICATORIA

A Dios: Quién supo guiarme por el buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mis Padres: Por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles ya que me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mi amada compañera de vida, por acompañarme en este proceso, por tu amor, tu comprensión, paciencia y fortaleza que permitieron que pudiese, no sólo trabajar, sino también llegar a buen puerto.

A mis hermanos por estar siempre presentes, acompañándome para poderme realizar.

A mi hija quien me prestó el tiempo que le pertenecía, porque ella tuvo que soportar largas horas sin la compañía de su papá, sin poder entender, a su corta edad, el porqué prefería estar frente a la pantalla del ordenador y no acostado y/o jugando con ella. A pesar de ello, cada vez que podíamos, al reunirnos, aprovechamos hermosos momentos, en los que su sola sonrisa me llenaba de ánimo y fuerzas, quien me motivó siempre con sus notitas, "No te rindas" y "Sé fuerte".

Nelson Andrés Cortes

AGRADECIMIENTOS

Expreso de manera especial mi gratitud y agradecimientos a:

A La Universidad de Nariño, por permitirme formar profesionalmente.

Al asesor del proyecto, Manuel Bolaños, su constante motivación carismática, interés y paciencia en el asesoramiento y concreción de éste trabajo.

A los Docentes del pregrado, Ingenieros de Sistemas por su paciencia y entrega.

A todas y a cada una de las personas de la Institución prestadora de servicios de salud Indígena Guáitara, por su paciencia y su tiempo.

RESUMEN

DEBIDO AL AUGE Y A LAS LEYES ACTUALES PLANTEADAS POR EL GOBIERNO COLOMBIANO Y SU ENTE ENCARGADO LA CONTRALORÍA PARA IDENTIFICAR LAS VIOLACIONES DE LAS LEYES INFORMÁTICAS Y DE COMUNICACIONES POR PARTE DE LAS EMPRESAS, POR LO TANTO SE CONSIDERO DE VITAL IMPORTANCIA EJECUTAR UNA AUDITORIA QUE EVALUÉ EL SISTEMA DE INFORMACIÓN (SI) DONDE SE IDENTIFICARAN LAS VULNERABILIDADES DE SEGURIDAD FÍSICA Y LÓGICA.

PARA EJECUTAR EL PROCESO DE AUDITORIA SE TOMA COMO MARCO DE REFERENCIA EL MODELO “COBIT” (OBJETIVOS DE CONTROL PARA TECNOLOGÍAS DE LA INFORMACIÓN), SELECCIONANDO LOS PROCESOS DE CADA DOMINIO QUE FUERON APLICADOS SEGÚN LOS OBJETIVOS DE ESTE PROYECTO.

LA AUDITORIA DE SISTEMAS SE REALIZÓ A LA IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES, CON EL FIN DE DAR RECOMENDACIONES PARA FORTALECER Y MEJORAR LA SEGURIDAD FÍSICA Y LÓGICA, ANALIZAR LA INFORMACIÓN SUMINISTRADA POR LA INSTITUCIÓN AUDITADA Y LA RECOLECTADA POR EL EQUIPO AUDITOR.

ABSTRACT

DUE TO THE PEAK AND TO THE OUTLINED CURRENT LAWS FOR THE COLOMBIAN GOVERNMENT AND THEIR IN CHARGE ENTITY THE CONTROLLERSHIP TO IDENTIFY THE VIOLATIONS OF THE COMPUTER LAWS AND OF COMMUNICATIONS FOR PART OF THE COMPANIES, THEREFORE YOU CONSIDERS OF VITAL IMPORTANCE TO EXECUTE AN AUDIT THAT I EVALUATED THE SYSTEM OF INFORMATION (IF) WHERE THE VULNERABILITIES OF PHYSICAL SECURITY AND LOGIC WERE IDENTIFIED.

TO EXECUTE THE PROCESS OF AUDIT HE/SHE TAKES LIKE MARK OF IT INDEXES THE PATTERN “COBIT” (OBJECTIVES OF CONTROL FOR TECHNOLOGIES OF THE INFORMATION), SELECTING THE PROCESSES OF EACH DOMAIN THAT WERE APPLIED ACCORDING TO THE OBJECTIVES OF THIS PROJECT.

THE AUDIT OF SYSTEMS WAS CARRIED OUT TO THE INDIGENOUS IPS GUÁITARA OF THE MUNICIPALITY OF IPIALES, WITH THE END OF GIVING RECOMMENDATIONS TO STRENGTHEN AND TO IMPROVE THE PHYSICAL AND LOGICAL SECURITY, TO ANALYZE THE GIVEN INFORMATION FOR THE ENTITY AUDITADA AND THE ONE GATHERED FOR THE TEAM AUDITOR.

CONTENIDO

Pág.

INTRODUCCIÓN 22
1. MARCO TEÓRICO 28
1.1 ANTECEDENTES 28
1.2 ASPECTOS GENERALES SOBRE AUDITORIA 30
1.3 EL AUDITOR 31
1.4 TIPOS DE AUDITORÍA 32
1.4.1 Auditoría interna 32
1.4.2 Auditoría externa 33
1.4.3 Diferencias entre auditoría interna y externa. 35
1.4.4 Auditoria 36
1.4.5 Auditoría financiera. 36
1.4.6 Auditoria administrativa u operativa. 37
1.4.7 Auditoria integral 37
1.4.8 Auditoria de sistemas 38
1.5 AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO 39
1.5.1 Alcance de la auditoria de sistemas. 40
1.5.2 Objetivos de la auditoria de sistemas. 40
1.5.3 Pruebas y herramientas para efectuar una auditoría de sistemas. 41
1.5.4 Pasos a seguir para una auditoria de sistemas en una organización. 42
1.6 METODOLOGÍAS DE AUDITORIA DE SISTEMAS 46
1.6.1 cobit (control objectives for information and related technology). 47
1.6.2 Iso 27000: 68
1.6.3 Magerit 72
1.6.4 Coso (Sponsoring Organizations of the Treadway Commission) 74
2. DESARROLLO DE AUDITORIA 80

2.1 METODOLOGÍA 80
2.2 ARCHIVO PERMANENTE 81
2.2.1 Decreto comunes 81
2.2.2 Ambiente general de la institución. 82
2.2.3 Reseña histórica. 82
2.2.4 Misión 83
2.2.5 Visión 83
2.2.6 Organización administrativa 84
2.2.7 Manual de funciones 86
2.2.8 Inventario de equipos de cómputo. 98
2.2.9 Portafolio de Servicios 99
2.3 ARCHIVO CORRIENTE 100
2.3.1 Memorando de planeación auditoria 100
2.3.2 Programa de auditoría 106
2.3.3 Diseño de los elementos para la auditoria 117
2.3.4 Modelo de Madurez. S 128
2.3.5 Hallazgos aplicados en la auditoría de la Ips Indígena Guáitara 129
2.3.5 Informe ejecutivo de auditoría 226
2.3.6 Informe general de auditoría. 230
3. MANUAL DE USUARIO 247
4. CONCLUSIONES 250
5. RECOMENDACIONES 252
BIBLIOGRAFÍA 253

LISTA DE TABLAS

Pág.

TABLA 1. FORMATO CUADRO DE DEFINICIÓN FUENTES DE CONOCIMIENTO..... 120
TABLA 2. FORMATO CUESTIONARIO CUANTITATIVO..... 122
TABLA 3. FORMATO MATRIZ DE PROBABILIDAD E IMPACTO..... 124
TABLA 4. FORMATO DE ENTREVISTA..... 126
TABLA5. FORMATO DE ENTREVISTA 2..... 127
TABLA 6. HALLAZGO PLANEACION Y ORGANIZACIÓN PO2_3_1..... 130
TABLA 7. HALLAZGO PLANEACIÓN Y ORGANIZACIÓN PO2_3_3..... 132
TABLA 8. HALLAZGO PLANEACIÓN Y ORGANIZACIÓN PO2_3_3..... 134
TABLA 9. MATRIZ DE PROBABILIDAD E IMPACTO PO2..... 136
TABLA 10. HALLAZGO PLANEACIÓN Y ORGANIZACIÓN PO4_3_1..... 137
TABLA 11. HALLAZGO PLANEACIÓN Y ORGANIZACIÓN PO4_3_2..... 139
TABLA 12. HALLAZGO PLANEACIÓN Y ORGANIZACIÓN PO4_3_3..... 141
TABLA 14. HALLAZGO PLANEACIÓN Y ORGANIZACIÓN PO9_3_1..... 145
TABLA 15. MATRIZ DE PROBABILIDAD E IMPACTO PO9..... 147
TABLA 16. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_1..... 149
TABLA 17. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_2..... 151
TABLA 18. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_3..... 153
TABLA 19. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_4..... 155
TABLA 20. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_5..... 157
TABLA 21. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_6..... 159
TABLA 22. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI3_3_6..... 160
TABLA 23. MATRIZ DE PROBABILIDAD E IMPACTO AI3..... 161
TABLA 24. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI6_3_1..... 162
TABLA 25. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI6_3_2..... 164
TABLA 26. HALLAZGO ADQUISICIÓN E IMPLEMENTACIÓN AI6_3_3..... 166
TABLA 27. MATRIZ DE PROBABILIDAD E IMPACTO AI6..... 171

TABLA 28. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS5_3_1 173
TABLA 29. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS5_3_2 175
TABLA 29. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS5_3_3 177
TABLA 30. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS5_3_4 179
TABLA 31. MATRIZ DE PROBABILIDAD E IMPACTO DS5 181
TABLA 32. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS9_3_1 182
TABLA 33. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS9_3_2 184
TABLA 34. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS9_3_3 186
TABLA 40. MATRIZ DE PROBABILIDAD E IMPACTO DS9 188
TABLA 41. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS11_3_1 189
TABLA 42. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS11_3_2 191
TABLA 43. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS11 193
TABLA 44. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_1 194
TABLA 45. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_2 197
TABLA 46. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_3 200
TABLA 47. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_4 202
TABLA 48. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_5 204
TABLA 49. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_5 206
TABLA 50. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_6 207
TABLA 51. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_7 210
TABLA 52. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_8 210
TABLA 53. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12_3_9 214
TABLA 54. HALLAZGO ENTREGA DE SERVICIO Y SOPORTE DS12 220
TABLA 55. HALLAZGO MONITOREO ME2_1_1 222
TABLA 56. MATRIZ DE PROBABILIDAD E IMPACTO ME 224

LISTA DE FIGURAS

Pág.

FIGURA 1. LAS TRES DIMENSIONES CONCEPTUALES DE COBIT 67
FIGURA 2. LOGOTIPO DE LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA” 82
FIGURA 3. ORGANIGRAMA DE LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA GUÁITARA 84
FIGURA 4. ESTRUCTURA ORGÁNICA DE SISTEMA DE INFORMACIÓN DE LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA GUÁITARA. 85
FIGURA 5. INVENTARIO DE EQUIPOS DE CÓMPUTO. 98
FIGURA 6. PORTAFOLIO DE SERVICIOS 99
FIGURA 7. MODELO DE MADUREZ 128
FIGURA 8. GRAFICA MODELO DE MADUREZ 129
FIGURA 9. PERSONAL DE TI (IMG01_P04_3_3) 143
FIGURA 10. CÁMARAS DE VIGILANCIA (IMG01_DS12_3_1) 196
FIGURA 11. REGISTRO DE VIGILANCIA (IMG02_DS12_3_1) 196
FIGURA 12. PERSONAL NO AUTORIZADO (IMG01_DS12_3_3) 202
FIGURA 13. AVISOS DE EVACUACIÓN (IMG01_DS12_3_5) 207
FIGURA 14. SENSORES DE HUMO Y CÁMARA (IMG01_DS12_3_6) 209
FIGURA 15. UPS (IMG01_DS12_3_8) 213
FIGURA 16. SWITCH (IMG01_DS12_3_9) 217
FIGURA 17. DISTRIBUCIÓN DE INSTALACIONES (IMG02_DS12_3_9) 217
FIGURA 18. CONEXIONES (IMG03_DS12_3_9) 218
FIGURA 19. CONEXIONES (IMG04_DS12_3_9) 218
FIGURA 20. CABLEADO UTP (IMG05_DS12_3_9) 219
FIGURA 21. CANALETAS (IMG06_DS12_3_9) 219
FIGURA 22. LISTADO DE CARPETAS (PRUEBAS) 248

GLOSARIO

Acción correctiva: Es aquella que llevamos a cabo para eliminar la causa de un problema.

Acción preventiva: Se anticipan a la causa, y pretenden eliminarla antes de su existencia. Evitan los problemas identificando los riesgos. Cualquier acción que disminuya un riesgo es una acción preventiva.

Activo: Se entiende cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

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

Análisis de riesgo: Según [ISO/IEC 13335-1:2004]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Aplicativo: Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

Archivo de datos: Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado Documento.

Archivo de programa: Archivo ejecutable que inicia una aplicación o programa. Los archivos de programa tienen las extensiones EXE, PIF, COM o BAT.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Autenticación: Proceso que tiene por objeto asegurar la identificación de una persona o sistema.

Bases de Datos: Colección de datos organizados de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la dase de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a estos.

Bitácoras: Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Backup: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables problemas si se realiza de forma habitual y periódica.

Centro de cómputo: Es un área de trabajo cuya función es la de concentrar, almacenar y procesar los datos y funciones operativas de una empresa de manera sistematizada.

COBIT: Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información, aceptados para ser empleados por gerentes de empresas y auditores.

Confidencialidad: Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, instituciones, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Control Interno: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos.

Cliente: Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Cliente-Servidor: Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

Criptografía: Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Datos: Hechos, especialmente los hechos numéricos, recopilados para referencia o información.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una institución autorizada.

Dominio: Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión de TI.

Equipo auditor: Grupo de personas encargadas de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

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

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Factibilidad: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Hardware: Los componentes físicos de un computador, tales como el teclado, el Mouse, las unidades de disco y el monitor.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.-.

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

Información: En sentido general, es todo lo que reduce la incertidumbre y sirve para realizar acciones y tomar decisiones.

Infraestructura: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

Integridad: Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Institución: Un grupo de individuos que trabajan para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, institución de caridad o fondo.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)

dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IP: Acrónimo de Internet. Es el protocolo que facilita la comunicación entre ordenadores conectados a la red Internet. Cada ordenador en Internet tiene una dirección IP única, que le identifica dentro de la red y permite su localización para posibilitar la comunicación.

ISACA: Information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISO: (Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas arreas, incluyendo la informática y las comunicaciones. Está formada por las organizaciones de normalización de sus 89 países miembro

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (trascripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

Lenguaje: En informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.

Mantenimiento correctivo: Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad, con el fin de prevenir su repetición.

Mantenimiento preventivo: Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades.

Normatividad: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Objetivo de control: Un estatuto del resultado o propósito que se desea alcanzar al implantar procedimientos de control en un proceso en particular.

Organización: Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones. Una organización puede ser pública o privada.

Password: Conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Políticas de seguridad: Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Plan estratégico de TI: Un plan a largo plazo, describe de forma cooperativa como los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso.

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toman las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Red: Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

Repositorio: Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros.

Riesgo: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

Sistema de información: Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software: término general que designa los diversos tipos de programas usados en computación.

TI: Tecnologías de Información

Técnica: La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

Técnicas: Conjunto de procedimientos de una ciencia los cuales nos ayudan a solucionar problemas.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario: Una persona o una institución externa o interna que recibe los servicios empresariales de TI.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Virus: Programa que se duplica así mismo en un sistema informático incorporándose a otros programas que son usados por varios sistemas.

INTRODUCCIÓN

Hoy en día, uno de los aspectos más importantes y críticos a la vez para el éxito y la supervivencia de cualquier organización, es la gestión efectiva de la información así como de las tecnologías relacionadas con ella.

Para muchas organizaciones, la información y las tecnologías que las soportan representan su medio o recurso más valioso, el actual estado de desarrollo de los sistemas de información hace que los mismos sean cada vez más complejos, integrados y relacionados; cada vez es necesario en todas las empresas y no solo en las grandes, garantizar el cumplimiento de las normas y procedimientos establecidos, para el manejo de las políticas relacionadas con la tecnología de la información, de esta forma, toda organización debe someterse a una auditoria de sistemas, la cual permite la revisión y la evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad.

En lo que tiene que ver con la seguridad de la información, éste debe ser un proceso integrador, quiere decir que con el uso de controles técnicos, administrativos y físicos, se debe lograr la confianza en los sistemas y garantizar que cumplan con los parámetros de disponibilidad, integridad, confidencialidad, confiabilidad y desempeño.

Desde el punto de vista de los sistemas de información, se presentó el proyecto "Técnicas de auditoría de sistemas aplicadas al sistema de información de la IPS INDIGENA GUAITARA del municipio de Ipiales", donde se identificó diferentes hallazgos y vulnerabilidades de seguridad física y lógica a las cuales se encuentra expuesta la información que se maneja diariamente, se evaluó sus entradas, procedimientos, controles, archivos y seguridad, a fin de que se logre una utilización más eficiente y segura.

Bajo este contexto y la preocupación de un mejoramiento continuo de la Ips Indígena Guáitara para garantizar la seguridad física y lógica de los datos que administra el Sistema Integral de nació la propuesta de presentar este trabajo de grado que lleva por titulo **AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES,** inscrito en la modalidad de Trabajo de aplicación, que se encuentra inscrito a la línea de investigación Sistemas Computacionales.

El presente documento se organizo de la siguiente forma: en la primera parte se planteo el problema y su sistematización, se planteo los objetivos que se alcanzaron luego se hablo de los antecedentes directamente relacionados con el proyecto, de la factibilidad y la metodología a seguir. En la última parte se

especificó los recursos que se utilizaron así como la distribución del tiempo de las tareas que se programaron para realizarse.

IDENTIFICACIÓN DEL PROBLEMA

TITULO DEL PROYECTO

AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓN DE LA IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES.

LÍNEA DE INVESTIGACIÓN

Este proyecto corresponde a la línea de investigación sistemas computacionales, ya que para el desarrollo del trabajo se utilizaron herramientas y conceptos sobre seguridad informática y administración de sistemas.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del problema. La IPS INDIGENA GUAITARA es una Institución Prestadora de Servicios de Salud Pública de carácter especial con responsabilidad administrativa y financiera, brinda servicios de primer nivel de atención, trabaja para mejorar el nivel de vida y mantener la salud de las comunidades indígenas de los Resguardos Indígenas de Ipiales, San Juan y Yaramal, por consiguiente es de vital importancia que los procedimientos de seguridad de la información que dicha institución maneja garanticen su veracidad e integridad.

Hasta la fecha el Sistema de Información de la IPS INDIGENA GUAITARA no había sido sometido a ningún tipo de estudio que permita verificar y evaluar su funcionamiento e identificar posibles falencias en los procedimientos de seguridad física y lógica de la información. Además, actualmente la IPS INDIGENA GUAITARA, no cuenta con documentación que permita corroborar el manejo correcto del sistema por parte de los usuarios directos e indirectos.

Formulación del problema. ¿Cómo aplicar técnicas de auditoría al Sistema de Información de la IPS INDIGENA GUAITARA, para realizar una revisión y evaluación de los controles físicos y lógicos, que salvaguardan la información?

Sistematización del problema.

¿Cómo verificar las condiciones de seguridad lógica de la información en la IPS INDIGENA GUAITARA con la realización de la auditoría al Sistema de Información?

¿Cómo verificar las condiciones de seguridad física de la información en la IPS INDIGENA GUAITARA con la realización de la auditoría al Sistema de Información?

¿Cómo realizar la evaluación de los controles que garantizan la seguridad física y lógica de la información que se maneja en la IPS INDIGENA GUAITARA para establecer los riesgos a los que se encuentra expuesta y recomendar controles para su protección?

OBJETIVOS

Objetivo general

Aplicar técnicas de auditoría al Sistema de Información de la IPS INDIGENA GUAITARA, que contribuyan a evidenciar vulnerabilidades en la seguridad física y lógica a los que se encuentra expuesta.

Las técnicas que permiten hacer una evaluación más eficiente y ayudan a examinar y evaluar correctamente este proceso de evaluación son: entrevistas, cuestionarios, encuestas, observación, inventarios, muestreo experimentación, examen, inspección, revisión documental, etc. A fin de evaluar y emitir un informe sobre el desarrollo normal de funciones y operaciones.

Objetivos específicos

Conocer el funcionamiento del Sistema de Información en la actualidad en cuanto los usuarios del sistema, el hardware y software, la seguridad física y lógica, entre otros.

Realizar un análisis de riesgos para identificar y conocer la causa de los mismos, para proponer alternativas de solución.

Aplicar el proceso de auditoría a los riesgos más relevantes que afecten el funcionamiento del sistema, utilizando las técnicas apropiadas para realizar las pruebas que me permitan evidenciar.

Elaborar un informe final de auditoría con las fallas encontradas, las soluciones propuestas y los planes de mejoramiento resultado de la auditoria.

JUSTIFICACIÓN

La auditoria de sistemas es de gran importancia para el excelente desempeño de los Sistemas de Información, ya que "*proporciona los controles necesarios para que los sistemas sean confiables y con un excelente nivel de seguridad*"[i1].

Para ayudar a cumplir a cabalidad las funciones de la IPS INDIGENA GUAITARA, esta se encuentra regida por los estándares de habilitación que exige el Instituto Departamental de Salud de Nariño. Es justificable la aplicación de medidas y estrategias para asegurar el adecuado y transparente manejo de los recursos y la información que está a cargo de dicha institución.

Por lo anterior, el proceso de auditoría de sistemas se convierte en elemento fundamental y de vital importancia, para determinar los hallazgos y vulnerabilidades más relevantes de seguridad física y lógica que actualmente se presentan en el sistema de información.

Con la ejecución de la auditoria se beneficiarán los diferentes usuarios de esta institución, ya que con base en los resultados presentados se podrán tomar las medidas necesarias, que permitan optimizar cada una de las tareas relacionadas con el procesamiento de la información.

La auditoria permitirá la elaboración de planes de mejoramiento para ser más eficientes y eficaces al dar repuesta a los procesos que se presenten en la entidad de manera que se beneficien los usuarios que manejen el sistema y los usuarios finales de los servicios.

[1] ECHENIQE GARCIA José A., Auditoría en informática, segunda edición 2a Ed., Mc Graw Hill D. F.

ALCANCE Y DELIMITACIÓN

En el desarrollo del proyecto se identificó e investigó las diferentes técnicas de auditoría de sistemas, con el propósito de determinar cuáles deben ser utilizadas. Dentro de las técnicas que se investigo se encuentran técnicas para obtener información como cuestionarios, entrevistas, flujogramas; técnicas para verificar controles como software de auditoría para terminales, software de auditoría de propósito especial, software generalizado de auditoría entre otras.

La aplicación de las técnicas y herramientas de auditoría dependió de la disponibilidad de los elementos de hardware y software de la institución auditada.

La aplicación de técnicas de auditoría se realizó al Sistema de Información de la IPS INDIGENA GUAITARA en el municipio de Ipiales, con el propósito de efectuar una revisión y evaluación de los controles físicos y lógicos, procedimientos de informática, observar su utilización, y evaluar la seguridad, con el fin de detectar problemas y plantear recomendaciones alternativas para que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Finalmente, los resultados de este proceso fueron plasmados en un informe donde se indicó la metodología de la auditoría, el sustento de la aplicación de diferentes técnicas y herramientas que servirá para que la institución, tome medidas preventivas y correctivas que subsanen los problemas detectados.

1. MARCO TEÓRICO

1.1 ANTECEDENTES

La auditoria de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia de que los datos que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de eficiencia.

Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información en uno solo, denominado sistema de información. En consecuencia por su naturaleza crítica el enfoque de auditoría debe anotar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoria tradicional, ósea mediante la creación de unos nuevos.

A principios de los años 80's, se empiezan a utilizar técnicas de tratamiento de la información por medio de computadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia.

Con la introducción de nuevas tecnologías, pronto se detectaron las limitaciones de los métodos tradicionales para realizar la auditoria de sistemas. En su afán de maximizar la eficiencia de los procesos de auditorías, surgen nuevos modelos que se adecuan a las crecientes necesidades del sector de las tecnologías de la información, entre ellos se tienen:

Directrices gerenciales de COBIT, desarrollado por la *InformationSystemsAudit Control Associatio*n (ISACA):

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y controle los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

The Management of the Control of Data InformationTechnology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA):

Este modelo está basado en el concepto de errores que establece responsabilidades relacionadas con la seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

SysTrust – Principios y criterios de confiabilidad de Sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA:

Este servicio pretende incrementar la confianza de alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos, manuales, automatizados, y datos. El modelo persigue determinar si el sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de prueba determinado bajo un ambiente dado).

Modelo de Evaluación de Capacidades de software (CMM), desarrollado por el Instituto de Ingenieros de Software (SEI):

Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

ISO/IEC 27001(*InformationTechnology – Security Techniques – Information Security Management System – Requirements*):

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Según el conocido “Ciclo de Deming”: PDCA – acrónimo de plan, *Do Check, Act* (Planificar, Hace, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/17799 (Actual ISO ICE 27002) y tiene su origen en la revisión de la norma Británica *British Standard* BS 7799 – 2: 2002.

Si se revisan los antecedentes de proyectos relacionados auditoría de sistemas en la universidad de Nariño se encuentran:

Proyecto: DEFINICION DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL CENTRO DE INFORMATICA DE LA UNIVERSIDAD DE NARIÑO.

Realizado por María Constanza Torres B. y Efraín Fajardo Guevara. El trabajo consistió en realizar los procesos de auditoría a la seguridad del centro de informática de la Universidad de Nariño.

Proyecto: TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACIÓN Y PÁGINAS WEB EN INSTITUCIÓNES OFICIALES DEL DEPARTAMENTO DE NARIÑO, ALCALDÍA DE TANGUA Y ALCALDÍA DE YACUANQUER.

Realizado por Lennin Geovanny Ibarra Gonzales y Diego Meza. El trabajo consistió en aplicar técnicas de auditoría en la contratación y en las páginas web de la alcaldía de Tangua y la alcaldía de Yacuanquer.

Proyecto: TECNICAS DE AUDITORIA DE SISTEMAS APLICADAS AL PROCESO DE CONTRATACIÓN Y PÁGINAS WEB EN INSTITUCIÓNES OFICIALES DEL DEPARTAMENTO DE NARIÑO, HOSPITAL CIVIL DE IPIALES Y HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE PASTO.

Realizado por Ricardo Alexander Cabrera y Luis Carlos Chávez Yela. El trabajo consistió en aplicar técnicas de auditoría en la contratación en las páginas web del Hospital Civil de Ipiales y Hospital Universitario Departamental de Pasto.

La información que se encuentra en estos proyectos, servirá de base para la comprensión de diferentes técnicas y metodologías utilizadas en auditoria de sistemas. Además, permiten identificar la manera de presentar los resultados e informes de auditoría, así como los diferentes tipos de pruebas.

Los proyectos que se tomaron en cuenta para la elaboración del proceso de auditoría ayudaron a verificar de lo que se puede evaluar, observar en que campos se puede aplicar las auditorias, identificar, analizar y tratar todos los aspectos del estándar COBIT, de esta manera lo que se hace es manejar lo mejor de ellas para adecuarlas y tratar eficientemente los datos.

1.2 ASPECTOS GENERALES SOBRE AUDITORIA

"La auditoría puede definirse como un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso." [2].

[2] http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/auditcontxactual.htm

Por otra parte, la auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización.

La auditoria como función de control debe ser la herramienta a utilizar para ayudar a los Funcionarios que tienen responsabilidad Administrativa, Técnica y Operacional a que no incurran en falta. Y es por ello que aquí el Control debe ser creativo, inteligente, y constructivo de asesoramiento oportuno a todas las direcciones o gerencias a fin de que la toma de decisiones sea acertada, segura y se logren los objetivos, con la máxima eficiencia.

La responsabilidad de un procedimiento de auditoría debe ir más allá de la búsqueda de problemas y de responsables, la visión de la auditoría debe dar la visión de la empresa en su conjunto, por lo que saca el máximo provecho de la información real y existente, convirtiéndola en herramienta de reingeniería capaz de retroalimentar procesos o crear nuevos, la auditoria se volvió capaz de identificar necesidades, problemas y soluciones a futuro, con estas facultades el proceso de auditoría se promueve como una función permanente y a largo plazo.

1.3 EL AUDITOR

Es aquella persona profesional, que se dedica a trabajos de auditoría habitualmente con libre ejercicio de una ocupación técnica.

El auditor socio-laboral puede ser interno o externo a la empresa y provenir de las más diversas disciplinas: ingeniería, derecho, sociología, economía,...etc. pero en cualquier caso deberá contar con una serie de características:

Deberá dominar las técnicas y metodologías del proceso auditor

Debe ser abierto en sus relaciones personales y que sepa dialogar

Debe poseer diversas actitudes como la independencia, la objetividad, la creatividad, el espíritu crítico, la diplomacia, etc.

El auditor debe mantener un cierto grado de independencia en los asuntos que se encuentra evaluando.

El auditor tiene la obligación de realizar con esmero y cuidado el dictamen o informe para el que fue contratado.

Debe poseer una actitud positiva frente a la institución evaluada.

Debe tener estabilidad emocional frente la institución.
Es su obligación la de respetar las ideas de los demás.

Debe tener capacidad para la negociación.

Sera discreto y respetuoso con la información de la empresa.

Su comportamiento debe ceñirse a la ética profesional.

En las organizaciones la auditoría puede ser realizada por un consultor externo que conozca las experiencias de otras organizaciones y sea considerado como una autoridad en investigación de recursos humanos. También pueden recurrir a su propio personal y constituir comités evaluadores, que puede estar compuesto por el director del departamento de recursos humanos y otros actores implicados en la organización: directivos de línea y trabajadores y otra forma es la combinación de ambas figuras: consultor externo y comité evaluador, trabajando en conjunción y de manera coordinada.

La misión del auditor es la de ayudar a los miembros de la dirección a ejercer eficazmente sus responsabilidades, proporcionándoles los análisis, las apreciaciones y las recomendaciones pertinentes sobre las actividades examinadas que recogerá en un informe.

1.4 TIPOS DE AUDITORÍA

a) El proceso de auditoría que se realiza en una empresa puede ser de dos tipos de acuerdo a sus respectivos enfoques:

Auditoría Interna
Auditoría Externa

1.4.1 Auditoría interna. Es una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección.

Es un control de dirección que tiene por objeto la medida y evaluación de la eficacia de otros controles.

“La auditoría interna surge con posterioridad a la auditoría externa por la necesidad de mantener un control permanente y más eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente, la auditoría interna clásica se ha venido ocupando fundamentalmente del sistema de

control interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger el activo, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera. Se ha centrado en el terreno administrativo, contable y financiero."[3].

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección. Con anterioridad, el control lo ejercía directamente la dirección de la empresa por medio de un permanente contacto con sus mandos intermedios, y hasta con los empleados de la empresa. En la gran empresa moderna esta peculiar forma de ejercer el control ya no es posible hoy día, y de ahí la emergencia de la llamada auditoría interna.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole análisis objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas.

1.4.2 Auditoría externa. Es un examen crítico y sistemático, el cual se encuentra debidamente detallado, que se le realiza a cualquiera de los sistemas de información de una organización y emite una opinión independiente sobre los mismos, además, verifica transacciones, cuentas, informaciones, o estados financieros, correspondientes a un período, evaluando la conformidad o cumplimiento de las disposiciones legales o internas vigentes en el sistema de control interno contable.

"Una auditoría externa debe hacerla una persona o firma independiente de capacidad profesional reconocidas. Esta persona o firma debe ser capaz de ofrecer una opinión imparcial y profesionalmente experta a cerca de los resultados de auditoría, basándose en el hecho de que su opinión ha de acompañar el informe presentado al término del examen y concediendo que pueda expresarse una opinión basada en la veracidad de los documentos y de los estados financieros y en que no se imponga restricciones al auditor en su trabajo de investigación." [4].

Los objetivos de la auditoría externa son: proporcionar a la dirección y a los propietarios de la empresa unos estados financieros certificados por una autoridad independiente e imparcial, proporcionar asesoramiento a la gerencia y a los

[3] http://www.gerencie.com/auditoria-interna.html
[4] http://www.gerencie.com/auditoria-externa.html

responsables de las distintas áreas de la empresa en materia de sistemas contables y financieros, procedimientos de organización y otras numerosas fases de la operatoria de una empresa, suministrar información objetiva que sirva de base a las instituciones de información y clasificación crediticia, servir de punto de partida en las negociaciones para la compraventa de las acciones de una empresa, reducir y controlar riesgos accidentales, fraudes y otras actuaciones anormales, liberar implícitamente a la gerencia de sus responsabilidades de gestión.

1.4.2.1Principios generales de la auditoría externa.

Exposición: Los estados financieros deben recoger por completo y con claridad todas las transacciones de la empresa.

Uniformidad: La base utilizada en la preparación de los estados financieros de un ejercicio no debe experimentar ninguna variación con respecto al ejercicio precedente.

Importancia o materialidad: Este es el criterio que debe presidir el trabajo del auditor es la importancia económica o materialidad de las partidas.

Moderación: De dos o más posibilidades igualmente validas se debe escoger siempre la que dé los resultados más desfavorables.

1.4.2.2 Normas generales de la auditoría externa. Afectan a las condiciones que debe de reunir el auditor de y a su comportamiento en el desarrollo de la actividad de auditoría.

Realización por una persona competente.

Realización por una persona independiente.

Cuidado profesional en la realización del trabajo y en la confección del informe.

1.4.2.3 Normas de trabajo de la auditoría externa. Hacen referencia a la preparación y ejecución del trabajo a realizar por el auditor, regulan el conjunto de técnicas de investigación e inspección aplicables a los hechos relativos a los documentos contables sujetos a examen, mediante los cuales el auditor fundamenta su opinión responsable e independiente.

Programación adecuada.

Supervisión adecuada.

Análisis del control interno para fijar el alcance de la pruebas.

Opinión basada en un material y un trabajo razonablemente suficiente.

1.4.2.4 Normas del informe de la auditoría externa. Regulan los principios que han de ser observados en la elaboración y presentación del informe de auditoría estableciendo la extensión y contenido de los diferentes tipos de informes, así como los criterios que fundamenten el modelo de informe a utilizar en cada caso.

Expresión de si los estados financieros se ajustan a los principios de contabilidad generalmente aceptados.

Expresión de si se han presentado los estados financieros de manera uniforme con respecto al periodo precedente.

Exposiciones informativas razonablemente adecuadas a los estados financieros.

El informe debe contener un dictamen sobre los estados financieros considerados en su conjunto.

1.4.2.5 Procedimientos de la auditoría externa. Procedimientos de la auditoría externa son la serie de trabajos que hay que realizar para el adecuado cumplimiento de los principios y las normas, antes de presentar el informe definitivo. Se pueden señalar los siguientes procedimientos:

Revisión de las actividades en las operaciones.

Inspecciones físicas y recuentos.

Obtención de pruebas de evidencia.

Obtención de pruebas de exactitud.

Preparación de reconciliaciones.

1.4.3 Diferencias entre auditoría interna y externa. Existen diferencias substanciales entre la Auditoría Interna y la Auditoría Externa, algunas de las cuales se pueden detallar así:

En la Auditoría Interna existe un vínculo laboral entre el auditor y la empresa, mientras que en la Auditoría Externa la relación es de tipo civil.
En la Auditoría Interna el diagnóstico del auditor, está destinado para la empresa; en el caso de la Auditoría Externa este dictamen se destina generalmente para terceras personas o sea ajena a la empresa.

La Auditoría Interna está inhabilitada para dar Fe Pública, debido a su vinculación contractual laboral, mientras la Auditoría Externa tiene la facultad legal de dar Fe Pública.

b). Existen algunos tipos de auditoría entre los que la auditoría de sistemas integra un mundo paralelo pero diferente y peculiar resaltando su enfoque a la función informática.

Entre los principales enfoques de auditoría tenemos los siguientes:

1.4.4 Auditoria fiscal. "Consiste en la investigación selectiva, comprobación científica y sistemática de los estados financieros, libros de cuentas, comprobantes, cuentas del balance, cuentas de resultados, documentación, registros y operaciones efectuadas por una empresa, tendientes a comprobar que las bases afectas a tributos se hayan determinado de acuerdo con las normas técnicas que regulan la contabilidad y cumpliendo con las disposiciones legales contenidas en el Código de Comercio, Código Orgánico Tributario, y demás leyes impositivas que corresponda aplicar."[5].

La auditoría fiscal suele ser llevada a cabo por un auditor correspondiente, que utiliza un grupo de actividades que resultan muy competentes a la hora de lograr una regularidad en la administración del patrimonio de una empresa, posee varios instrumentos fiscales, con la finalidad de verificar el cumplimiento en forma correcta de las obligaciones tributarias formales y sustanciales de todo contribuyente, así como también determinar los derechos tributarios a su favor. Es por ello que al efectuar el examen se deben aplicar las respectivas técnicas y procedimientos de auditoría.

1.4.5 Auditoría financiera. Es un examen objetivo, sistemático, profesional e independiente, efectuado de acuerdo con normas de Auditoría generalmente aceptadas tomando como base los estados de resultados, estados de flujo de efectivo, estado de utilidades retenidas o déficit acumulado y cuotas a los estados financieros.

[5] http://www.monografias.com/trabajos16/auditoria-fiscal/auditoria-fiscal.shtml

"Su objetivo es evaluar y verificar las operaciones que han dado lugar a los mencionados estados financieros con el fin de emitir una opinión o dictamen sobre si presentan razonablemente la situación financiera de las empresas, los resultados de sus operaciones y los cambios que ésta haya sufrido: todo ello en concordancia con principios y normas de contabilidad generalmente aceptadas o con las disposiciones legales vigentes aplicables para cada caso, y asegurándose de que dichos estados financieros hayan sido preparados en forma consistente de un período a otro."[6].

1.4.6 Auditoria administrativa u operativa. Es el revisar y evaluar si los métodos, sistemas y procedimientos que se siguen en todas las fases del proceso administrativo aseguran el cumplimiento con políticas, planes, programas, leyes y reglamentaciones que puedan tener un impacto significativo en operación de los reportes y asegurar que la organización los esté cumpliendo y respetando.

Forma parte de una estrategia, de un proceso de cambio que requiere una clara decisión del más alto nivel y un consenso de voluntades destinado a lograr que una organización tenga la capacidad para transformarse y crecer de manera efectiva.

"Por sus características, permite que se revele en qué áreas se requiere de un estudio más profundo, qué acciones se pueden tomar para subsanar deficiencias, cómo superar obstáculos, cómo imprimir mayor cohesión al funcionamiento de las mismas y, sobre todo, un análisis causa-efecto que concilie en forma congruente los hechos con las ideas."[7]

1.4.7 Auditoria integral. Es el proceso de obtener y evaluar objetivamente, en un período determinado, evidencia relativa a la información financiera, al comportamiento económico y al manejo de una institución con la finalidad de informar sobre el grado de correspondencia entre aquellos y los criterios o indicadores establecidos o los comportamientos generalizados.

El objetivo de la auditoria integral es evaluar los sistemas de control, implantados por la Gerencia General que le permitan medir el rendimiento económico y los recursos financieros de la empresa.

Además con la auditoria integral se pretende conocer la normativa que regula a la Auditoría Integral, analizar el ambiente de aplicación de la Auditoría Integral, verificar a través de la utilización de un conjunto estructurado de proceso tomando como objetivo la evaluación sistemática y permanente del ente económico para una aseveración verificable.

[6] http://www.monografias.com/trabajos16/auditoria-fiscal/auditoria-fiscal.shtml
[7] http://www.monografias.com/trabajos16/auditoria-fiscal/auditoria-fiscal.shtml

La Auditoría Integral implica la ejecución de un trabajo con el trabajo o enfoque, por analogía de las revisiones financieras, de cumplimiento, control interno y de gestión, sistema y medio ambiente.

1.4.8 Auditoria de sistemas. Es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría de sistemas deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría de sistemas es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).
Tiene por objetivo encontrar una relación óptima entre el costo y beneficio de los sistemas automáticos o informáticos diseñados e instalados para una determinada empresa. Además de hacer que los sistemas informáticos resulten mucho más fáciles y prácticos de usar para aquellos empleados encargados de operarlos, asegurar una mayor integridad y confiabilidad en cuanto a la información que se encuentra almacenada en los sistemas realizando algún control periódico.

Existen varios campos de acción en los que la auditoria informática de sistemas puede operar entre ellos se tienen las auditorias más destacadas del tipo:

Sistemas operativos. Engloba los Subsistemas de Teleprocesos, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir la posible incompatibilidad entre otros productos de Software Básicos adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

Software básico. Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al software desarrollado por el personal informático de la empresa, el auditor debe verificar

que este no agreda ni condiciona al Sistema Igualmente, debe considerar el esfuerzo en términos de costes, por si hubiera alternativas más económicas.

La auditoría, al igual que cualquier otra actividad, requiere de una buena planeación, que le permita desarrollarse eficientemente y oportunamente.

1.5 AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

Desde que la informática se enfocó hacia el apoyo de la sistematización en las áreas del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nómina, etc., lo que originó el proceso conocido como auditoria a sistemas de información.

"La auditoria de sistemas es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes."[8].

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

La auditoria de sistemas permite además verificar que la información desde su entrada, procedimientos, controles, almacenamientos y salidas, sea integra y verificable y por tanto permita el apoyo a la toma de decisiones dentro de una organización

Dentro de este procedimiento es necesario evaluar los mecanismos de control implantados en una organización, determinando así, si son adecuados y cumplen con los objetivos o estrategias, de esta manera, es posible proponer cambios que se deberían realizar para el mejoramiento de los mismos. Estos mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

[8] http://www.slideshare.net/veroalexa10/auditoria-informatica-4714423

1.5.1 Alcance de la auditoria de sistemas. "El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría de sistemas, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas."[9].

1.5.2 Objetivos de la auditoria de sistemas.

1.5.2.1 Objetivo general de la auditoria de sistemas. El objetivo principal de la auditoria de sistemas es evaluar el uso adecuado de los sistemas para el correcto ingreso de datos, el procesamiento adecuado de la información y la emisión oportuna de los resultados en la organización, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas de información dentro de la empresa.

1.5.2.2 Objetivos específicos de la auditoria de sistemas

Participar en el desarrollo de nuevos sistemas.

Evaluar los controles.

Cumplir con la metodología.

Evaluar la seguridad en el área informática.

Evaluar la suficiencia en los planes de contingencia.

Respaldar, proveer qué va a pasar si se presentan fallas.

Opinar sobre la utilización de los recursos informáticos.

Resguardar y proteger los activos.

Control de modificación a las aplicaciones existentes.

Fraudes

Control a las modificaciones de los programas.

Participar en la negociación de contratos con los proveedores.

[9] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

Revisar la utilización del sistema operativo y los programas utilitarios.

Controlar la utilización de los sistemas operativos.

Programas utilitarios.

Auditoría de la base de datos.
Estructurar sobre la cual se desarrollan las aplicaciones.

La revisión de la eficaz gestión de los recursos informáticos.

1.5.2.3 Fines de la auditoría de sistemas.

Fundamentar la opinión del auditor interno (externo) sobre la confiabilidad de los sistemas de información.

Expresar la opinión sobre la eficiencia de las operaciones en el área de TI.

La auditoria de sistemas sirve para mejorar ciertas características en la empresa como:

Eficiencia

Eficacia

Rentabilidad

Seguridad

1.5.3 Pruebas y herramientas para efectuar una auditoría de sistemas. En la realización de una auditoria de sistemas el auditor puede realizar las siguientes pruebas.

Pruebas sustantivas: Verifican el grado de confiabilidad del sistema de información de la organización. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

Pruebas de cumplimiento: "Verifican el grado de cumplimiento de aquello extraído el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente."[10].

[10]http://www.slideshare.net/veroalexa10/auditoria-informatica-4714423

Las principales herramientas de las que dispone un auditor informático son:
Observación
Realización de cuestionarios

Entrevistas a auditados y no auditados

Muestreo estadístico

Flujogramas

Listas de chequeo

Mapas conceptuales

1.5.4 Pasos a seguir para una auditoria de sistemas en una organización.

1.5.4.1 Estudio preliminar. Para realizar dicho estudio se examinan las funciones y actividades generales del área o departamento de sistemas, con el fin de tener un contacto inicial con el personal de dicha área, y conocer a grandes rasgos la distribución del sistema, características de equipos, instalaciones y medidas de seguridad visibles.

Para su realización el auditor debe conocer lo siguiente:

a. Organización

Es de vital importancia conocer dentro del departamento o área de sistemas quien es el jefe, quien diseña y quien ejecuta, para lo cual es necesario conocer:

Organigrama: El organigrama permite conocer la estructura oficial dentro de la organización a auditar.

Departamentos: Es importante conocer los departamentos que hacen parte de la organización y las funciones que se deben llevar a cabo dentro de cada uno de ellos.
Relaciones Jerárquicas y funcionales entre órganos de la Organización: Es necesario verificar si dentro de la organización se cumplen las relaciones funcionales y jerárquicas que se evidencian dentro del organigrama.

b. Corrientes de información

Los flujos de información entre los diferentes departamentos dentro de una organización son de vital importancia ya que evidencian una gestión eficiente,

siempre y cuando estas corrientes no vayan en direcciones no contempladas dentro del organigrama.
En muchas ocasiones es posible que se hayan creado canales de información alternativos, lo cual ocurre cuando existen pequeños o grandes fallos en la estructura de la organización.

Además, la aparición de corrientes de información no planeados pueden obedecer a afinidades personales o desacato a las reglas establecidas. Los cuales pueden producir perturbaciones dentro de la organización.

1.5.4.2 Flujos de información. Dentro del proceso de auditoría es necesario verificar que los nombres de los cargos dentro de la organización correspondan a las funciones que realiza esa persona.

Puede ocurrir que bajo nombres de cargos diferentes se realicen funciones idénticas, en este caso se estaría realizando tareas redundantes lo cual podría conllevar a deficiencias estructurales.

1.5.4.3 Entorno operacional. Es importante conocer por parte de los auditores de sistemas la referencia del entorno en el cual se va a trabajar, esto se logra determinando:

Ubicación geográfica del o los centros de procesamiento de información de la empresa. Evaluando además el personal responsable de cada uno de ellos.

Arquitectura y configuración de Hardware y Software: es fundamental la verificación de la compatibilidad e intercomunicación de los equipos ya que estas, están estrechamente ligadas a los grados de seguridad lógica de las organizaciones.
Situación geográfica de los Sistemas: el equipo auditor debe estudiar la información que proporcione la organización sobre los elementos físicos y lógicos de las instalaciones.
Comunicación y Redes de Comunicación: se debe disponer de un inventario, estado y características de las redes de comunicación.

1.5.4.4 Aplicaciones bases de datos. Finalmente para el equipo auditor es necesario tener una idea general de los procesos informáticos realizados dentro de la organización.

Para ello es necesario recolectar la siguiente información:

Inventario de Hardware y Software.

Volumen, antigüedad y complejidad de las Aplicaciones.

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones.

Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto:

Metodología del diseño: La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

La documentación de programas disminuye gravemente el mantenimiento de los mismos.

Documentación: El auditor recaudara información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

Estos datos proporcionan una visión aceptable de las características de la carga informática.

1.5.4.5 Elaboración del plan y de los programas de trabajo. El plan de trabajo se realiza de acuerdo a los siguientes criterios:

El proceso de auditoría se llevara a cabo en áreas generales o específicas.

La auditoria se hará de manera global o especifica.
De acuerdo a si se manejaran recursos genéricos o específicos se realizará un cronograma de trabajo.
El Plan establece disponibilidad futura de los recursos durante la revisión.

El Plan estructura las tareas a realizar por cada integrante del grupo auditoria.

En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades, esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

1.5.4.6 Actividades de la auditoría de sistemas. La auditoría de sistemas general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.
a. Técnicas de Trabajo:

Análisis de la información recabada del auditado

Análisis de la información propia

Cruzamiento de las informaciones anteriores

Entrevistas

Simulación

Muestreos

b. Herramientas:

Cuestionario general inicial

Cuestionario Checklist

Estándares

Monitores

Simuladores (Generadores de datos)

Paquetes de auditoría (Generadores de Programas)

Matrices de riesgo

c. Informe Final

El informe final de la auditoria de sistemas se realiza por escrito, el cual contempla la siguiente estructura:

Definición de objetivos y alcance de la auditoría

Enumeración de temas objeto de la auditoria

Cuerpo de la auditoria: para lo cual se mostrara los siguiente para cada tema:

Situación actual

Tendencias futuras

Puntos débiles y amenazas

Recomendaciones y planes de acción

Redacción posterior de la Carta de Introducción o Presentación

Algunas Características que deben ser consideradas en los informes son:

Las características de fondo se refieren a que la información sea veraz y oportuna, el uso de la terminología se exacta y objetiva, que exista congruencia con lo observado sin hacer ninguna distorsión de lo encontrado.

Las características de forma: el estilo de redacción concreto conciso, clara, sencilla y amena, que no haya redundancia, redacción impecable en ortografía.

1.6 METODOLOGÍAS DE AUDITORIA DE SISTEMAS

El auditor en cualquier área deberá seguir una metodología en donde utilice diferentes técnicas y herramientas para poder asegurar una correcta recolección y evaluación de evidencia que le permita establecer si se cumple o no con los objetivos organizacionales.

Las metodologías para la auditoria de sistemas o auditoria a la tecnología de información son muy variadas, encontrándose entre ellas la que propone una revisión de objetivos de control propuesta en el COBIT por la ISACA (Information Systems Audit and Control Association). Con esta metodología se permite la verificación y comprobación del sistema de control en tecnologías de la información. Los controles ahí descritos y la guía de auditoría pueden ser utilizados por los auditores o por los directores como una forma de verificar el cumplimiento de los objetivos. Sin embargo, una metodología completa debe abarcar más pasos para poder asegurar una evaluación completa que incluya revisión de elementos ligados a los objetivos de control y elementos de presentación de documentos con recomendaciones y hechos importantes dirigidos a los interesados en el negocio.

Para esto, se hace necesario aplicar una auditoría de sistemas llevando a cabo una metodología adecuada, que permita evaluar de manera objetiva las vulnerabilidades o falta de controles existentes en la empresa.

“Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo tiene la desventaja de depender mucho de la experiencia,

habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica."[11].

"En la auditoria de sistemas existen varias metodologías como: COBIT (ISACA), COSO, SAC, AICPA (SAS), IFAC (NIA), MARGERIT y EDP."[12] . Sin embargo, las metodologías más utilizadas son: COBIT, MARGERIT y COSO.

Estas últimas hacen parte de los modelos a seguir dentro del control interno y son necesarias para desarrollar cualquier proyecto de manera ordenada y eficaz, por lo que cada una cumple un papel importante y al optar por una de ellas, el auditor debe cumplirlas a cabalidad.

1.6.1 COBIT (Control Objectives for Information and related Technology). Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association), se formo como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI)[13].

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

[11] PIATTINI, Mario y Emilio del Peso. Auditoría Informática. Un enfoque práctico. Editorial RA-MA.
[12] Tesis, Auditoria al modulo de historia clínica. Jenny Burgos y Carolina Domínguez. Año 2007. Pág. 59-60 y 87-94.
[13] www.megapuntes.com.ar/auditoria/ALUMNOS2008/ISACA.doc

COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:
- Planificación y organización
- Adquisición e implantación
- Soporte y servicios
- Monitoreo

Estos dominios agrupan objetivos de control de alto nivel que cubren tanto los aspectos de información como de la tecnología que la respalda, facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

"Así mismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano."[14].

1.6.1.1 Dominio: planificación y organización (PO). Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Procesos:

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

[14] http://www.channelplanet.com/index.php?idcategoria=13932

El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.

Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos.

PO2 Definición de la arquitectura de información

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.

El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.

La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

PO3 Determinación de la dirección tecnológica

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y

debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.

Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI

Objetivo: Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.

Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente.

Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.

Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.

La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.

El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

PO5 Manejo de la inversión

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.

El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información.

La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

PO6 Comunicación de la dirección y aspiraciones de la gerencia

Objetivo: Asegurar el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.

Las directrices tecnológicas.

El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.

El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.

Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

PO7 Administración de recursos humanos

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.

Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.

La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.

La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

PO8 Asegurar el cumplimiento con los requerimientos externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales. Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.

Leyes, regulaciones y contratos

Revisiones regulares en cuanto a cambios

Búsqueda de asistencia legal y modificaciones

Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

Privacidad

Propiedad intelectual

Flujo de datos externos y criptografía

PO9 Evaluación de riesgos

Objetivo: : Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.
Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.

Actualización de evaluación de riesgos

Metodología de evaluación de riesgos

Medición de riesgos cualitativos y/o cuantitativos

Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.

Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

PO10 Administración de proyectos

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.

Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.

Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
Presupuestos de costos y horas hombre.

Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.

Plan de administración de riesgos para eliminar o minimizar los riesgos.

Planes de prueba, entrenamiento, revisión post-implementación.

PO11 Administración de calidad

Objetivo: Satisfacer los requerimientos del cliente.

Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.

Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.

Documentación de pruebas de sistemas y programas

Revisiones y reportes de aseguramiento de calidad.

1.6.1.2 Dominio: adquisición e implementación (AI). Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Procesos:

AI1 Identificación de soluciones automatizadas

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.

Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.

Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.

Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.

Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)

Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.

Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

AI2 Adquisición y mantenimiento del software aplicativo

Objetivo: Proporcionar funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.

Requerimientos de archivo, entrada, proceso y salida.
Interface usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.

Personalización de paquetes

Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.

Controles de aplicación y requerimientos funcionales

Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

AI3 Adquisición y mantenimiento de la infraestructura tecnológica

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.

Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.

Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

AI4 Desarrollo y mantenimiento de procedimientos

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.

Manuales de Operaciones y controles, de manera que estén en permanente actualización.

Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 Instalación y aceptación de los sistemas

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.

Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.

Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.

Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera más económica.

AI6 Administración de los cambios

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.
Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

Identificación de cambios tanto internos como por parte de proveedores.

Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
Evaluación del impacto que provocaran los cambios.

Autorización de cambios

Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.

Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

1.6.1.1 Dominio: entrega y dar soporte (DS). En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de

soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos

DS1 Definición de niveles de servicio

Objetivo: Establecer una comprensión común del nivel de servicio requerido. Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

Definición de las responsabilidades de los usuarios y de la función de servicios de información.

Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.

Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.

Garantías de integridad.

Convenios de confidencialidad.

Implementación de un programa de mejoramiento del servicio.

DS2 Administración de servicios prestados por terceros

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos
Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.

Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.

Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

DS3 Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.

Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información.

Monitoreo y reporte de los recursos de tecnología de información.

Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.

Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño.

Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas..

DS4 Asegurar el servicio continuo

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

Planificación de Severidad

Plan Documentado

Procedimientos Alternativos

Respaldo y Recuperación

Pruebas y entrenamiento sistemático y singulares

DS5 Garantizar la seguridad de sistemas

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.

Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario.

Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación,

almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas.

Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos.

Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.

Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización

DS6 Educación y entrenamiento de usuarios

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados

Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

Currículo de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.

Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.
Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

DS7 Identificación y asignación de costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.

Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades.

Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

DS8 Apoyo y asistencia a los clientes de TI

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda.

Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas.

Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

DS9 Administración de la configuración:
Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición.

Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración.

Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización.

Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas.

DS10 Administración de problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

DS11 Administración de datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.
Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

DS12 Administración de las instalaciones

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas

humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13 Administración de la operación

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

1.6.1.4 Dominio: monitoreo evaluación (ME). Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos

M1 Monitoreo del proceso

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

M2 Evaluar lo adecuado del control interno

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

M3 Obtención de aseguramiento independiente

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

M4 Proveer auditoría independiente

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa.

Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

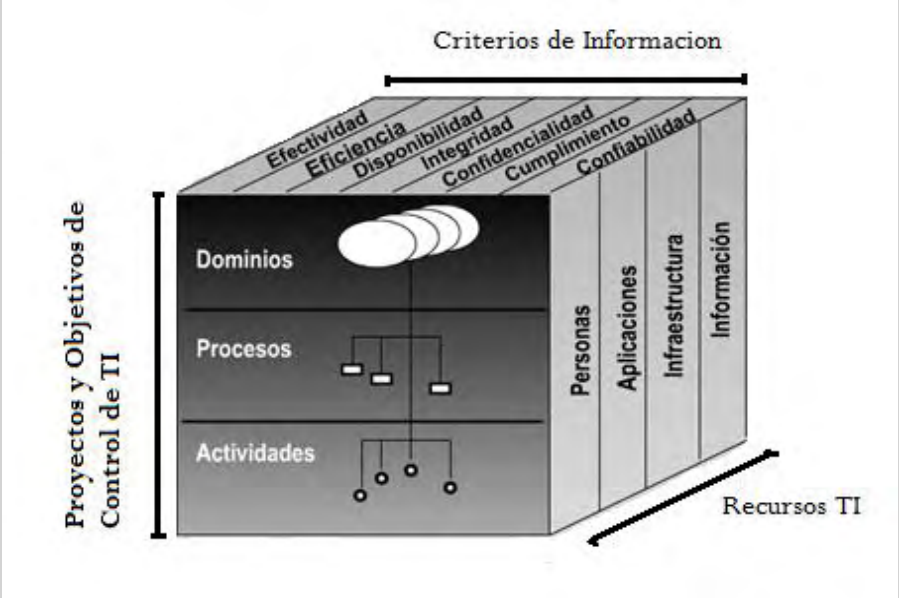
Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán".

Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

Los recursos de las TI
Los criterios empresariales que deben satisfacer la información
Los procesos de TI
Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Como se muestra en la figura 1.

Figura 1. Las tres dimensiones conceptuales de COBIT



Fuente: GUSTIN Enith, SOLARTE Francisco Javier, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, Copyright © 2011

Además, se toma en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Toda organización, necesita desarrollar una tecnología que le permita rediseñar actividades y procesos para lograr un mejor desempeño en las mismas, es así

como el COBIT es fundamental en toda empresa, pues esta metodología reduce posibles vulnerabilidades y riesgos de los recursos de las tecnologías de información y así mismo evalúa el resultado de los objetivos de la empresa.

1.6.2 ISO 27000: Sistemas de gestión de la seguridad de la información. La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación.

¿Qué es ISO 27000?

Es una familia de estándares internacionales para Sistemas de Gestión de la Seguridad de la Información (SGSI).

1. Requisitos para la especificación de sistemas de gestión de la seguridad de la información
2. Proceso del análisis y gestión del riesgo
3. Métricas y medidas de protección
4. Guías de implantación
5. Vocabulario claramente definido para evitar distintas interpretaciones de conceptos técnicos y de gestión y mejora contínua.

Alcance ISO27000

General: Cubre todos los tipos de organizaciones. También especifica los requerimientos a establecer, poniendo en ejecución, funcionando, supervisando, repasando, manteniendo y mejorando la documentación del Sistema de Administración en la Seguridad de la Información (ISMS), dentro del contexto de la Totalidad de los riesgos del negocio.

Aplicación: El conjunto de requerimientos precisados en este estándar internacional son genéricos y se piensa sean aplicables a todas las organizaciones, sin importar su tipo, tamaño y naturaleza.

1.6.2.1 ISO 27001 Sistemas de gestión de la seguridad de la información. Esta norma muestra cómo aplicar los controles propuestos en la ISO 17799, estableciendo los requisitos para construir un SGSI, “auditable” y “certificable”.

La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización. El hecho de

disponer de la certificación según ISO/IEC 27001 le ayuda a gestionar y proteger sus valiosos activos de información.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

1.6.2.2 Riesgo informático. Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{Riesgo} = \frac{\text{Amenaza} + \text{Vulnerabilidad}}{\text{Contramedida}}$$

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como falencias (flaws) o brechas (breaches)) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

1. Personas tanto internas como externas de la organización.
2. Desastres naturales.
3. Por servicios, suministros y trabajos no confiables e imperfectos.
4. Por la incompetencia y las deficiencias cotidianas.
5. Por el abuso en el manejo de los sistemas informáticos.
6. Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

1.6.2.3 Controles. Es el conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Clasificación general de los controles

Controles Preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones
Sistemas de claves de acceso.

Controles detectivos: Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.
Ejemplo: Archivos y procesos que sirvan como pistas de auditoría
Procedimientos de validación.

Controles Correctivos: Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

Principales Controles físicos y lógicos

Controles particulares tanto en la parte física como en la lógica se detallan a continuación:

Autenticidad

Permiten verificar la identidad

Passwords
Firmas digitales

Exactitud

Aseguran la coherencia de los datos

Validación de campos

Validación de excesos

Totalidad

Evitan la omisión de registros así como garantizan la conclusión de un proceso de envió

Conteo de registros
Cifras de control

Redundancia

Evitan la duplicidad de datos

Cancelación de lotes
Verificación de secuencias

Privacidad

Aseguran la protección de los datos

Compactación
Encriptación

Existencia

Aseguran la disponibilidad de los datos

Bitácora de estados
Mantenimiento de activos

Protección de Activos

Destrucción o corrupción de información o del hardware

Extintores
Passwords

Efectividad

Aseguran el logro de los objetivos

Encuestas de satisfacción

Medición de niveles de servicio

Eficiencia

Aseguran el uso óptimo de los recursos

Programas monitores
Análisis costo-beneficio

1.6.3 MAGERIT. **Análisis y gestión de riesgos de los sistemas de la información.** El Consejo Superior de Informática ha elaborado la Metodología de Análisis y Gestión de Riesgos de los sistemas de información, MAGERIT. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes, pero que también dan lugar a ciertos riesgos que deben minimizarse con medidas que garanticen la seguridad y generen confianza en la utilización de estos medios.

El ciclo de gestión de la seguridad siempre establece como primera etapa el análisis y la gestión de los riesgos del sistema que tratamos de proteger. Para una correcta definición e implantación de la seguridad, es necesario identificar y determinar los diferentes elementos significativos dentro del entorno de la seguridad de los sistemas de información.

Elementos de MAGERIT

A continuación se define brevemente los elementos considerados significativos por MAGERIT para el estudio de la Seguridad en Sistemas de Información.

Activos: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

Amenazas: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Vulnerabilidad de un activo: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

Impacto en un activo: consecuencia sobre éste de la materialización de una amenaza.

Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización

Servicio de salvaguarda: acción que reduce el riesgo.

Mecanismo de salvaguarda: procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

Descripción del Proceso de Análisis y Gestión de Riesgos

En el proceso de análisis y gestión de riesgos de la seguridad en los sistemas de información se puede identificar las siguientes etapas:

Planificación: En esta fase, se establece el objetivo del proyecto, el dominio de estudio y las restricciones generales. Deben también definirse las métricas con las que se valorarán los diferentes elementos de seguridad, de manera que los resultados finales de medición del riesgo sean definidos en función de los parámetros adecuados para cuantificar el riesgo por la organización (por ejemplo, definir la escala de frecuencias para medir la vulnerabilidad, definir las cantidades monetarias por las que cuantificar el impacto, etc.).

Análisis de riesgos: Una vez definido el dominio, los analistas de riesgos procederán a realizar las entrevistas al personal de la organización para la obtención de información. En esta fase se identificarán los activos de la organización, identificando las relaciones que se establecen entre activos.

De esta forma se obtiene el "árbol de activos" que representan las distintas dependencias y relaciones entre activos, es decir, todos aquellos elementos que están "encadenados entre sí" en términos de seguridad.

También se identifican el conjunto de amenazas, estableciendo para cada activo, cual es la vulnerabilidad que presenta frente a dicha amenaza.

Además, se cuantifica el impacto, para el caso en el que la amenaza se materializase.

Dado que los activos se encuentran jerarquizados y se encuentran establecidas las relaciones de dependencia entre los activos de las diferentes categorías, se debe conseguir de forma explícita documentar la "cadena de fallo" en caso de un incidente de seguridad.

La experiencia y la sucesiva revisión de la información generada en estudios de riesgos anteriores permitirán ajustar de forma más exacta las diferentes

dependencias entre activos. Con toda esta información, se tiene una estimación del costo que podría producir la materialización de una amenaza sobre un activo. Teniendo en cuenta las relaciones funcionales y de dependencias entre activos, se hallan los valores de riesgo.

Gestión de riesgos: En esta fase, se procede a la interpretación del riesgo.
Una vez identificado los puntos débiles, deben seleccionarse el conjunto de funciones de salvaguarda que podrían ser usados para disminuir los niveles de riesgo a los valores deseados. Para ello, deberán especificarse los mecanismos de salvaguarda que se encuentran implantados hasta ese momento y cuál es su grado de cumplimiento.

Este proceso se ayuda de la simulación. Se van probando selecciones de diferentes mecanismos de salvaguarda y se estudia en qué medida reducen los niveles de riesgo a los márgenes deseados. Es muy importante realizar las correctas estimaciones de la efectividad de los diferentes mecanismos de salvaguarda para ajustar de forma precisa los valores de riesgo.

Selección de mecanismos de salvaguarda: Una vez obtenidos estos resultados, se establece de nuevo reuniones con el equipo responsable del proyecto de la organización en estudio. De esta forma, se analizan los resultados obtenidos y se establece un plan de implantación de mecanismos.

1.6.4 COSO (Sponsoring Organizations of the Treadway Commission). COSO inicio en 1985 recomendando que las organizaciones patrocinadoras de la Comisión trabajen juntas para desarrollar sistemas integrados de orientación sobre el control interno. These five organizations formed what is now called the Committee of Sponsoring Organizations of the Treadway Commission.

El modelo COSO define el control interno como un conjunto de procesos, realizado por los directivos de una organización, y creado para garantizar el logro de los objetivos.

COSO consta de cinco elementos, estos elementos proporcionan un marco eficaz para describir y analizar el sistema de control interno, los cuales son:

1.6.4.1 Entorno de control. Sirve como base para los demás componentes del control interno, proporcionando disciplina y estructura. El entorno de control tiene una incidencia generalizada en las actividades de la organización, influye sobre las actividades de control, los sistemas de información y comunicación y en la supervisión.

La base fundamental del entorno de control está determinada por el personal y su nivel de concientización sobre éste, es por ello que las organizaciones se esfuerzan por tener recursos competentes e inculcan un sentido de integridad y

control. A tal efecto establecen políticas y procedimientos adecuados, y a menudo con un código de conducta escrito.

"Debe considerarse en la evaluación que los procedimientos existan, que hayan sido apropiadamente notificados, que sean conocidos, que sean adecuadamente comprendidos y que exista evidencia de que se aplican."[15]

1.6.4.2 Evaluación del riesgo. Cada empresa se enfrenta a una variedad de riesgos de fuentes externas e internas que deben ser evaluados. Una condición previa para la evaluación de riesgos es el establecimiento de objetivos y por lo tanto la evaluación de riesgos es la caracterización y análisis de los riesgos relevantes para la consecución de los objetivos asignados. "La evaluación de riesgos es un requisito previo para establecer cómo los riesgos deberían ser manejados, dado que estos afectan a la supervivencia y éxito de la empresa. Es imposible reducir el riesgo a cero, es por ello que la dirección determina cual es el nivel de riesgo aceptable".[16]

1.6.4.3 Las actividades de control. Las actividades de control son las políticas y procedimientos que ayudan a asegurar el cumplimiento de las directrices establecidas por la dirección para controlar los riesgos que pueden obstaculizar el logro de los objetivos de la institución. Las actividades de control se originan en toda la organización, en todos los niveles y en todas las funciones. Estos incluyen una amplia gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de desempeño operativo, la seguridad de los activos y la separación de funciones.

Las actividades de control se dividen en tres categorías en función al objetivo relacionado:

Operaciones.

Fiabilidad de la información financiera.

Cumplimiento de la legislación.

"Los tipos de control afectan a diversas áreas. En función a las circunstancias, una actividad de control puede ayudar a alcanzar los objetivos correspondientes a

[15] http://www.mercadotendencias.com/informe-coso-entorno-de-control/
[16] http://www.mercadotendencias.com/informe-coso-evaluacion-de-los-riesgos/

diversas categorías, es decir que por ejemplo los controles operacionales pueden contribuir a la fiabilidad de la información financiera."[17].

1.6.4.4 Información y comunicación. "Actualmente dada la facilidad y la disponibilidad, las organizaciones tienen acceso a un gran caudal de datos, existen algunos que son útiles y relevantes para la empresa y para la realización de los objetivos propuestos por ésta. Esa gran base de datos, al ser útil para la organización pasa a ser información necesaria para la consecución de sus actividades y fines. La información recogida debe ser relevante para la gestión del negocio, además de ser clara y oportuna."[18].

Los sistemas de información juegan un papel importante en los sistemas de control interno que producen los informes, incluidos los operativos, financieros y el cumplimiento de información relacionada, que permiten elaborar y controlar la institución. De manera más amplia, la comunicación eficaz debe garantizar los flujos de información hacia abajo, y hasta a través de la organización.

1.6.4.5 Seguimiento. Los sistemas de control interno deben ser supervisados, un proceso que evalúa la calidad del desempeño del sistema en el tiempo. Esto se logra a través de continuas actividades de supervisión o evaluaciones por separado. Las fallas de control interno detectadas a través de estas actividades deberían notificar las medidas de planificación y correctivas garantizando la mejora continua del sistema.

Algunas diferencias entre COSO y COBIT, que son los dos modelos más difundidos actualmente son:

El modelo COSO está enfocado a toda la empresa, mientras que el COBIT se limita a las tecnologías de la información (TI).

El COBIT establece como uno de sus objetivos la seguridad de la información, por el contrario COSO, no lo toma en cuenta en su evaluación.

El modelo de control interno que presenta el COSO no es muy completo, a diferencia de la metodología COBIT que contempla políticas, procedimientos y estructuras organizativas, además de procesos para definir el modelo de control interno.

1.6.5 MECI - Modelo Estándar de Control Interno: Es una herramienta de gestión que busca unificar criterios en materia de control interno para el sector

[17] http://www.mercadotendencias.com/informe-coso-actividades-de-control/
[18] http://www.mercadotendencias.com/informe-coso-informacion-y-comunicacion/

público, estableciendo una estructura para el control a la estrategia, la gestión y la evaluación.

Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el fin de orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado.

Principios:

1. Autorregulación: Establecer de manera participativa las normas, procesos y procedimientos bajo un entorno de integridad, eficiencia y transparencia en la actuación pública.

2. Autogestión: Interpretar, coordinar y aplicar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada.

3. Autocontrol: Es la capacidad de cada servidor público, independientemente de su nivel jerárquico, para controlar su trabajo, detectar desviaciones, efectuar correctivos y garantizar los resultados que se esperan en el desarrollo de su función.

Base técnica y aplicada:

1. Se fundamenta en la construcción de una Ética Institucional.
2. Toma como base modelos internacionales de Control Interno-COSO.
3. Se orienta a la prevención de riesgos.
4. Se hace efectivo en una Organización por Procesos.
5. Encauza la Organización Pública hacia un Control corporativo permanente.
6. Dispone la entidad hacia una medición de la gestión en tiempo real.
7. Enfatiza la generación de información suficiente, pertinente, oportuna, de utilidad organizacional y social.
8. Controla la efectividad de los procesos de Comunicación Pública y Rendición de Cuentas.
9. Fortalece la función de Evaluación Independiente a la Gestión.
10. Se orienta hacia la estandarización de metodologías y procedimientos de Evaluación del CI y de Auditoría.
11. Otorga alto nivel de importancia a los Planes de Mejoramiento.

Objetivo general del modelo:

Establecer las políticas, los métodos y mecanismos de prevención, control, evaluación y de mejoramiento permanente de la entidad pública, que le permiten el cumplimiento de sus objetivos institucionales y la finalidad social del Estado en su conjunto.

Objetivos específicos:

De Control Estratégico:

1. A la existencia y Cumplimiento de acuerdos o protocolos éticos.
2. Control Organizacional
3. Control al Planeamiento
4. Control a la Gestión Humana
5. Prevención de Riesgos

De Control de Ejecución:

1. Generación de políticas de ejecución.
2. Control a la operación de la entidad.
3. Orientado al diseño y generación de acciones y mecanismos de autocontrol y auto-evaluación**.**

De Control de Evaluación:

1. Seguimiento a la gestión.
2. Verificación y evaluación permanente de C.I.
3. Evaluación independiente del SCI y de auditoría interna
4. Mejoramiento continúo de la gestión y capacidad de respuesta a los grupos de interés.
5. Integración de las observaciones de los órganos de control a las acciones de mejoramiento.

De Control de Cumplimiento:

1. Verificación al cumplimiento de la función constitucional, leyes y normas vigentes.
2. Obligaciones de información frente a los diferentes grupos de interés.
3. Rendición de cuentas.
4. Cumplimiento de obligaciones ante el gobierno nacional.
5. Cumplimiento de obligaciones ante los órganos de Control externo.
6. De cumplimiento al Control Fiscal.

De Control de Información

1. Generación de mecanismos para producir información base para reportes
2. Generación de información legalmente establecida por los diferentes órganos de control.
3. Información legalmente obligatoria proveniente de la autorregulación, que garantice la rendición de cuentas públicas.

Etapas de desarrollo:

Etapa 1: Planeación del diseño e implementación del Modelo.
Etapa 2: Diseño e implementación del Modelo.
Etapa 3: Evaluación a la implementación del Modelo.
Etapa 4: Elaboración del Nomograma.

2. DESARROLLO DE AUDITORIA

2.1 METODOLOGÍA

Para realizar la auditoría externa al Sistema de Información de la Institución Prestadora de Servicio de Salud Indígena Guáitara, donde se utilizo una metodología tipo de investigación cuantitativa, ya que permite examinar los datos de manera científica, o de manera más específicamente en forma numérica, generalmente con ayuda de herramientas del campo de la estadística.

Es responsabilidad de la dirección el contenido de la información suministrada por la institución y analizada por el equipo auditor conformado por los estudiantes Julio Cesar Burgos Chaguezac y Nelson Andrés Cortes Bernal.

Para alcanzar los objetivos propuestos, se utilizo la metodología de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del equipo auditor, también, se estudian y aplican conceptos y esquemas teóricos, también cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas para tener un funcionamiento de calidad.

La auditoría realizada por el equipo auditor fue dividida en varias etapas así:

FASE I: **CONCEPTUALIZACIÓN**

En esta fase se realiza la recolección, clasificación y análisis de información sobre tipos de auditoría y técnicas de auditoría de sistemas.

FASE II: PLANEACIÓN

En la fase de planeación se realizan las siguientes actividades:

Identificar el alcance y los objetivos de la auditoria a realizar.
Realizar el estudio inicial en la institución tomada como caso de estudio.
Determinar los recursos necesarios para realizar la auditoria.
Elaboración del plan de trabajo.

FASE III: REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

En esta etapa del proyecto se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. Se realizan las siguientes actividades:

Elección de los procesos a auditar.
Ejecución de la auditoria.
Elaboración de un análisis de Hallazgos y riesgos que permitan identificar cuáles de las actividades identificadas tienen una menor eficiencia, cuáles de los procesos tienen mayor impacto dentro del sistema.
Elaboración del informe con los Hallazgos encontrados, detectando las causas y su efecto.
Elaboración del modelo de madurez en el cual se encuentra el sistema auditado.
Elaboración del informe final.

FASE IV: PRESENTACIÓN DEL INFORME FINAL

En esta etapa del proceso se presentará ante directivas de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”, la sustentación y presentación del informe donde se darán a conocer los problemas encontrados y se establecerán posibles soluciones.

2.2 ARCHIVO PERMANENTE

El archivo permanente contiene información constante. Esta información es de vital importancia y se considera necesaria para comprender en forma exacta, rápida y sencilla las características de las áreas objeto de auditoría.

2.2.1 Decreto comunes. Para la institución auditada se tuvo en cuenta el decreto que se cita a continuación.

Decreto 1360 de 1989 “Por el cual se reglamenta el soporte lógico (software) en el registro nacional de derechos de autor”.

2.2.2 Ambiente general de la institución.

Nombre de la institución: INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”

NIT: 900056747-9

Figura 2. Logotipo de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”

LOGOTIPO

Fuente: Portafolio de la entidad IPS Guáitara.

2.2.3 Reseña histórica. La INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”, nació a la vida jurídica en el año 2005, gracias al interés demostrado por los gobernadores indígenas de los resguardos de Ipiales, San Juan y Yaramal, habilitando los servicios de medicina general, odontología, enfermería, servicio farmacéutico, con el objeto social de salvaguardar la salud de la comunidad indígena del municipio de Ipiales, precisamente el día 15 de diciembre de 2005 se obtiene el registro de habilitación numero 5235601166 por parte del Instituto Departamental de Salud de Nariño, pero, es a partir del primero de abril del año 2006 cuando a través de un contrato de capitación para cuatro mil quinientos afiliados a la empresa EMSSANAR, cuando arranca a prestar los servicios de primer nivel menesteres.

Para el año 2007 logramos que la EPS EMSSANAR, contratar con la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”, un total de 6500 afiliados correspondientes en un 90 % al resguardo indígena de Ipiales, y en un 10 % del resguardo indígena de Yaramal, situación que nos permitió llegar hasta el 30 de abril del 2008, donde por diferentes razones conocidas por todos, la empresa antes mencionada nos suspenderá el contrato de

capitación pactada y es a partir del mes de mayo cuando empezamos a prestar nuestros servicios a la empresa MALLAMAS EPSI atendiendo a 3589 afiliados bajo un contrato de modalidad capitado suscrito hasta el 31 de diciembre de 2008 a la empresa SALUD CONDOR EPS con 3354 afiliados bajo un contrato también de modalidad capitado con vigencia entre 1 de mayo de 2008 hasta 31 de marzo de 2009.

2.2.4 Misión. Somos una institución prestadora de servicios de salud que garantiza la atención del primer nivel con calidad a toda la población indígena del Municipio de Ipiales; orientada a mantener una población saludable; optimizando recursos humanos, económicos y tecnológicos comprometidos con el mejoramiento continuo generando fuentes de trabajo en nuestra región.

2.2.5 Visión. Seremos una empresa reconocida como una institución líder en su modelo de atención especial para las comunidades indígenas, prestando servicios de salud integral con humanismo, calidad y confianza generada a través de nuestros trabajadores, usuarios y proveedores.

2.2.6 Organización administrativa:

Figura 3. Organigrama de la institución prestadora de servicios de salud indígena Guáitara

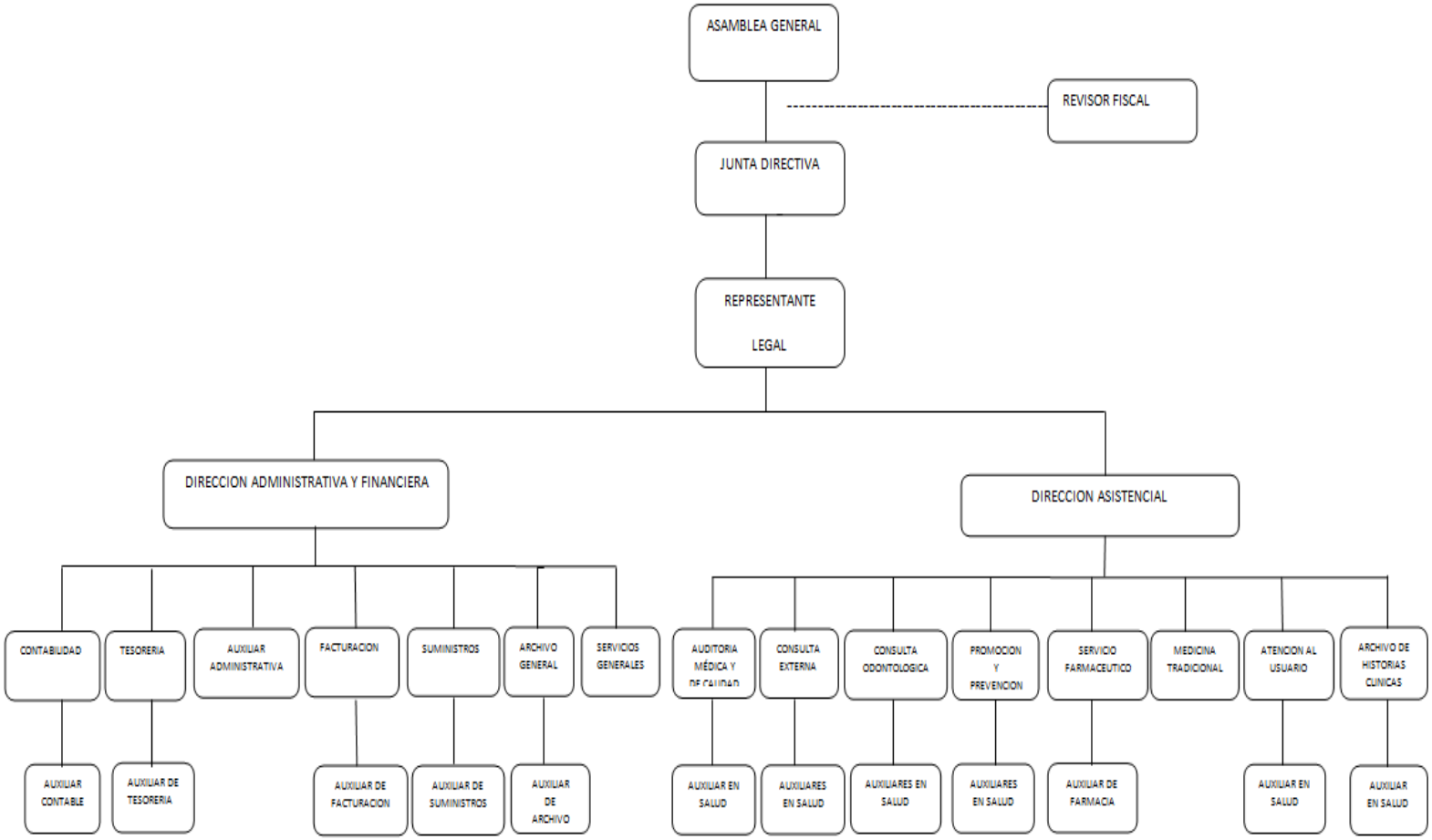
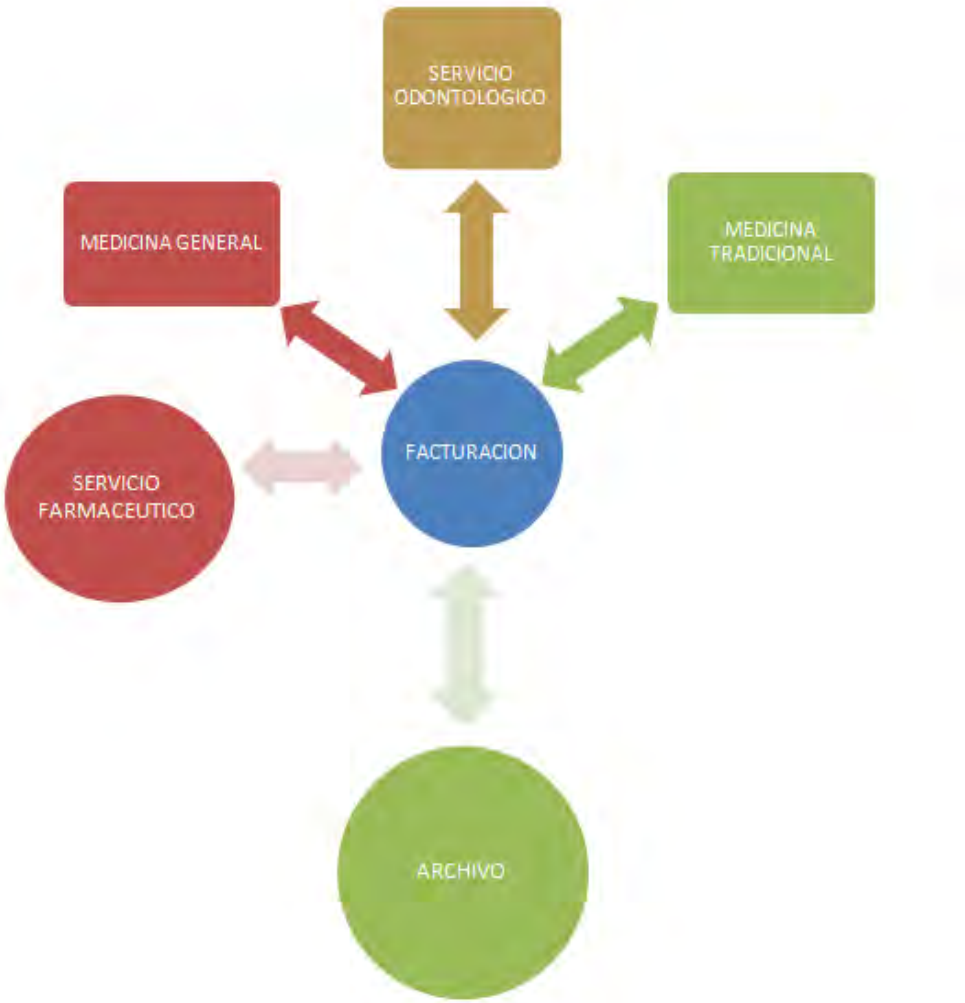


Figura 4. Estructura Orgánica de Sistema de Información de la Institución Prestadora de Servicios de Salud Indígena Guáitara.



2.2.7 Manual de funciones. A continuación se presenta el manual de funciones de la empresa de los cuales se tendrá en cuenta el manejo de la información en de las dependencias facturación, servicio farmacéutico, archivo, contabilidad y suministro de activos fijos.

I. IDENTIFICACIÓN DEL CARGO

Asamblea general
Denominación del cargo: Miembros de la asamblea general
No. de Cargos: Treinta y cinco (35)
Dependencia orgánica: Área administrativa

II. OBJETO DEL CONTRATO

La Asamblea General se constituye como órgano de dirección dentro de la IPS DE SALUD INDÍGENA GUÁITARA, dictara decisiones las cuales son de obligatorio cumplimiento, siempre que se hayan adoptado de conformidad con la Constitución Política, Las Leyes, Los estatutos y las formas y procedimientos de las comunidades del resguardo indígena de Ipiales.

III. FUNCIONES

1. Establecer las orientaciones, políticas y directrices generales de la IPS DE SALUD INDÍGENA "GUÁITARA", para el cumplimiento de su objeto social, de conformidad con las particularidades étnicas y culturales de la comunidad.

2. Analizar los informes de los órganos administrativos y control.

3. Examinar, modificar, aprobar, o improbar las cuentas, los estados financieros básicos y el proyecto de distribución de excedentes de la junta directiva presente acompañado de un informe especial. Estos documentos deben reposar en la secretaria ocho (8) días antes a la reunión para que los miembros puedan examinarlos y tomar nota de ellos.

4. Fijar contribuciones extraordinarias, siempre y en todo caso con destinación especifica.

5. Nombrar al Revisor Fiscal y su suplente, fijar su remuneración cuando hubiere lugar.

6. Conocer en única instancia casos de mantener el orden público, disponibilidad de miembros de la Junta Directiva y del Revisor Fiscal, lo mismo que de conflictos entre estos y adoptar las medidas oportunas
7. Delegar funciones en junta directiva cuando lo estime conveniente.

8. Las demás que señalen la Ley y los Estatutos Institucionales.

IV. REQUISITOS

Personas mayores de edad pertenecientes al Resguardo Indígena de Ipiales, siempre y cuando no se hallen excluidos de los derechos y beneficios del Resguardo de conformidad con usos y costumbres y no hayan atentado contra los intereses de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA "GUÁITARA".

Los miembros de la Asamblea General aunque ejercen funciones públicas a favor de la comunidad que representan y particularmente de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA "GUÁITARA", no adquieren vinculación laboral o contractual alguna con esta última, ni obtendrán por dicha circunstancia remuneración de ninguna clase.

I. IDENTIFICACIÓN

Junta Directiva
Denominación del Cargo: Miembros de la junta directiva
No. de Cargos: Nueve (9)
Dependencia orgánica: Área Administrativa
Dependencia Jerárquica: Asamblea General

II. OBJETO DEL CONTRATO

La Junta Directiva, dentro de los parámetros legales dictara instructivos donde se consagren los términos de operación en la prestación de los servicios de salud y todas disposiciones a tener en cuenta para garantizar sus adecuada y oportuna prestación y el normal funcionamiento en todos los procesos adoptados por la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA "GUÁITARA" Formulación y adopción de políticas, planes, programas y proyectos de ejecución en la IPS. Ejercerá la dirección y representación legal de la institución.

III. FUNCIONES

1. Aprobar y fijar la planta de personal con base en el estudio de las necesidades del recurso humano que exige INSTITUCIÓN PRESTADORA DE

SERVICIOS DE SALUD INDÍGENA “GUÁITARA”, para funcionar y prestar adecuadamente y en forma eficiente los servicios y los programas de actividades a desarrollar en lo económico y social, con fundamento en las funciones, los procesos y procedimientos a desarrollar, la clasificación y la remuneración de los empleos.

I. IDENTIFICACIÓN

Representante Legal
Denominación del Cargo: Representante Legal
No. de Cargos: Uno (1)
Dependencia orgánica: Área Administrativa
Dependencia Jerárquica: Junta Directiva

II. OBJETO DEL CONTRATO

Formulación y adopción de políticas, planes, programas y proyectos de ejecución en la IPS. Ejercerá la dirección y representación legal de la institución.

III. FUNCIONES

1. Llevar la representación legal, judicial y extrajudicial de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”.

2. Suscribir los contratos laborales del personal que haya seleccionado para prestar servicios en la institución.

3. Suscribir los contratos que deba celebrar la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA” y velar por el cumplimiento respectivo.

4. Convocar a reuniones extraordinarios a la Junta Directiva de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”.

5. Participar en las reuniones ordinarias o extraordinarias que se lleven a cabo por la Junta Directiva, con voz pero sin voto.

6. Revisar en coordinación con el Director Asistencial y la Junta Directiva, los reglamentos internos, los programas de trabajo acordados y supervisar la ejecución de los mismos.

Apoyar la resolución de dificultades en interpretación o aplicación de los Estatutos Institucionales, con el apoyo del Director Asistencial, la Junta Directiva y el Asesor Jurídico.

8. Solicitar autorización a la junta directiva para suscribir contratos cuya cuantía exceda los veinte (20) salarios mínimos mensuales legales vigentes.

9. Asumir y dar cuenta de todos los litigios que surjan en el desarrollo de las actividades de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA "GUÁITARA", y construir apoderados judiciales para la defensa de los intereses de la I:P:S.

10. Girar y firmar cheques, cuentas y documentos para pago, de acuerdo con el orden establecido y la liquidez de la institución.

11. Velar porque el componente del sistema de control interno esté establecido en las funciones de todos los cargos de la empresa.

12. Vela por el desarrollo de personal teniendo en cuenta, la capacitación, el entrenamiento y el bienestar social.

13. Diseñar, proponer, aplicar y velar por el cumplimiento del sistema de estimulo y motivación del personal.

14. Realizar la planeación estratégica del talento humano requerido en la institución.

15. Participar en los aspectos relacionados con la administración de salarios e incentivos financieros vigentes para institución.

16. Presentar reporte de novedades del personal de la I.P.S. para liquidación de contratos y nómina.

17. Velar por la aplicación y registro del sistema de evaluación de desempeño, que apunte al logro de resultados esperados por la institución y promueva el auto control y el mejoramiento continuo.

18. Velar por la aplicación del régimen disciplinario en coordinación con los jefes de las dependencias.

19. Proponer y desarrollar esquemas y manuales de valoración de empleos, requisitos mínimos, funcionales por cargo y escalas de remuneración, dirigidos a promover la productividad institucional.

20. Velar por el mantenimiento de un nivel óptimo de capacidad y habilidad de talento humano bajo la óptica de los objetivos organizacionales.

21. Dirigir el diseño y rediseño de los puestos de trabajo de la institución, de tal forma que se logre aumento en la productividad, el control de riesgos ocupacionales, el desarrollo de las personas y una adecuada calidad de vida laboral.

22. Forma parte de la comisión encargada de establecer las especificaciones y características de los implementos de dotación para los funcionarios de la institución.

23. Conjuntamente con el equipo de trabajo identificar la Misión, Visión, Valores, Objetivos, factores claves de éxito de la institución.

24. Trabajar coordinadamente con los Jefes de División, de Selección, Coordinadores de áreas y participantes activamente de los grupos de mejoramiento y de calidad que se constituyan en la institución.

25. Las demás que prevén los estatutos institucionales y las que por delegación le encarguen la Junta Directiva.

I. IDENTIFICACIÓN DEL CARGO

Facturación
Denominación del cargo: Auxiliar de facturación
No. de Cargos: Uno (1)
Dependencia Orgánica: Dirección Administrativa
Dependencia Jerárquica: Director Administrativo

II. OBJETO DEL CONTRATO

Ejecución de labores auxiliares en las áreas de facturación, admisiones, elaboración, consolidación y control de los servicios prestados por la IPS La Asamblea General se constituye como órgano de dirección dentro de la IPS.

III. FUNCIONES

1. Atender y orientar a las personas en relación con sus necesidades y expectativas de acuerdo con políticas institucionales y normas de salud.

2. Admitir al usuario en la red de servicios de salud según niveles de atención y normatividad vigente.

3. Facturar la prestación de los servicios de salud según normatividad y contratación.

4. Generar actitudes y prácticas saludables en los ambientes de trabajo.

Manejar valores e ingresos relacionados con la operación del establecimiento.

6. Elaborar las facturas y demás documentos o formatos que generen ingresos económicos en el sitio de trabajo y que impliquen la prestación de servicios (Centro de Cobros).

7. Recolectar, verificar y procesar la información necesaria par al elaboración de las cuentas de de la y anexar la documentación de la atención con las especificaciones que se ameriten.

8. Seleccionar, organizar y analizar la documentación según el manual de normas y procedimientos vigentes en la institución.

9. Apoyar al suministro y conservación de la información requerida por el sistema de información existente en la institución y velar por la adecuada utilización y funcionamiento de los equipos de cómputo.

10. Las demás actividades afines que le sean asignadas.

IV. REQUISITOS

ESTUDIOS: Aprobación de seis años de Educación Secundaria.
Conocimientos básicos en sistemas.

EXPERIENCIA:
Un (1) año mínimo de experiencia en el área.

I. IDENTIFICACIÓN DEL CARGO

Almacén
Denominación del cargo: Almacenista
No. de Cargos: Uno (1)
Dependencia orgánica: Dirección Administrativa
Dependencia Jerárquica: Director Administrativo

II. OBJETO DEL CONTRATO

Recepción, distribución y entrega de los elementos requeridos por las Áreas de la institución.

III. FUNCIONES

1. Colaborar con el adecuado almacenamiento de las mercancías en el desarrollo de los programas, proyectos y actividades de las diferentes dependencias, así como coordinar el oportuno suministro de elementos en la institución.

2. Coordinar la elaboración de un programa de recibo y entrega de mercancías y elementos.

3. Colaborar con las labores relacionadas con la adquisición, almacenamiento y distribución de los suministros requeridos en la institución.

4. Coordinar el adecuado control de los inventarios y de los activos devolutivos.

5. Velar por la adecuada entrega de los suministros necesarios y velar por la racional utilización de los mismos en las diferentes áreas.

6. Hacer entrega de las dotaciones de los empleados que por Ley tienen derecho, en coordinación con el Director Administrativo.

7. Responsabilizarse por el desarrollo e implementación de las políticas Gerenciales en Salud Ocupacional establecidas para la institución.

8. Responsabilizarse por si mismo (AUTOCONTROL) aplicación de los métodos y procedimientos del sistema de Control Interno.

IV. REQUISITOS

EDUCACIÓN: Diploma de bachiller en cualquier modalidad.
EXPERIENCIA: Un (1) año mínimo de experiencia relacionada.

I. IDENTIFICACIÓN DEL CARGO

Oficina administrativa
Denominación del cargo: Auxiliar Administrativo
No. de Cargos: Uno (1)
Dependencia orgánica: Área Administrativa
Dependencia Jerárquica: Director Administrativo

II. OBJETO DEL CONTRATO

Ejecución de labores de oficina y de asistencia administrativa.

III. FUNCIONES

1. Ejecución de labores de secretariado, de mecanografía, de actas, de notas, cartas, memorandos, informes, lo mismo que los asuntos tratados en reuniones, conferencias.

2. Preparar el material requerido y citar según las indicaciones dadas, a los comités y a las reuniones, conferencias.

3. Velar por la buena imagen de la institución y por la calidez en la atención a los clientes externos e internos.

4. Redactar oficios y correspondencia de acuerdo con las instrucciones recibidas y los manuales y normas y procedimientos existentes en la institución.

5. Proporcionar la información requerida por el público y concertar las entrevistas solicitadas.

6. Archivar la correspondencia y otros documentos de la dependencia de acuerdo con las normas establecidas en la Institución.

7. Ejecutar y recibir llamadas telefónicas transmitiendo o recibiendo los mensajes correspondientes.

8. Guardar la debida reserva y discreción con la información de la institución y especialmente de la dependencia.

9. Apoyar el suministro y conservación de la información requerida por el sistema de información existente en la institución y velar por la adecuada utilización y funcionamiento de los equipos de cómputo.

10. Las demás actividades afines que le sean asignadas.

IV. REQUISITOS

EDUCACIÓN: Titulo de bachillerato técnico comercial y conocimientos en el manejo de procesador de texto y hojas electrónicas.
EXPERIENCIA: Tres años de experiencia relacionada.

I. IDENTIFICACIÓN DEL CARGO

Servicios Generales
Denominación del cargo: Vigilante
No. de Cargos: Dos (2)
Dependencia orgánica: Servicios Generales
Dependencia Jerárquica: Director Administrativo

II. OBJETO DEL CONTRATO

Ejecución de labores de vigilancia y portería de la IPS.

III. FUNCIONES

1. Prestar los servicios de vigilancia y responder por los bienes, e inmuebles a su cargo.

2. Revisar los vehículos o paquetes que entres o salgan de la Institución de acuerdo a las instrucciones recibidas.

3. Cuidar que las puertas y ventanas de las diferentes dependencias queden debidamente aseguradas cuando se retire el personal.

4. Atender a los usuarios internos y externos en forma respetuosa, suministrando información que le soliciten y que se le haya autorizado.

5. Permanecer en el lugar de trabajo que se le asigne.

6. Velar que las personas porten su identificación en un lugar visible.

7. Responder por el manejo adecuado del arma de dotación a su cargo.

8. Reportar oportunamente a los superiores las situaciones irregulares, de riesgo o emergencia que se presente en el área y en el turno.

9. Hacer entrega y recibo del libro de cambios de turno observando el adecuado registro de las novedades y verificación de los elementos a su cargo.

10. Colaborar con el buen funcionamiento de los equipos o sistemas de agua, luz, durante la ausencia del personal a cargo.

11. Cumplir las normas de presentación personal y hacer cumplir aquellas establecidas en el área.
12. Las demás que le asigne y sean afines con la naturaleza del cargo.

IV. REQUISITOS

EDUCACIÓN: Dos (2) años de educación básica secundaria o educación básica primaria completa.

EXPERIENCIA: Sin experiencia

I. IDENTIFICACIÓN DEL CARGO

Director Asistencial
Denominación del cargo: Director asistencial
No. de Cargos: Uno (1)
Dependencia orgánica: Área Administrativa
Dependencia Jerárquica: Representante Legal

II. OBJETO DEL CONTRATO

Coordinador y Administrador de la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA", Ejecutor de las resoluciones de la Junta Directiva.

Tendrá a su cargo el manejo, orientación y dirección de los empleados de la institución.

III. FUNCIONES

1. Administrar con eficiencia la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA", de conformidad con las directrices y orientaciones de la junta Directiva y los Estatutos institucionales.

2. Responder por las prestaciones de servicios de salud en los términos previstos en los estatutos institucionales y prestar sus servicios profesionales a la población que lo requiera, de conformidad con las disponibilidades establecidas previamente.

3. Coordinar la ejecución de planes, programas y proyectos aprobados por la Junta Directiva.

4. Rendir oportunamente informes legales, estatutarios y ocasionales, asesorar y presentar iniciativas relacionadas con el objeto social a la junta directiva

5. Dirigir la planta de personal vinculada a la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA".

6. Proyectar el presupuesto anual, presentarlo a estudio a la Junta Directiva y cuando haya sido expedido, ejecutarlo con sujeción a las normas respectivas, con eficiencia y transparencia absoluta y dentro de las políticas señaladas para efecto.

7. Dirigir y controlar en coordinación con las áreas correspondientes, la prestación de los servicios de salud a la población, atender sus reclamaciones y velar por su debida atención, y en general, por que se cumplan las tareas administrativas y los objetivos de la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA".

8. Promover y coordinar la elaboración del Manual de Funciones, requisitos y reglamentos relacionados con los Estatutos Institucionales, los procesos y procedimientos de la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA" y de los demás que juzgue convenientes y someterlos a consideración de la Junto Directiva y una vez aprobados por ésta, cumplirlos y hacerlos cumplir.

9. Mantener comunicación permanente con las comunidades y sus autoridades, atender la información general que precisen en coordinación con las áreas respectivas de la Institución, y facilitarles información sobre los servicios que presta la institución y recoger las opiniones y sugerencias que formulen los afiliados.

10. informar al la Junta Directiva y al Representante Legal sobre el comportamiento, rendimiento y necesidades del personal, con el fin de que se tomen decisiones dirigidas a nombrar y remover libremente a los empleados de la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA", de acuerdo a la Planta de Personal aprobada por la Junta Directiva, previo estudio de los contratos de trabajo, las necesidades de la organización en materia de personal.

11. Velar porque todas las personas al servicio de la INSTITUCIÓN PRESTADORA DE SERVICIO DE SALUD INDÍGENA "GUÁITARA", cumplan estrictamente con sus obligaciones y sancionarlas en caso de infracción, dando cuenta cuando así se lo solicite la Junta Directiva.

12. Formular la política de capacitación de los talentos humanos de la empresa de acuerdo a las necesidades del sistema de salud, las exigencias de la interpretación docente – asistencial y los requerimientos de la institución.

13. Coordinar que las funciones de los cargos de las personas que conforman el equipo de trabajo a cargo y procurar la obtención de su compromiso, motivación y sentido de pertenencia.

14. Mantener informados y actualizados a los funcionarios que conforman el equipo de trabajo a cargo y procurar la obtención de su compromiso, motivación y sentido de pertenencia.

15. Programar reuniones de trabajo en forma periódica, que fomente la participación, la comunicación y el dialogo dentro del equipo. Estas reuniones deben tener una agenda de trabajo prevista.

16. las demás propias de la Dirección Asistencial y las que le encomienden la Junta Directiva.

IV. REQUISITOS

EDUCACIÓN:
1. Ser profesional en el área de salud.
2. Poseer conocimiento y experiencia profesional mínima de tres años.
3. Certificado de antecedentes disciplinarios vigentes, expedido por la Procuraduría General de la Nación.
4. Tener disponibilidad exclusiva para el desempeño del cargo.

EXPERIENCIA: Sin experiencia

2.2.8 Inventario de equipos de cómputo.

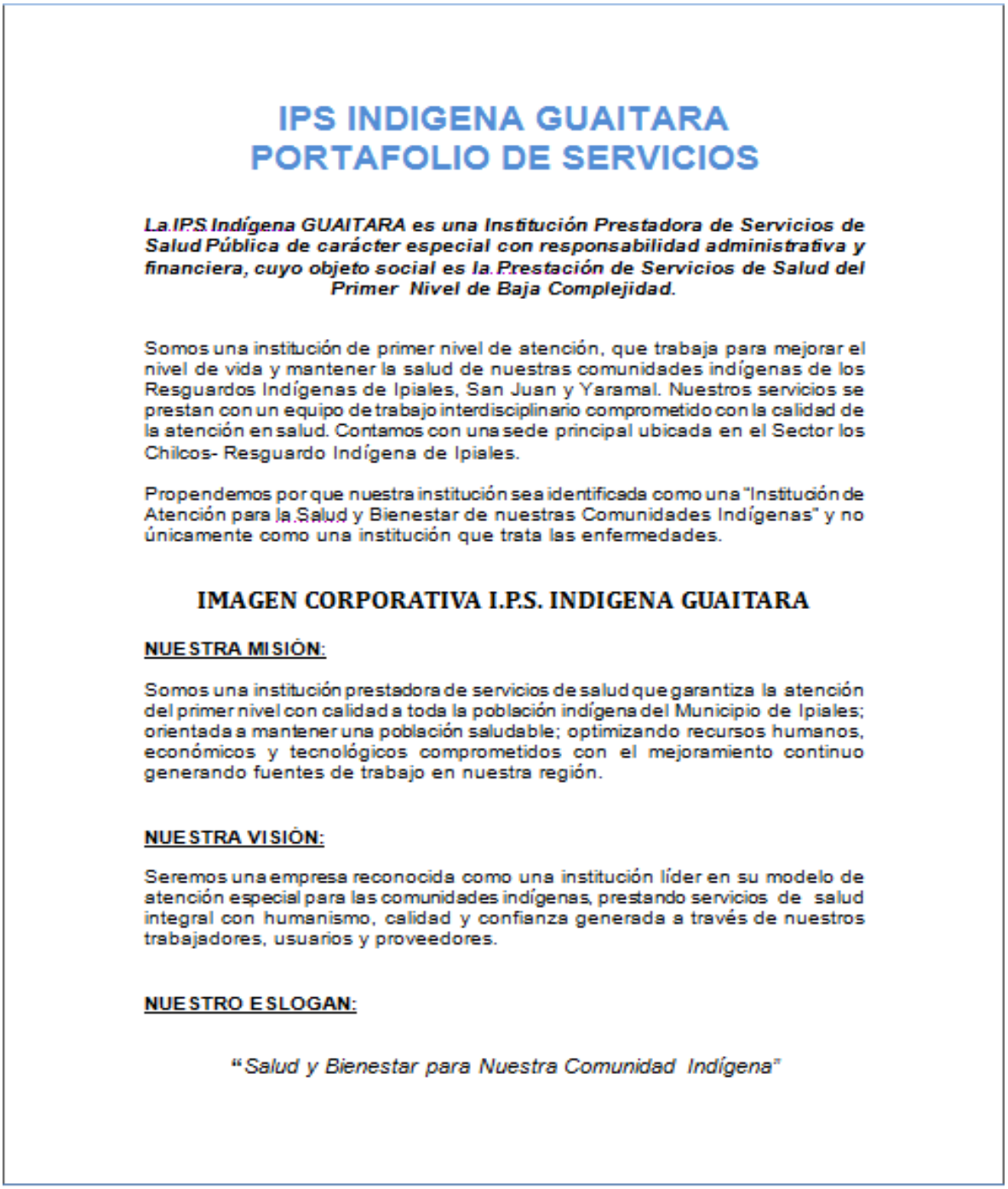
Figura 5. Inventario de equipos de cómputo.

DEPENDENCIA	FECHA DE ADQUIS	INVENTARIO	MARCA	N°	PRECIO	CODIGO	ESTADO
ENFERMERIA	01/01/2006	COMPUTADOR CPU TECLADO Y MOUSE PANTALLA		1	250.000	83151004	REGULAR
SERVICIO FARMACEUTICO	03/04/2009	C.P.U. MONITOR COLOR NEGRO, TECLADO Y MAUS GENIUS REGULADOR	LG	1	1.800.000	167002	BUENO
ATENCION AL USUARIO	17/09/2009	CPU CON QUEMADOR LG MONITOR SAMSUNG SYNCMASTER 943SNX SERIE MY19H9LS408476 18,5 TECLADO Y MOUSE GENIUS	SAMSUNG	1	1.310.000	167002	BUENO
ARCHIVO HISTORIAS CLINICAS	17/09/2009	CPU CON QUEMADOR LG MONITOR SAMSUNG SYNCMASTER 943SNX SERIE MY19H9LS4084520, 2 PARLANTES NEXT,	SAMSUNG	1	1.310.000	167002	BUENA
AUXILIAR ADMINISTRATIVA	11/09/2010	C.P.U COLOR NEGRO CON GRIS PHOENX QUEMADOR LG PANTALLA SAMSUNG TECLADO Y MOUSE GENIUS REGULADOR	PHOENX	1	1.347.150	167002	BUENO
ATENCION AL USUARIO - SATELITE	06/09/2010	CPU COLOR NEGRO CON GRISTECLADO Y MOUSE GENIUS PANTALLA PLANA		1	1.347.000	167002	BUENO
FACTURACION - SATELITE	06/10/2010	C.P.U COLOR NEGRO 2 PARLANTES MOUSE Y TECLADO GENIUS PANTALLA PLANA		1	1.347.000	167002	BUENO
SERVICIO FARMACEUTICO - SATELITE	01/01/2006	C.P.U COLOR NEGRO CON GRIS NEX MONITOR SAMSUNG MOUSE Y TECLADO COLOR NEGRO		1	230.000	83151004	BUENO
TESORERIA	21/01/2011	EQUIPO DE COMPUTO BOARD ASROCKCHIP INTEL H55 TORRE MINI ATX DE LUJO MONITOR LCD 18.5 SAMSUNG COMBO TECLADO Y MOUSE GENIUS CAMARA WED GENIUS Accesorios	PROCESADOR INTEL CORE 13	1	1.243.524	167002	BUENO
CONTABILIDAD	21/01/2011	EQUIPO DE COMPUTO BOARD ASROCKCHIP INTEL H55 TORRE MINI ATX DE LUJO MONITOR LCD 18.5 SAMSUNG COMBO TECLADO Y MOUSE GENIUS CAMARA WED GENIUS Accesorios REGULADOR ASC 1000W FORROS, PAD	PROCESADOR INTEL CORE 13	1	1.243.524	167002	BUENO
REPRESENTANTE LEGAL	04/04/2011	COMPUTADOR PORTATIL HP G42-362LA	CNF0458121	1	1.099.000	167002	BUENO
BODEGA		COMPUTADORES PILLIPS		2			
CONTABILIDAD		COMPUTADOR SANSUNG		1			

Fuente: Inventario suministros IPS Indígena Guáitara

2.2.9 Portafolio de Servicios.

Figura 6. Portafolio de servicios



IPS INDIGENA GUAITARA
PORTAFOLIO DE SERVICIOS

La IPS Indígena GUAITARA es una Institución Prestadora de Servicios de Salud Pública de carácter especial con responsabilidad administrativa y financiera, cuyo objeto social es la Prestación de Servicios de Salud del Primer Nivel de Baja Complejidad.

Somos una institución de primer nivel de atención, que trabaja para mejorar el nivel de vida y mantener la salud de nuestras comunidades indígenas de los Resguardos Indígenas de Ipiales, San Juan y Yaramal. Nuestros servicios se prestan con un equipo de trabajo interdisciplinario comprometido con la calidad de la atención en salud. Contamos con una sede principal ubicada en el Sector los Chilcos- Resguardo Indígena de Ipiales.

Propendemos por que nuestra institución sea identificada como una "Institución de Atención para la Salud y Bienestar de nuestras Comunidades Indígenas" y no únicamente como una institución que trata las enfermedades.

IMAGEN CORPORATIVA I.P.S. INDIGENA GUAITARA

NUESTRA MISIÒN:

Somos una institución prestadora de servicios de salud que garantiza la atención del primer nivel con calidad a toda la población indígena del Municipio de Ipiales; orientada a mantener una población saludable; optimizando recursos humanos, económicos y tecnológicos comprometidos con el mejoramiento continuo generando fuentes de trabajo en nuestra región.

NUESTRA VISIÒN:

Seremos una empresa reconocida como una institución líder en su modelo de atención especial para las comunidades indígenas, prestando servicios de salud integral con humanismo, calidad y confianza generada a través de nuestros trabajadores, usuarios y proveedores.

NUESTRO ESLOGAN:

"Salud y Bienestar para Nuestra Comunidad Indígena"

Fuente: Portafolio de Servicios IPS Indígena Guáitara

2.3 ARCHIVO CORRIENTE

2.3.1 Memorando de planeación auditoria.

Antecedentes: La auditoria de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia de que los datos que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de eficiencia.

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y controle los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

Objetivos

Objetivo general:

Aplicar técnicas de auditoría al Sistema de Información de la IPS INDIGENA GUAITARA, que contribuyan a evidenciar vulnerabilidades en la seguridad física y lógica a los que se encuentra expuesta.

Las técnicas que permiten hacer una evaluación más eficiente y ayudan a examinar y evaluar correctamente este proceso de evaluación son: entrevistas, cuestionarios, encuestas, observación, inventarios, muestreo experimentación, examen, inspección, revisión documental, etc. A fin de evaluar y emitir un informe sobre el desarrollo normal de funciones y operaciones.

Objetivos específicos:

Conocer el funcionamiento del sistemas de información en la actualidad en cuanto los usuarios del sistema, el hardware y software, la seguridad física y lógica, entre otros.

Realizar un análisis de riesgos para identificar y conocer la causa de los mismos, para proponer alternativas de solución.

Aplicar el proceso de auditoría a los riesgos más relevantes que afecten el funcionamiento del sistema, utilizando las técnicas apropiadas para realizar las pruebas que me permitan evidenciar.

Elaborar un informe final de auditoría con las fallas encontradas, las soluciones propuestas y los planes de mejoramiento resultado de la auditoria.

Alcance y delimitación: En el desarrollo del proyecto se identifico e investigo las diferentes técnicas de auditoría de sistemas, con el propósito de determinar cuáles deben ser utilizadas. Dentro de las técnicas que se investigo se encuentran técnicas para obtener información como cuestionarios, entrevistas, flujogramas; técnicas para verificar controles como software de auditoría para terminales, software de auditoría de propósito especial, software generalizado de auditoría entre otras. La aplicación de las técnicas y herramientas de auditoría dependió de la disponibilidad de los elementos de hardware y software de la institución auditada.

La aplicación de técnicas de auditoría se realizo al Sistema de Información de la IPS INDIGENA GUAITARA en el municipio de Ipiales, con el propósito de efectuar una revisión y evaluación de los controles físicos y lógicos, procedimientos de informática, observar su utilización, y evaluar la seguridad, con el fin de detectar problemas y plantear recomendaciones alternativas para que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Los puntos a evaluar serán los siguientes:

De las instalaciones físicas se evaluará:

Protección física de datos
Programas instalaciones
Equipos redes y soportes
Personal de las dependencias
Medidas de evacuación, alarmas, salidas alternativas
Estructura, diseño y distribución de las instalaciones eléctricas, de cableado de la red de datos
Sustituciones o sustracción de quipos, componentes, soportes magnéticos, documentación u otros activos
Seguridad de oficinas, recintos e instalaciones, protección eléctrica, contra incendios.
Áreas de acceso publico
Ubicación y protección de hardware
Mantenimiento de los equipos
Desastres naturales, incendios accidentales tormentas e inundaciones.
Amenazas ocasionadas por el hombre.

De equipos o hardware se evaluará:

Seguridad física de los medios
Actas e informes técnicos
Inventarios
La existencia de hojas de vida de los equipos de cómputo

La elaboración correcta de bitácoras de los mantenimientos realizados.

De seguridad lógica se evaluara:

Que cada usuario solo pueda acceder a los recursos que se le autorice el propietario.
Autenticación.
Quien asigna la contraseña inicial y sucesivas.
Longitud mínima y composición de caracteres.
Controles existentes para evitar y detectar virus.
Que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
Que la información recibida sea la misma que ha sido transmitida.
Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
Que se disponga de pasos alternativos de emergencia para la transmisión de información

Metodología: Para realizar la auditoría externa al Sistema de Información de la Institución Prestadora de Servicio de Salud Indígena Guáitara, donde se utilizo una metodología tipo de investigación cuantitativa, ya que permite examinar los datos de manera científica, o de manera más específicamente en forma numérica, generalmente con ayuda de herramientas del campo de la estadística.

Para alcanzar los objetivos propuestos, se utilizo la metodología de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del equipo auditor, también, se estudian y aplican conceptos y esquemas teóricos, también cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas para tener un funcionamiento de calidad.

La auditoría realizada por el equipo auditor fue dividida en varias etapas así:

Fase I: Conceptualización

En esta fase se realiza la recolección, clasificación y análisis de información sobre técnicas de auditoría de sistemas.

Fase II: Planeación

En la fase de planeación se realizan las siguientes actividades:

Identificar el alcance y los objetivos de la auditoria a realizar.

Realizar el estudio inicial en la institución tomada como caso de estudio.

Determinar los recursos necesarios para realizar la auditoria.

Elaboración del plan de trabajo.

Fase III: Realización de las actividades de auditoria

En esta etapa del proyecto se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. Se realizan las siguientes actividades:
Elección de los procesos a auditar.

Ejecución de la auditoria.

Elaboración de un análisis de Hallazgos y riesgos que permitan identificar cuáles de las actividades identificadas tienen una menor eficiencia, cuáles de los procesos tienen mayor impacto dentro del sistema.

Elaboración del informe con los Hallazgos encontrados, detectando las causas y su efecto.

Elaboración del modelo de madurez en el cual se encuentra el sistema auditado.

Elaboración del informe final.

Fase IV: Presentación del informe final

En esta etapa del proceso se presentará ante directivas de la INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUD INDÍGENA “GUÁITARA”, la sustentación y presentación del informe donde se darán a conocer los problemas encontrados y se establecerán posibles soluciones.

Recursos:

Recursos humanos

Para el desarrollo de este proyecto se cuenta con los estudiantes egresados de ingeniería de sistemas: NELSON ANDRES CORTES, JULIO CESAR BURGOS con la asesoría del Ingeniero MANUEL BOLAÑOS GONZALEZ, colaboración de la Doctora ADRIANA CHACUA Directora Administrativa y EDWIN BASTIDAS CALDERON Representante Legal.

Recursos tecnológicos

Computador portátil para realizar informes con las siguientes características:

Procesador Intel Core i3
Memoria RAM de 3 Gb
Disco duro de 250 Gb
Un quemador de Dvd de 16X
Sistema Operativo Windows Seven, Office 2010

Computador portátil para realizar informes con las siguientes características:

Procesador Intel Core 2 Duo.
Memoria RAM de 2 Gb.
Disco Duro de 160 Gb.
Un quemador de DVD LG de 16X.
Sistema Operativo Windows Seven, Office 2007.
Impresora de inyección HP 3650
Software utilizado para pruebas dentro del proceso de auditoría.
Cámara Digital para la captura del registro fotográfico.

Recursos materiales:

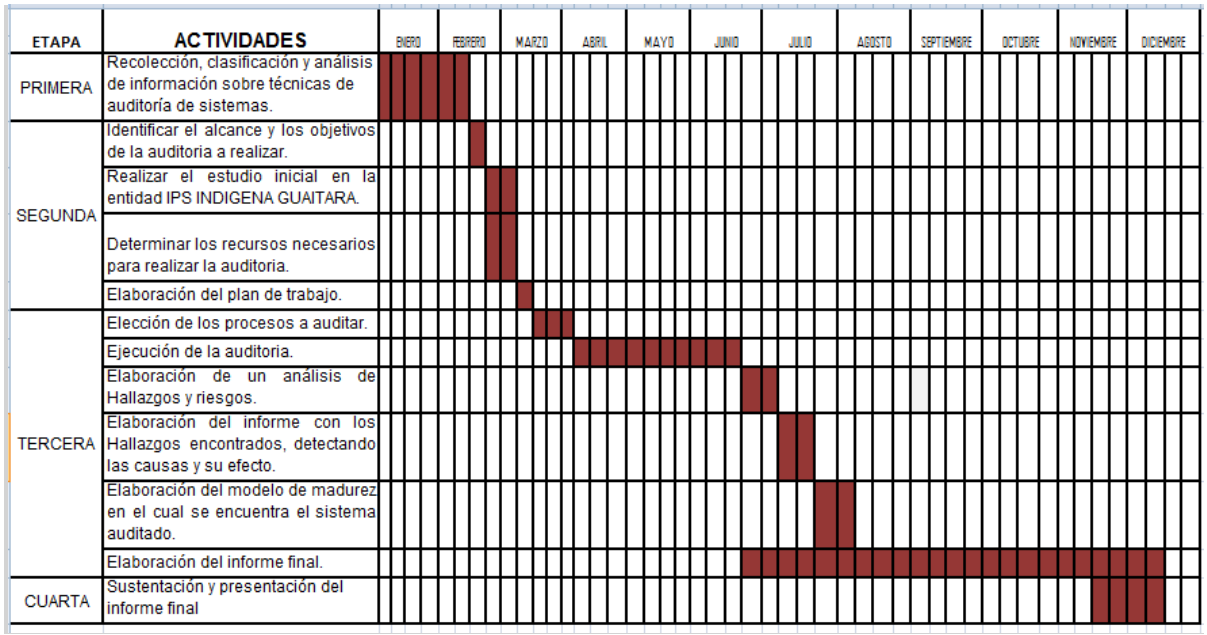
El proyecto se lleva a cabo utilizando los recursos disponibles en la entidad.

Recursos financieros

CANTIDAD	DETALLE	VALOR UNITARIO	VALOR TOTAL
8	Resma de papel tamaño carta	10.000	80.000
70	Horas de internet	1.000	70.000
12	Pasajes (Transporte)	7.000	84.000
16	Pasajes(Transporte)	10,000	160.000
320	Fotocopias de material de consulta	50	16.000
10	Alquiler de videocámara(horas)	25.000	250.000
1	Sistemas de tinta (impresora)	100.000	100.000
2	Digitalización de video	15.000	30.000
		Total	790.000

Nota: Estos gastos están a cargo de los estudiantes quienes realizarán el proyecto.

Cronograma:



2.3.2 Programa de auditoría. Esta auditoría se ejecutara mediante la aplicación de la metodología COBIT (objetivos de control para la información y tecnologías afines), donde se evaluarán algunos objetivos de control que se encuentran dentro de los 4 dominios para evidenciar las vulnerabilidades de la seguridad física y lógica en el proceso de auditoría de la IPS INDÍGENA GUÁITARA, de esta manera se aplicó y se describen a continuación:

2.3.2.1 Dominio 1: planeación y organización (PO). Este dominio se refiere a la identificación de la Tecnología de Información y en cómo esta puede contribuir a cumplir los objetivos del negocio. Los procesos que se aplican son los siguientes:

- **Niveles de Seguridad:** El área de Sistemas de Información deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de control apropiado (mínimo) para cada una de las clasificaciones.

b. PO4 Definir los procesos, la organización y las relaciones de TI

Asegurar el control y el buen funcionamiento de la institución estableciendo una organización de TI que cumpla con los requerimientos de personal, funciones, roles y responsabilidades garantizando el cumplimiento de los objetivos y la seguridad de la información. Los objetivos de control que se evaluarán son:

- **Establecimiento de roles y responsabilidades**: Identificar y dar a conocer a los funcionarios de la organización las funciones y responsabilidades asignadas, así como también se deberá realizar una descripción y actualización periódica de los roles establecidos. La Institución y el lugar donde se encuentra el Sistema de Información deberá asegurar que todo el personal en la dependencia conozca sus funciones y responsabilidades en relación con los sistemas de información.

  Todos deberán estar conscientes de que tienen una cierta responsabilidad con respecto a la seguridad y al control interno.

- **Responsabilidad sobre el riesgo, la seguridad y el cumplimiento:** El área de Sistemas de Información deberá asignar al personal competente responsabilidad de la seguridad lógica y física de los activos de la información. En caso necesario deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles relacionados con ellos.

- **Propiedad de datos y de sistemas:** El área de Sistemas de Información deben asignar responsabilidad a funcionarios que puedan cumplir el rol de ser propietario de datos y de sistemas. Estos funcionarios están comprometidos a aplicar requerimientos de seguridad aplicables a la entrega y recepción, procesamiento y almacenamiento físico de la información.

- **Supervisión:** El área de Sistemas de Información deberá implementar prácticas de supervisión adecuadas en la Institución para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente y para evaluar todo lo referente al personal que interactúa con el sistema.

- **Segregación de Funciones:** El área de Sistemas de Información deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico, además deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular deberá mantenerse una segregación de funciones entre las siguientes funciones:

  - Uso de sistemas de información;
  - Entrada de datos;
  - Operación de cómputo;
  - Administración de redes;
  - Administración de sistemas;
  - Desarrollo y mantenimiento de sistemas
  - Administración de cambios
  - Administración de seguridad; y
  - Auditoría de seguridad

- **Asignación de Personal para Tecnologías de la Información**: Las evaluaciones de los requerimientos de asignación de personal deberán llevarse a cabo regularmente para asegurar que la función de servicios de información cuente con un número suficiente de personal competente de tecnología de información. Los requerimientos de asignación de personal deberán ser evaluados por lo menos anualmente o al presentarse cambios mayores dentro del Sistema, en el ambiente operacional o de tecnología de información. Deberá actuarse oportunamente tomando como base los resultados de las evaluaciones para asegurar una asignación de personal adecuada en el presente y en el futuro.

- **Descripción de Puestos para el Personal de la Función de Servicios de Información:** El área de Sistemas de Información deberá asegurar que las Descripciones es de los puestos para el personal de la función de servicios de información sean establecidos y actualizados regularmente. Estas Descripciones de puestos deberán delinear claramente tanto la responsabilidad como la autoridad, incluir las definiciones de las habilidades y la experiencia

necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

- **Personal de TI:** El área de Sistemas de Información deberá definir e identificar al personal clave de TI basado en las necesidades para tener en claro los diferentes roles que debe cumplir cada funcionario.

d. PO9 Evaluación de riesgos de TI

Cumplir a cabalidad los objetivos de TI, adoptando estrategias para evitar y disminuir riesgos que puedan afectar el cumplimiento de estos objetivos. Se evaluaran los siguientes objetivos de control:

- **Evaluación del Riesgo del Negocio:** El área de Sistemas de Información deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema.

- **Enfoque de Evaluación de Riesgos:** El área de Sistemas de Información deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

- **Identificación de eventos:** La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones consecuencias y probabilidad de amenaza.

- **Medición de Riesgos:** El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genera como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

- **Plan de Acción contra Riesgos:** El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.
- **Aceptación de Riesgos:** El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

- **Evaluación de riesgos:** Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.

- **Respuesta a los riesgos:** Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continúa.

2.3.2.2 Dominio 2: adquirir e implementar (AI). En este dominio las soluciones tienen que ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Igualmente, tiene en cuenta los cambios y mantenimiento que deben tener los sistemas que existan dentro de la empresa. Los procesos utilizados en este dominio son:

b. AI3 Adquisición y mantenimiento de la infraestructura tecnológica

La Institución debe contar con procesos para adquirir, implantar y dar mantenimiento a una infraestructura integrada y estándar de TI enfocándose en proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología. Se evaluaran los siguientes objetivos de control:

- **Mantenimiento Preventivo para Hardware:** El área de Sistemas de Información deberá calendarizar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

- **Seguridad del Software del Sistema:** El área de Sistemas de Información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

- **Instalación del Software del Sistema:** En la Institución se deberán implementar procedimientos para asegurar que el software del sistema sea instalado de acuerdo al marco de referencia de adquisición y mantenimiento de infraestructura de tecnología. Las pruebas deberán ser llevadas a cabo antes de autorizarse su utilización en ambiente de producción.

- **Mantenimiento del Software del Sistema:** En la Institución se deberá implementar procedimientos para asegurar que el software del sistema sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

- **Controles de Cambios para el Software del Sistema:** el área de Sistemas de Información deberá implementar procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la organización.

c. AI6 Administración de Cambios

Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- **Transferencia de conocimiento al personal de operaciones y soporte:** Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.

- **Inicio y Control de Requerimientos de Cambio:** El área de Sistemas de Información deberá asegurar que todas las requisiciones de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios. Las solicitudes deberán categorizarse, priorizarse y establecerse procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estado de su solicitud.

- **Control de Cambios:** El área de Sistemas de Información deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración.

- **Documentación y Procedimientos:** El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

- **Mantenimiento Autorizado:** El área de Sistemas de Información deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados.

2.3.2.3 Dominio 3: entregar y dar soporte (DS). Este dominio hace referencia a la entrega de los servicios solicitados, en donde se incluyen, la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte de servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. A continuación se establecerán los procesos de control necesarios:

a. DS5 Garantizar la seguridad de sistemas

Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- **Administración de Medidas de Seguridad:** La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio.

- **Seguridad de Acceso a Datos en Línea:** En un ambiente de tecnología de información en línea, el área de Sistemas de Información deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

- **Administración de Cuentas de Usuarios:** El área de Sistemas de Información deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

- **Revisión Gerencial de Cuentas de Usuarios** El área de Sistemas de Información se deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

- **Control de Usuario de las Cuentas de Usuario:** Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

- **Vigilancia de Seguridad:** El área de Sistemas de Información debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

- **Clasificación de Datos:** Se deberá asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran "no protección" deberán contar con una decisión formal que les asigne dicha clasificación.

- **Administración Centralizada de Identificación y Derechos de Acceso:** Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

- **Reportes de Actividad de Violación y Seguridad:** El área de Sistemas de Información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo51 (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

- **Manejo de Incidentes:** Se deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

- **Ruta Confiable:** Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (trusted paths). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

- **Protección de las Funciones de Seguridad:** Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgaciónde sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

- **Prevención, Detección y Corrección del Software Dañino:** Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

- **Arquitectura de Firewalls y Conexiones con las Redes Públicas:** Si existe conexión con Internet u otras redes públicas en la organización. Se deberá contar con sistemas Firewall adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.

b. DS9 Administrar la configuración

Implantar un repositorio de configuraciones de recursos de TI, en el cual se pueda identificar, mantener y actualizar estos elementos y que estén disponibles cuando se los requiera. Los objetivos de control a evaluar son:

- **Registro de la Configuración:** Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo). El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

- **Registro de Estatus:** Se deberá asegurar que los registros de configuración reflejen el estado real de todos los elementos de la configuración incluyendo la historia de los cambios.

- **Control de la Configuración:** Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de la función de servicios de información sean revisadas periódicamente.

- **Software no Autorizado:** El área de Sistemas de Información deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización.

c. DS11 Administrar datos

Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Los objetivos de control que se evaluarán son:

- **Protección de Información Sensible durante transmisión y transporte**: El área de Sistemas de Información deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

- **Protección de Información Crítica a Ser Desechada:** El área de Sistemas de Información deberá definir e implementar procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos deberán garantizar que ninguna información marcada como "borrada" o "desechada", pueda ser accedida por personas internas o externas a la organización.

- **Administración de Almacenamiento:** Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y las políticas de seguridad.

- **Períodos de Retención y Términos de Almacenamiento**: Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de entrada y de salida), así como los datos (claves, certificados) utilizados para su encriptamiento y autenticación.

- **Respaldo y Restauración**: Se deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

- **Funciones de Respaldo**: Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

- **Almacenamiento de Respaldos**: Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

d. DS12 Administración de las Instalaciones

Garantizar que los recursos de TI, tanto de personal como de equipos de cómputo, estén debidamente protegidos contra cualquier daño ocasionado por factores naturales o fallas humanas. Por lo tanto es necesario crear un proceso el cual controle el acceso a personal no autorizado y contemple una buena administración de la seguridad física. Se evaluaran los siguientes objetivos de control:

- **Seguridad Física:** Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.

- **Discreción de las Instalaciones de Tecnología de Información:** Se deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones donde se encuentran los equipos de computo que almacena la información critica, no se fácil.

- **Protección contra Factores Ambientales:** Se deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

2.3.2.4 Dominio 4: monitorear y evaluar (ME). Todos los procesos de una institución necesitan ser evaluados regularmente a través del tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio incluye la administración del desempeño, el monitoreo del control interno, el cumplimento regulatorio y la aplicación del gobierno. De este dominio se toman los siguientes procesos:

a. ME2 Monitorear y evaluar el control interno

Realizar una constante evaluación al control interno, verificando que se cumplan las leyes y protegiendo el logro de los objetivos de TI. Se evaluarán los siguientes objetivos de control:

- **Monitoreo de Control Interno:** El área de Sistemas de Información deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

- **Operación Oportuna de Controles Internos**: La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la Gerencia.

- **Reporte sobre el Nivel de Control Interno**: El área de Sistemas de Información deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

- **Seguridad de Operación y Aseguramiento de Control Interno**: La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos a través de una "autoauditoría" o de una auditoría independiente para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

2.3.3 Diseño de los elementos para la auditoria. Para el desarrollo de la auditoría de sistemas en la Institución IPS INDIGENA GUAITARA se diseñaron y se utilizaron los siguientes formatos de recolección de información:

Para dar comienzo a la auditoria, se realizaron diferentes entrevistas, información que sirve para el reconocimiento de los diferentes procesos y actividades en el desarrollo de este trabajo.

2.3.3.1 Observación directa. Se utiliza esta técnica como un elemento de auditoría muy importante que permite observar, tomar información y registrarla. En las visitas a las instituciones también se evidencio información mediante fotografías y videos, sirviendo de apoyo en el análisis que finalmente se hizo.

2.3.3.2 Cuadro de definición de fuente de conocimiento, pruebas de análisis y pruebas de auditoría: Permite obtener la información necesaria para establecer las fuentes de conocimiento, mediante la aplicación de los dominios del COBIT, además se describe las pruebas aplicables que se tuvieron en cuenta para esta evaluación.

Los campos que utiliza este formato se describen a continuación:

REF: Identificación del cuadro de definición.

INSTITUCIÓN AUDITADA: Nombre de la institución a la cual se aplica el proceso de auditoría.

AREA AUDITADA: Nombre del área a la cual se aplicara la auditoria (p.ej. red de datos, seguridad física y lógica)

RESPONSABLES: Nombres del equipo Auditor.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se describe el objetivo del proceso establecido dentro de los dominios del COBIT.

MATERIAL DE SOPORTE: Nombre del material que da soporte al proceso establecido.

DOMINIO: Nombre del dominio del COBIT que se va a evaluar.

PROCESO: Nombre del proceso que se va a auditar dentro de los dominios del COBIT.

FUENTES DE CONOCIMIENTO: fuentes de donde se obtuvo la información para el proceso de auditoría.

REPOSITORIO DE PRUEBAS APLICABLES: Se divide en dos tipos de pruebas:

DE ANÁLISIS: Espacio destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

DE EJECUCIÓN: Espacio destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

Todos los cuadros de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría utilizados en el proceso de auditoría se encuentran en los Anexos entregados en medio digital.

En la página siguiente hay un ejemplo del cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría., en este caso es para el proceso M2. Evaluar lo Adecuado del control interno, que se ubica dentro del dominio de Monitoreo del COBIT. Ver tabla 1.

Tabla 1. Formato cuadro de definición fuentes de conocimiento

	CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA			REF
				PLAN M2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indigena "GUAITARA"			**PAGINA**
				1 de 1
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andres Cortes			

DESCRIPCIÓN DE ACTIVIDAD / PRUEBA: Buscar asegurar el logro de los objetivos de control interno establecidos para los procesos de TI, a través del compromiso de la Gerencia de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular.

MATERIAL DE SOPORTE: COBIT

DOMINIO	Monitoreo (M)	**PROCESO**	Evaluar lo adecuado del control interno

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANALISIS	**DE EJECUCION**
_Entrevista a los encargados del area o dependencia facturacion de la Ips Indígena Guáitara _Entrevista al Coordinador de Sistemas y de Comunicaciones.	_Analisis políticas y procedimientos relacionados con los procesos de monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del Sistema de Información de la Ips Indígena Guáitara. _	_Revision de procesos de monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la Información del Sistema de Información . _

AUDITORES RESPONSABLES
JULIO CESAR BURGOS
NELSON ANDRES CORTES

2.3.3.3 Cuestionario cuantitativo. El cuestionario es una técnica utilizada para recopilar datos, permite llegar a un mayor número de participantes y facilita el análisis, consiste en una serie de preguntas, escritas, que debe responder el entrevistado. Además permite dar un puntaje que permite analizar los riesgos de cada proceso.

Los campos que utiliza este formato se describen a continuación:

REF: Espacio reservado para la identificación del cuestionario.

INSTITUCIÓN AUDITADA: Nombre de la institución a la cual se aplica el proceso de auditoría.

ÁREA AUDITADA: Nombre del área a la cual se aplicara la auditoria (p.ej. red de datos, seguridad física y lógica)

RESPONSABLES: Nombres del equipo Auditor.

DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: En este espacio se describe el objetivo del proceso establecido dentro de los dominios del COBIT.

MATERIAL DE SOPORTE: Nombre del material que da soporte al proceso establecido.

DOMINIO: Nombre del dominio del COBIT que se va a evaluar.

PROCESO: Nombre del proceso que se va a auditar dentro de los dominios del COBIT.

PREGUNTA: Descripción de la información requerida la cual se quiere investigar.

SI – NO – NA: Aquí se establece un valor de 1 a 5 de acuerdo a si cumple o no con la información requerida. Teniendo en cuenta que:

1: Es el mínimo puntaje que se le puede asignar y es irrelevante.
5: Es el máximo puntaje que se le puede asignar y es de gran importancia.

RPT: fuente de donde se obtuvo la información requerida.

En la página siguiente hay un ejemplo del cuestionario cuantitativo, en este caso es para el proceso M2. Evaluar lo adecuado del control interno, que se ubica dentro del dominio de Monitoreo de COBIT. Ver tabla 2.

Tabla 2. Formato cuestionario cuantitativo

	CUESTIONARIO CUANTITATIVO		REF
			PLAN M2_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"		PAGINA 1DE1
AREA AUDITADA	Seguridad Física y Lógica		
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortes		
MATERIAL DE SOPORTE:	COBIT		
DOMINIO	Monitoreo(M)	PROCESO	Evaluar lo adecuado del control interno (M2)

PREGUNTA	SI	NO	NA	RPT
1. ¿En la IPS Indígena Guáitara existen políticas y procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica a los activos de Tecnologías de la información del sistema de información?		5		
2. ¿Estas políticas contemplan:		5		
_Descripción detallada de los procedimientos de monitoreo se deben aplicar?		5		
_Cuál es la periocidad ideal para ejecutar los procesos de monitoreo?		5		
_Que debe ejecutar el monitoreo?		5		
3. ¿Estas políticas y procedimientos estan documentados?		5		
4. ¿Estas políticas y procedimientos son de conocimiento de los funcionarios del área de Tecnología de la Información?		5		
TOTALES		30		
TOTAL CUESTONARIO		30		
PORCENTAJE DE RIESGO: _____=_____= = %				

Las equivalencias que se utilizan para asignares valores a los requerimientos, va entre 1 y 5, siendo 1 un valor insignificante, esto quiere decir que no es importante, pero el valor 5 un valor critico, cuando aparece el 5 en el lado de los NO, esto automáticamente se convierte en un hallazgo.

TOTALES: espacio para asignar el valor de:

- Sumatoria de los valores de la columna SI
- Sumatoria de los valores de la columna NO
- Sumatoria de los valores de la columna NA

TOTAL CUESTIONARIO: En este espacio se asigna la suma de los totales (SI, NO y NA).

Para calcular el porcentaje de riesgo, aplicamos la siguiente fórmula matemática

PORCENTAJE DE RIESGO: Para calcular el porcentaje de riesgo se aplica la siguiente fórmula matemática:

$$\text{Porcentaje de Riesgo}_1 = \frac{\text{Totales SI} * 100}{\text{Total Cuestionario} - \text{Totales NA}}$$

Luego de obtener el anterior porcentaje se calcula el porcentaje de riesgo total así:

$\text{Porcentaje de Riesgo}_{\text{Total}} = 100 - \text{Porcentaje de Riesgo}_1$

Después de haber calculado este porcentaje, se procede a determinar el nivel de riesgo en el que se encuentra, para esto se tiene en cuenta la siguiente escala:

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

Riesgo Bajo: Las deficiencias que se presentan en este nivel no son de gran importancia, sin embargo se deben considerar soluciones preventivas a largo plazo.

Riesgo Medio: Las medidas para reducir el riesgo deben implantarse en un periodo determinado puesto que el daño causado puede ser controlado.

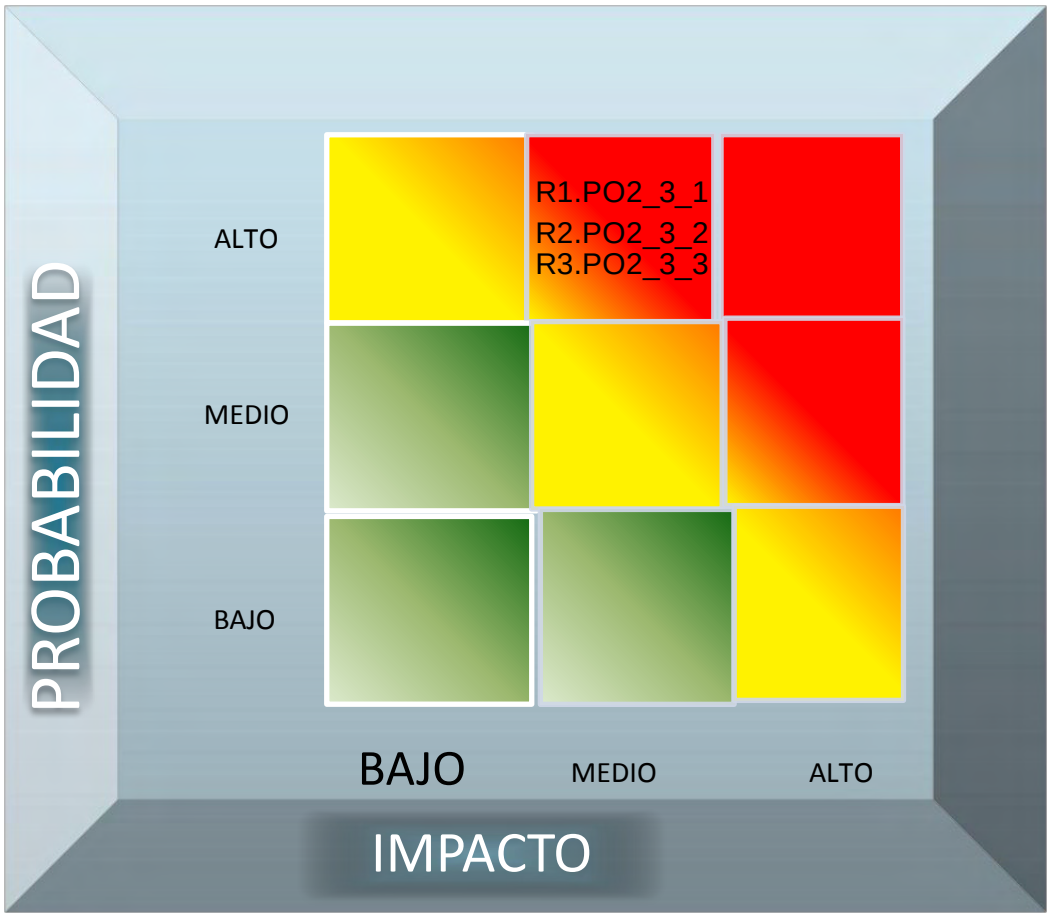
Riesgo Alto: En este nivel se deben establecer estrategias radicales e inmediatas para reducir el riesgo, porque de lo contrario afectaría el logro de los objetivos de la institución.

Todos los cuestionarios cuantitativos utilizados en el proceso de auditoría se encuentran en los anexos entregados en medio digital:

2.3.3.4 Matriz de probabilidad e impacto. La matriz de probabilidad e impacto es un elemento fundamental para determinar el nivel de riesgo de cada proceso auditado y a su vez identificar los riesgos más críticos. El porcentaje de riesgo obtenido se ubica en la respectiva casilla de acuerdo a la clasificación del riesgo.

En la tabla 3 se muestra el diseño de la matriz de probabilidad e impacto:

Tabla 3. Formato matriz de probabilidad e impacto.



Riesgo Bajo

Riesgo Moderado

Riesgo Intolerable

2.3.3.5 Entrevista. Las entrevistas que se hicieron a la institución fueron realizadas por el equipo auditor. Cabe resaltar que la institución auditada no tenía conocimiento de estas visitas, por lo tanto los entrevistados no tuvieron previa preparación.

Se realizaron dos tipos de entrevistas:

Entrevistas con preguntas abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una.

Entrevistas con preguntas cerradas: el entrevistado se limita a contestar Si o No, se recoge información útil para nuestra investigación, permitiendo en este formato adicionar la cantidad de algunos elementos y algunas observaciones.

Todas las entrevistas aplicadas y los formatos utilizados en el proceso de auditoría se encuentran en los Anexos entregados en medio digital.

En las páginas siguientes se presentan ejemplos de los cuestionarios de entrevistas que se utilizaron para realizar este proceso de Auditoría.

Tabla 4. Formato de entrevista

	ENTREVISTA		**REF**
			ENT_DS12_3_1
			PAGINA
			1 de 1
ENTIDAD AUDITADA	Institución Prestadora de Servicio de Salud Indígena "GUÁITARA"		
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de información
AUDITORES RESPONSABLES			
ENTREVISTADO	ADRIANA CHACUA		
CARGO: Directora General			
JULIO CESAR BURGOS – NELSON ANDRES CORTES			

PREGUNTA	**SI**	**NO**
1. ¿Conoce usted de la existencia de políticas o procedimientos relacionados con la utilización de hardware (Hardware permitido, hardware no permitido) en los equipos de cómputo? 2. ¿Existen extintores de incendios ubicados en sitios estratégicos y de fácil acceso dentro de las instalaciones de la Institución Prestadora de Servicio? 3. ¿Existen dispositivos detectores de humo, detectores de calor, y supresores de incendios dentro de las instalaciones de la Institución Prestadora de Servicio? 4. ¿Existen planes de evacuación de las instalaciones de la Institución Prestadora de Servicio, en caso de presentarse una catástrofe natural? 5. ¿Existen planes están documentados y son de su conocimiento? 6. ¿Existen señales que indiquen la ruta de evacuación de las instalaciones de la Institución Prestadora de Servicio? 7. ¿Existe sistema de alarma y detección de movimientos en las instalaciones de la Institución Prestadora de Servicio? 8. ¿los sistemas de alarma y detección de movimiento están actualmente en funcionamiento?		

Tabla5. Formato de entrevista 2

	ENTREVISTA			**REF**
				ENT_DS12_3_1
				PAGINA
				1 de 1
ENTIDAD AUDITADA	Institución Prestadora de Servicio de Salud Indígena "GUÀITARA"			
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de información	
				AUDITORES RESPONSABLES
ENTREVISTADO				
CARGO				

1. ¿Cuáles son sus funciones dentro del Sistema de Información SII de la Institucion prestadora de servicio?

_____

2. ¿Conoce usted la existencia de un manual de funciones para los usuarios del Sistema de Información?

_____

3. ¿Qué medidas de seguridad para evitar que otras personas entre a su computador tiene implementadas?

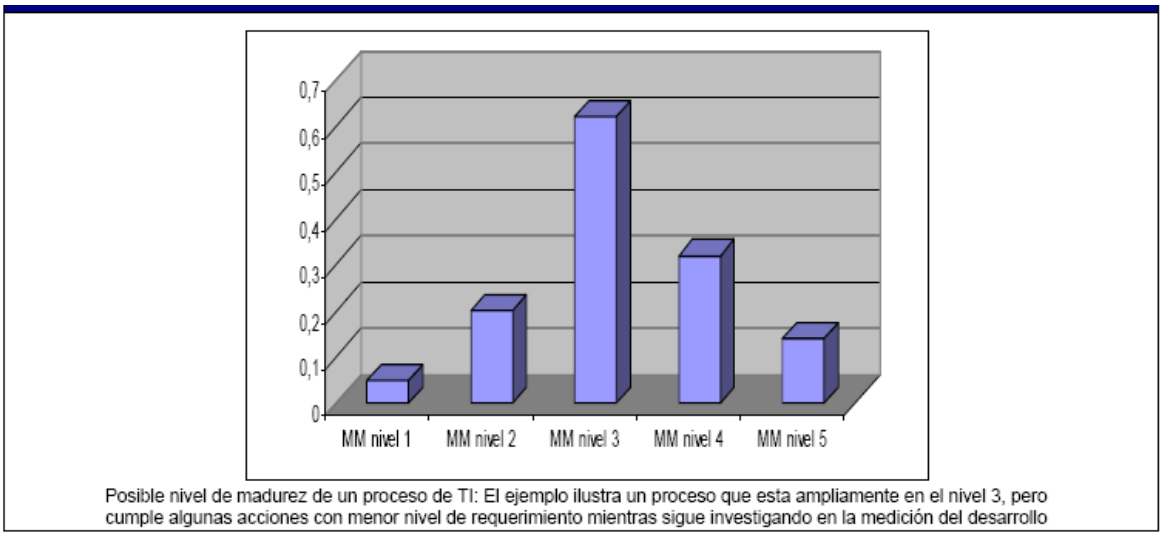
_____

Nombre: _____

Firma: _____

2.3.4 Modelo de Madurez. Se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5. El propósito no es evaluar el nivel de adherencia a los objetivos de control.
Los niveles de madurez están diseñados como perfiles de procesos de TI que una organización reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Una evaluación de la madurez de COBIT resultará en un perfil donde las condiciones relevantes a diferentes niveles de madurez se han conseguido, como se muestra en el ejemplo gráfico de la figura siguiente.

Figura 7. Modelo de Madurez

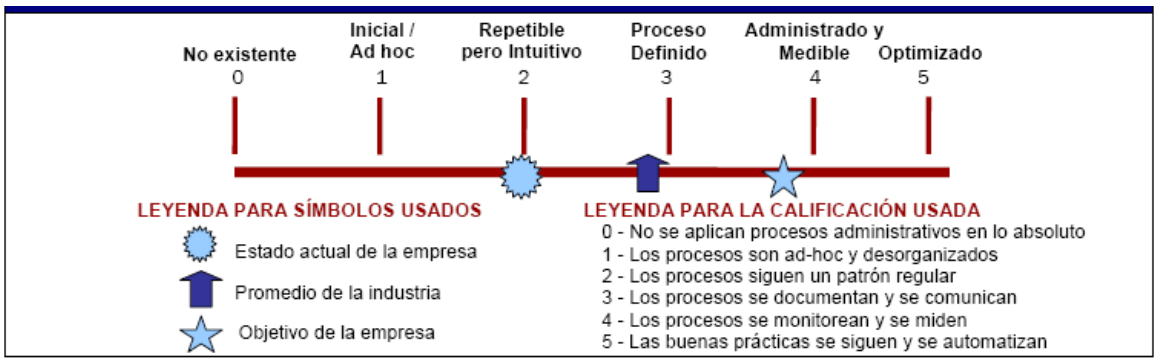


Posible nivel de madurez de un proceso de TI: El ejemplo ilustra un proceso que esta ampliamente en el nivel 3, pero cumple algunas acciones con menor nivel de requerimiento mientras sigue investigando en la medición del desarrollo

Esto se debe a que cuando se emplea la evaluación de la madurez con los modelos de COBIT, a menudo algunas implementaciones estarán en diferentes niveles aunque no esté completa o suficiente.
• El desempeño real de la empresa—Dónde se encuentra la empresa hoy.
• El objetivo de mejora de la empresa—Dónde desea estar la empresa
• El crecimiento requerido entre “como es” y “como será”

Gráficamente el modelo de madurez se describe a continuación.

Figura 8. Grafica modelo de Madurez



Estas escalas deben ser prácticas en su aplicación y razonablemente fáciles de entender.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto.

La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

2.3.5 Hallazgos aplicados en la auditoría de la Ips Indígena Guáitara. Después de haber realizado el análisis de riesgos se procede a identificar las vulnerabilidades de cada proceso evaluado.

2.3.4.1 Dominio: Planeación y organización (PO): Dentro del dominio de Planeación y Organización (PO) del COBIT, se seleccionaron los procesos PO2. Definición de la arquitectura de la información, PO4. Definición de la organización y las relaciones TI y PO9. Evaluación de riesgos, para ser evaluados, los hallazgos o las no conformidades detectadas están clasificados y agrupados por cada uno de los procesos.

PO2 Determinar la dirección tecnológica: Los hallazgos o no conformidades para este proceso se muestran en la siguiente página.

Tabla 6. Hallazgo Planeacion y Organización PO2_3_1

	HALLAZGOS			**REF** **PLAN PO2_3_1**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUÁITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Hallazgo:

No existe un Manual Técnico y de Soporte para el Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

El Sistema de Información de la Ips Indígena Guáitara , debe implementar un manual técnico y de soporte que contenga:

_Las características del aplicativo, para que sirve, que pretende resolver y a quien va dirigido.

_Requerimientos de software y hardware para su funcionamiento.

_Instrucciones y pasos a seguir para realizar el proceso de instalación y puesta en funcionamiento del aplicativo.

_Descripción del funcionamiento de los diferentes módulos que conforman el sistema de Información.

_Descripción de reportes del Sistema de Información.

_Descripción de logs de Sistema de Información.

_Listado de archivos y especificaciones.

	HALLAZGOS			**REF**
				PLAN PO2_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Consecuencia:
La no existencia de un manual técnico y de soporte para el Sistema de Información de la Ips Indígena Guáitara, dificulta y extiende los procesos para realizar cambios y ajustes dentro de él.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel de Madurez: 3

Evidencias:
ENT_PO2_3_1

Tabla 7. Hallazgo Planeación y Organización PO2_3_3

	HALLAZGOS			**REF** **PLAN PO2_3_2**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud IndIgena “GUAITARA”			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Hallazgo:

No existe un Diccionario de Datos del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

El Diccionario de Datos del Sistema de Información de la Ips Indígena Guáitara debe contener:

_Estructura física y lógica de la base de datos del Sistema de Información.

_Las definiciones de los objetos de la base de datos: tablas, vistas, índices, disparadores, procedimientos y funciones.

_El espacio asignado y utilizado por los objetos.

_Información sobre las restricciones de integridad.

_Los valores por defecto de las columnas de las tablas. Información de los privilegios y roles otorgados a los usuarios.

	HALLAZGOS			REF
				PLAN PO2_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Impacto:
Al no contar con un Diccionario de Datos en la entidad se dificultaría la localización de errores y realización de cambios o ajustes al Sistema de Información de la Ips Indígena Guáitara.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel de Madurez: 1

Evidencias:
ENT_PO2_3_2

Tabla 8. Hallazgo Planeación y Organización PO2_3_3

	HALLAZGOS			**REF** **PLAN PO2_3_3**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud IndIgena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Hallazgo:

No se cuenta con un modelo para la arquitectura de la información del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

El Sistema de Información debe estar documentado (arquitectura de la información) donde se indique la información clara de cómo están organizados y relacionados entre sí cada uno de los elementos que lo conforman. El modelo de la arquitectura debe contener:

_identificación de entradas
_Identificación de procesos.
_Identificación de sitios de almacenamiento.
_Identificación de reportes.
_Identificación de la interacción con otros sistemas.
_Definición de usuarios finales.
_Los planes de Tecnologías de la Información a corto y largo plazo.

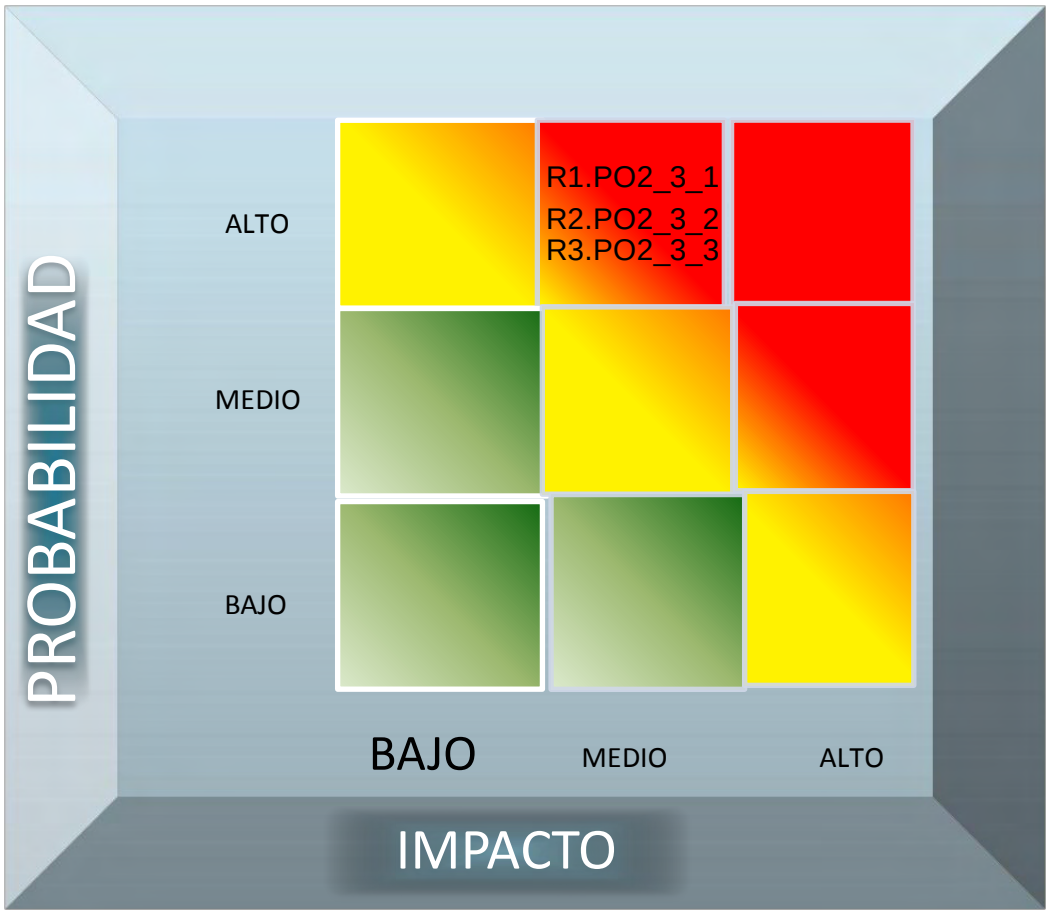
	HALLAZGOS			REF
				PLAN PO2_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Impacto:
La no existencia de un modelo de la arquitectura para el Sistema de Información, puede generar demoras y aumentos significativos en los costos (tiempo y dinero) cuando se requieran realizar actividades de ajuste dentro de los módulos.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel de Madurez: 1

Evidencias:
ENT_PO2_3_3

Tabla 9. Matriz de probabilidad e Impacto PO2



R1PAIM Extender los procesos para realizar cambios y ajustes dentro del Sistema de Información.

R2PAIM Dificulta los procesos de localización de errores y realización de cambios o ajustes al sistema.

R3PAIM Generar demoras y aumentos significativos en los costos (tiempo y dinero) cuando se requieras realizar actividades de ajuste.

PO4 Definir los procesos, organización y relaciones de TI: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 10. Hallazgo Planeación y Organización PO4_3_1

	HALLAZGOS			REF PLAN PO4_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
ÁREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI(P04)	

Hallazgo:
No existe un manual de funciones para los usuarios que interactúan con el Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:
_Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
_Definición de las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan.
_Definición de responsabilidades de cada uno de los usuarios.
Se debe dar a conocer a los usuarios el manual de funciones el cual también debe contener recomendaciones de procesos a seguir por parte de los usuarios para garantizar la seguridad de la información.

	HALLAZGOS			REF
				PLAN PO4_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI(P04)	

Impacto:
La no existencia de un manual de funciones para los usuarios del Sistema de Información de la Ips Indígena Guáitara, puede generar que se presenten daños dentro del éste, ocasionados por el mal manejo del mismo, además puede generar retrasos en la ejecución de tareas dentro del sistema, por no saber cual es el procedimiento para realizarlas. Esto se verá reflejado en la prestación de un servicio ineficaz e ineficiente a la comunidad del municipio de Ipiales.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel De Madurez: 1

Evidencias:
ENT_PO4_3_1

Tabla 11. Hallazgo Planeación y Organización PO4_3_2

	HALLAZGOS			REF
				PLAN PO4_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI(P04)	

Hallazgo:

No existe un manual de funciones para el personal de TI relacionado con el Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

Se debe contar con un manual de funciones para los usuarios de TI que interactúen con el Sistema de Información de la Ips Indígena Guáitara, donde se indique:

_Definición de las funciones que los usuarios de TI deben desempeñar de acuerdo con el rol que tengan.

_Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema de Información.

_Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

Debe garantizarse que este manual sea de conocimiento del personal de TI que interactúa con el Sistema de Información de la entidad.

	HALLAZGOS			REF
				PLAN PO4_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI(P04)	

Impacto:

La no existencia de un manual de funciones para el personal de TI que interactúa con el Sistema de Información, puede ocasionar daños no intencionales dentro del mismo por la realización de procesos no adecuados.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel de Impacto: 2

Evidencias:
ENT_PO4_3_2

Tabla 12. Hallazgo Planeación y Organización PO4_3_3

	HALLAZGOS			REF
				PLAN PO4_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI(P04)	

Hallazgo:

Existe personal clave e indispensable para el funcionamiento del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

Debe existir dentro del personal de TI por lo menos 2 funcionarios que tengan los conocimientos necesarios para proveer soporte al Sistema de Información de la Ips Indígena Guáitara. El correcto funcionamiento, no puede depender de una sola persona.

	HALLAZGOS			REF
				PLAN PO4_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Definición de la Organización y de las Relaciones de TI(P04)	

Consecuencia:

La existencia de personal indispensable para el funcionamiento del Sistema de Información, genera dependencia, y puede ocasionar el paro indefinido de las actividades de la Ips Indígena Guáitara (con respecto al Sistema), en caso de ausencia de estas personas.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alta
Nivel de Madurez: 2

Evidencias:
ENT_PO4_3_3
IMG01_PO4_3_3

Figura 9. Personal de TI (IMG01_P04_3_3)

REF	IMG01_P04_3_3

	HALLAZGOS			REF
				PLAN PO2_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indigena “GUAITARA”			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeacion y Organización (PO)	**PROCESO**	Definición de la Arquitectura de la Información(P02)	

Impacto:
La no existencia de un modelo de la arquitectura para el Sistema de Información, puede generar demoras y aumentos significativos en los costos (tiempo y dinero) cuando se requieran realizar actividades de ajuste dentro de los módulos.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio

Evidencias:

ENT_PO2_3_3

R1PAIM Generar que se presenten daños dentro del SI, ocasionados por el mal manejo del mismo, además puede generar retrasos en la ejecución de tareas dentro del sistema, por no saber cuál es el procedimiento para realizarlas.

R2PAIM Puede ocasionar daños no intencionales dentro del SI por la realización de procesos no adecuados.

R3PAIM ocasionar el paro indefinido de las actividades de la Ips Indígena Guáitara (con respecto al SI), en caso de ausencia de personas claves.

PO9. Evaluación de riesgos: Los hallazgos o no conformidades para este proceso se muestran a continuacion.

Tabla 14. Hallazgo Planeación y Organización PO9_3_1

	HALLAZGOS			**REF**
				PLAN PO9_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación y Análisis de Riesgos (PO9)	

Hallazgo:

Las políticas y procedimientos para el análisis y gestión del riesgo para las TI, dentro de la Ips Indígena Guáitara y específicamente para el Sistema de Información, carecen de elementos fundamentales para garantizar la minimización del riesgo.

Recomendaciones:
Se debe tener en cuenta las políticas y procedimientos para el análisis y gestión del riesgo para las TI en la Ips Indígena Guáitara, las cuales deben abarcar los siguientes temas:
_La definición del contexto de la entidad.
_El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión del riego
_La identificación de los activos de los Sistema de Información.
_La identificación y clasificación de los riesgos a los que se encuentran expuestos los activos de los Sistemas de Información.
_La determinación de la probabilidad de ocurrencia de los riesgos que amenazan los activos de los Sistemas de Información.
_La determinación del impacto que causaría la ocurrencia de los riesgos.
_La identificación de controles que mitiguen los riesgos.
_La toma de decisiones frente a los riesgos
_La toma de decisiones frente a los riesgos.
_La elaboración del Plan de Seguridad Informática.

	HALLAZGOS			REF
				PLAN PO9_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	Evaluación y Análisis de Riesgos (PO9)	

Consecuencia:

Los activos de TI del Sistema de Información de la Ips Indígena Guáitara están expuestos a sufrir daños físicos y lógicos, ocasionados por la ocurrencia de un evento potencialmente catastrófico sobre el cual no se ejerce ningún tipo de control.

Nivel de Riesgo:

Probabilidad: Alta

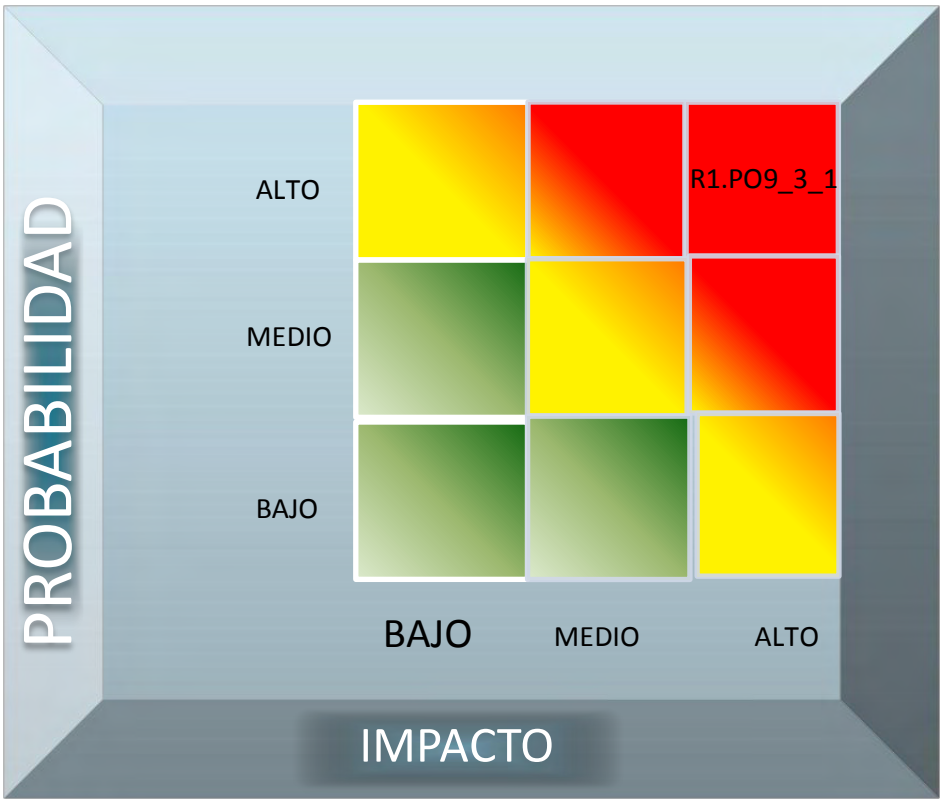
Impacto: Alta

Nivel de Madurez: 3

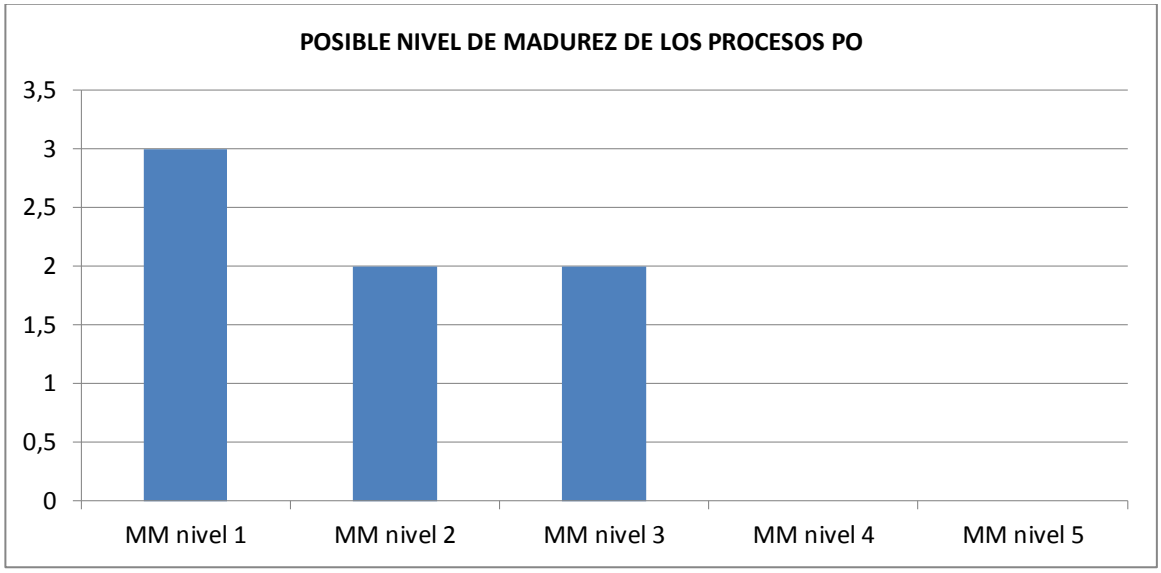
Evidencias:

ENT_PO9_3_1

Tabla 15. Matriz de probabilidad e impacto PO9



R1PAIA Daños físicos y lógicos, ocasionados por la ocurrencia de un evento potencialmente catastrófico sobre el cual no se ejerce ningún tipo de control.



Dominio – Adquisición e implementación (AI): Dentro del dominio de Adquisición e Implementación (AI) del COBIT, se seleccionaron los procesos AI3. Adquisición y mantenimiento de la infraestructura tecnológica, AI6. Administración de cambios, para ser evaluados, los hallazgos o las no conformidades detectadas están clasificados y agrupados por cada uno de los procesos.

AI3.Adquisicion y mantenimiento de la infraestructura tecnológica Evaluación de riesgos: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 16. Hallazgo Adquisición e Implementación AI3_3_1

	HALLAZGOS			REF
				PLAN AI3_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Hallazgo:

No existe en la Ips Indígena Guáitara un documento que brinde soporte y sirva de guía para la realización del proceso de adquisición de software y hardware.

Recomendaciones:

Debe existir en la Ips Indígena Guáitara un documento que describa cual debe ser el proceso a seguir para la adquisición de software y hardware, el proceso correcto es:

_Realización de una solicitud formal que describa las características o requerimientos que debe cumplir el software o el hardware que se va a adquirir.

_Se deben solicitar por lo menos tres cotizaciones diferentes de los productos a adquirir

_Análisis (mediante cuadros comparativos) de las cotizaciones y elección de la propuesta (costo/beneficio) para la entidad.

Estas políticas deben ser de conocimiento general, para garantizar la transparencia en estos procesos.

	HALLAZGOS			REF
				PLAN AI3_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Consecuencia:

La no existencia de un documento que brinde soporte claro sobre cómo debe ser el proceso de adquisición de software y hardware, genera que este proceso se pueda llevar a cabo irregularmente. Estas irregularidades serán evaluadas por los entes de control.

Nivel de Riesgo:

Probabilidad: Media

Impacto: Medio

Nivel de Madurez: 2

Evidencias:

ENT_AI3_3_1

Tabla 17. Hallazgo Adquisición e Implementación AI3_3_2

	HALLAZGOS			REF PLAN AI3_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Hallazgo:

Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios del Sistema de Información no están documentadas.

Recomendaciones:

Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios que interactúan con el Sistema de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

_Instalación, configuración y actualización de los programas antivirus.

_Revisión periódica del estado de los programas antivirus.

_Escaneo periódico de la terminales de trabajo utilizando los programas antivirus.

_Desfragmentación periódica de los discos duros de las terminales de trabajo.

_Limpieza física de los equipos de trabajo utilizando sopladora, cremas y productos químicos especializados

	HALLAZGOS			REF
				PLAN AI3_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Consecuencia:

El desconocimiento por parte de los usuarios encargados de realizar el proceso de mantenimiento preventivo, de los procesos que deben realizar para llevar a cabo este trabajo, puede generar el deterioro y daño de las terminales de trabajo de los usuarios que interactúan con el Sistema de Información.

Nivel de Riesgo:
Probabilidad: Media
Impacto: Medio
Nivel de Madurez: 2

Evidencias:
ENT_AI3_3_2

Tabla 18. Hallazgo Adquisición e Implementación AI3_3_3

	HALLAZGOS			**REF** **PLAN AI3_3_3**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Hallazgo:
Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios del Sistema de Información no están documentadas.

Recomendaciones:
Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios que interactúan con el Sistema de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

_Pruebas de funcionamiento de cada uno de los dispositivos (CPU, RAM, board, tarjeta de red, tarjeta de video, etc.) que conforman la terminal de trabajo.
_Reparación del dispositivo defectuoso.
_Reemplazo del dispositivo defectuoso.
_Pruebas de funcionamiento de la terminal una vez realizados el mantenimiento.

	HALLAZGOS			REF
				PLAN AI3_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Consecuencia:
El desconocimiento por parte de los usuarios encargados de realizar el proceso de mantenimiento correctivo, de los procesos que deben realizar para llevar a cabo este trabajo, puede generar daños físicos en las terminales de trabajo de los usuarios que interactúan con el Sistema de Información.

Nivel de Riesgo:
Probabilidad: Media
Impacto: Medio
Nivel de Madurez : 3

Evidencias:
ENT_AI3_3_3

Tabla 19. Hallazgo Adquisición e Implementación AI3_3_4

	HALLAZGOS			REF
				PLAN AI3_3_4
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Hallazgo:

No existe un documento donde se explique a los funcionarios que interactúan con el Sistema de Información, cual es el proceso que deben seguir cuando se presenta un daño en su terminal de trabajo.

Recomendaciones:

El proceso que deben seguir los funcionarios que interactúan con el Sistema de Información, cuando se presente algún tipo de daño en sus terminales de trabajo, debe estar documentado y ser de obligatorio cumplimiento. Este proceso debe contemplar:

_Realización por parte del funcionario responsable del equipo, de una solicitud por escrito para la revisión del equipo.

_Entrega (mediante acta o documento) por parte del funcionario del equipo dañado al personal de mantenimiento.
_Recepción (mediante acta o documento) por parte de personal de mantenimiento del equipo a revisar.
_Revisión y arreglo de acuerdo a las políticas y procedimientos estipulados para estos fines.
_Entrega (mediante acta o documento) por parte del personal de mantenimiento y recepción por parte del funcionario que reporto el daño, del equipo de cómputo ya reparado.

	HALLAZGOS			REF
				PLAN AI3_3_4
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Consecuencia:

La no existencia de un procedimiento claro a realizar en caso de presentarse algún tipo de daño en una terminal de trabajo, puede ocasionar demoras e inconformidades en el proceso de reparación del equipo.

Nivel de Riesgo:
Probabilidad: Baja
Impacto: Bajo
Nivel de Madurez: 2

Evidencias:
ENT_AI3_3_4

Tabla 20. Hallazgo Adquisición e Implementación AI3_3_5

	HALLAZGOS			REF PLAN AI3_3_5
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Hallazgo:

No existe en la Ips Indígena Guáitara, un manual de funciones para el personal de TI encargado de realizar el mantenimiento preventivo y correctivo de los equipos de cómputo.

Recomendaciones:

Debe existir en la entidad un manual de funciones para el personal de TI, que tiene a su cargo la realización de los procesos de mantenimiento preventivo y correctivo de los equipos de cómputo. Este manual debe contener

_Descripción del cargo.
_Descripción de las funciones y responsabilidades.
_Descripción del perfil del usuario que va a desempeñar el cargo.

	HALLAZGOS			REF
				PLAN AI3_3_5
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Consecuencia:

La no existencia de un manual de funciones para el personal de TI encargado de realizar los procesos de mantenimiento preventivo y correctivo de los equipos de cómputo, puede generar daños físicos o lógicos en las terminales de trabajo, producto de procedimientos mal realizados.

Nivel de Riesgo:

Probabilidad: Media
Impacto: Medio
Nivel de Madurez: 3

Evidencias:

ENT_AI3_3_5

Tabla 21. Hallazgo Adquisición e Implementación AI3_3_6

	HALLAZGOS			REF PLAN AI3_3_6
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

Hallazgo:
No existe dentro del personal de TI, un funcionario experto en el manejo (configuración, reparación, etc.) de redes de datos.

Recomendaciones:
Debe existir dentro de la entidad debe haber un funcionario de absoluta idoneidad profesional, encargado de la red de datos que soporta el normal funcionamiento del Sistema de Información de la Ips Indígena Guáitara.

Tabla 22. Hallazgo Adquisición e Implementación AI3_3_**6**

	HALLAZGOS			**REF** **PLAN AI3_3_6**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Adquisición y Mantenimiento de la Infraestructura Tecnológica(AI3)	

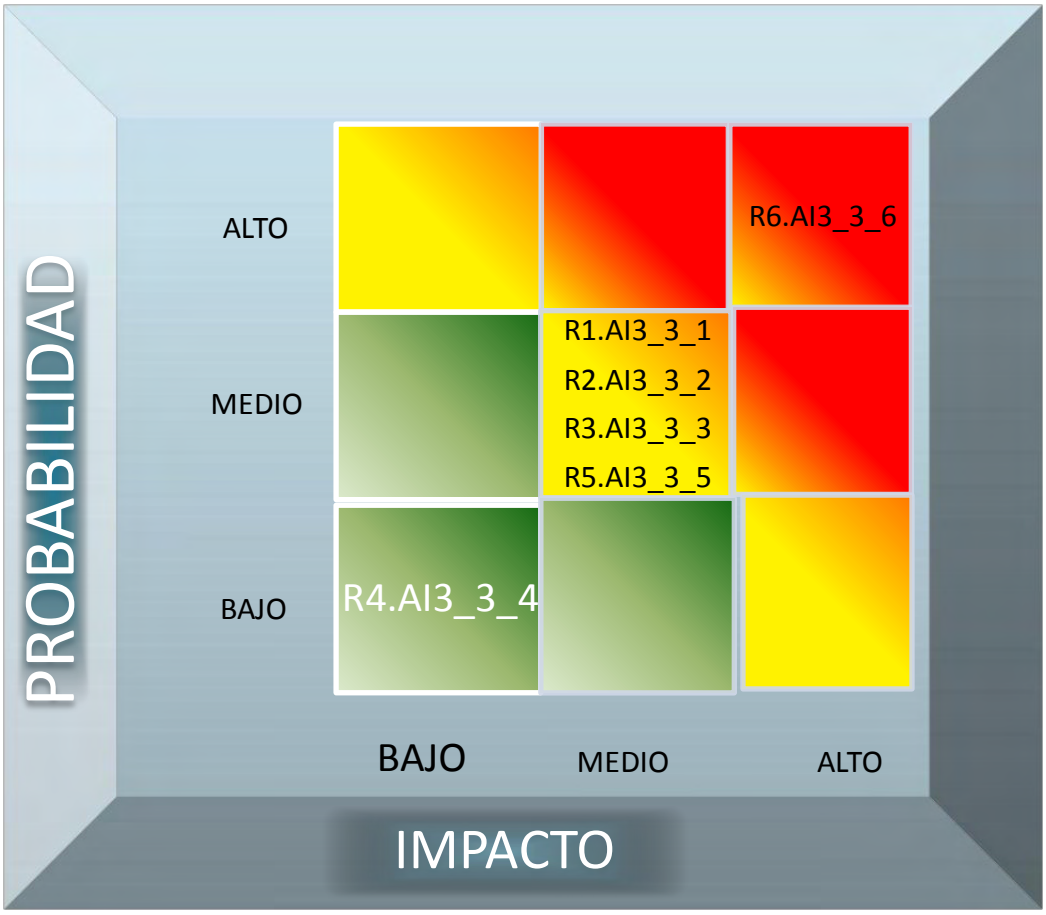
Consecuencia:

La no existencia dentro del personal de TI de un funcionario especialista en el manejo, configuración y mantenimiento de redes de datos, puede ocasionar la parálisis total del Sistema de Información, cuando se presente un daño en la red que soporta su funcionamiento.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 1

Evidencias:
ENT_AI3_3_6

Tabla 23. Matriz de probabilidad e impacto AI3



R1PMIM Proceso de adquisición de infraestructura tecnológicas se pueda llevar a cabo irregularmente.

R2PMIM Generar el deterioro de las terminales de trabajo.

R3PMIM Generar daños físicos en las terminales de trabajo.

R4PBIB Demoras e inconformidades en el proceso de reparación del equipo.
R5PMIM Daños físicos o lógicos en las terminales de trabajo, producto de procedimientos mal realizados.

R6PAIA Parálisis total del Sistema Integral de Información, cuando se presente un daño en la red que soporta su funcionamiento.

AI6. Administración de cambios: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 24. Hallazgo Adquisición e Implementación AI6_3_1

	HALLAZGOS			REF
				PLAN AI6_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Administración de Cambios (AI6)	

Hallazgo:

No existen políticas y/o procedimientos para la administración de los cambios en el Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

Deben existir políticas y/o procedimientos claros para la administración de los cambios dentro del Sistema de Información. El proceso que se debe realizar debe contemplar:

_Realización de una solicitud formal de cambios, por parte del interesado, esta debe contener la justificación del cambio.
_Priorización de las solicitudes de cambios.
_Acceso por parte del programador al código fuente para la realización del cambio
_Finalización por parte del programador del cambio.
_Solicitudes para realización de pruebas.
_Finalización del proceso de pruebas de aceptación.
_Determinación y aceptación del impacto causado por el cambio.
_Actualización de la documentación para registrar el cambio.

	HALLAZGOS			REF PLAN AI6_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Administración de Cambios (AI6)	

Consecuencia:
La no existencia de unas políticas y/o procedimientos claros para la administración del los cambios realizados dentro del Sistema de Información, puede generar que los cambios alteren el buen funcionamiento del sistema, porque no se sometieron a un proceso de análisis antes de realizarlos.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 2

Evidencias:
ENT_AI6_3_1

Tabla 25. Hallazgo Adquisición e Implementación AI6_3_2

	HALLAZGOS			REF
				PLAN AI6_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Administración de Cambios (AI6)	

Hallazgo:

No existen bitácoras de registros de cambios realizados al Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:

Deben existir bitácoras donde se registren y se lleve un control de los cambios realizados a través del tiempo al Sistema de Información de la Ips Indígena Guáitara . Estas bitácoras deben contener:

_Fecha de solicitud del cambio
_Persona que solicita el cambio.
_Soporte (motivo) para solicitar cambio.
_Cambios realizados - personal de Tecnologías de la Información.
_Aprobación de cambios realizados – usuario solicitante.
_Fecha de actualización de la documentación.

	HALLAZGOS			REF
				PLAN AI6_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Administración de Cambios (AI6)	

Consecuencia:
La no existencia de bitácoras de registro de los cambios realizados al Sistema de Información de la Ips Indígena Guáitara, puede generar retrasos en la realización de un ajuste importante dentro del sistema, puesto que el personal encargado de realizar dicho proceso no tiene documentos de consulta sobre los cambios realizados, teniendo que entrar a revisar y analizar el código fuente del aplicativo.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 0

Evidencias:
ENT_AI6_3_2

Tabla 26. Hallazgo Adquisición e Implementación AI6_3_3

	HALLAZGOS			REF PLAN AI6_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Administración de Cambios (AI6)	

Hallazgo:

No existe dentro del personal de TI de la Ips Indígena Guáitara, un funcionario especializado y encargado de la realizar el mantenimiento y los cambios al Sistema de Información.

Recomendaciones:

Debe existir dentro del personal de TI, un funcionario de absoluta idoneidad profesional encargado de llevar a cabo el mantenimiento del Sistema de Información y la realización de los ajustes al código fuente del mismo. Es recomendable que este funcionario sea de carrera administrativa, para que el conocimiento adquirido continúe dentro de la entidad.

	HALLAZGOS			REF PLAN AI6_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Adquisición e Implementación(AI)	**PROCESO**	Administración de Cambios (AI6)	

Consecuencia:

La no existencia de un funcionario dentro de la planta del personal de TI especializado y encargado de realizar el mantenimiento y los cambios o ajustes al código fuente del Sistema de Información, limita la realización de estos procedimientos a la celebración de contratos, con las implicaciones en tiempo y costo que esto con lleva.

Nivel de Riesgo:

Probabilidad: Alta

Impacto: Alto

Nivel de Madurez: 3

Evidencias:

ENT_AI6_3_3

	HALLAZGOS			REF
				PLAN AI6_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Asegurar el Servicio Continuo (DS4)	

Hallazgo:

No existen políticas, procedimientos y/o estrategias dentro de la Ips Indígena Guáitara para garantizar la continuidad de los servicios de TI para el Sistema de Información.

Recomendaciones:

Deben existir en la Ips Indígena Guáitara políticas, estrategias o procedimientos para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema de Información. Estas políticas deben:

_Contemplar la existencia de un marco de referencia.

_Estar alineadas con la estrategia de continuidad del negocio.

_Contemplar la identificación de los procesos críticos y el análisis del impacto estos procesos.

_Garantizar la existencia de un Plan de Continuidad, que contenga:

*Guía de cómo utilizar el plan.

*Procedimientos de emergencia para asegurar la seguridad del personal, incluyendo procedimientos de evacuación.
*Condiciones para declarar un desastre.

*Identificación de los procesos de negocio críticos y recursos de TI que deben ser recuperados

	HALLAZGOS			REF
				PLAN AI6_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Asegurar el Servicio Continuo (DS4)	

Recomendaciones:

*Identificación crítica de personas afectadas y de los responsables por cada función del Plan.
*Explicación paso por paso de los procedimientos de respuesta que incluyen los procedimientos de operación en caso de emergencia.
*Procedimientos de comunicación con empleados, autoridades y comunidad en general.

_Identificar estrategias de continuidad.
_Garantizar que el almacenamiento de la información y los recursos críticos para garantizar la continuidad del sistema, fuera de las instalaciones de la Ips Indígena Guáitara.
_Realizar de pruebas y la actualización del Plan de Continuidad.
_Garantizar el entrenamiento a los usuarios y la distribución del Plan de Continuidad.
_Estar documentadas.
_Ser de conocimiento de todos los funcionarios comprometidos en el proceso.

	HALLAZGOS			REF
				PLAN AI6_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				3 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Asegurar el Servicio Continuo (DS4)	

Consecuencia:

La no existencia de políticas, procedimientos y/o estrategias dentro de la Ips Indígena Guáitara, para garantizar la continuidad de los servicios de TI para el Sistema de Información, puede generar el cese total de actividades, en caso de presentarse un evento potencialmente catastrófico.

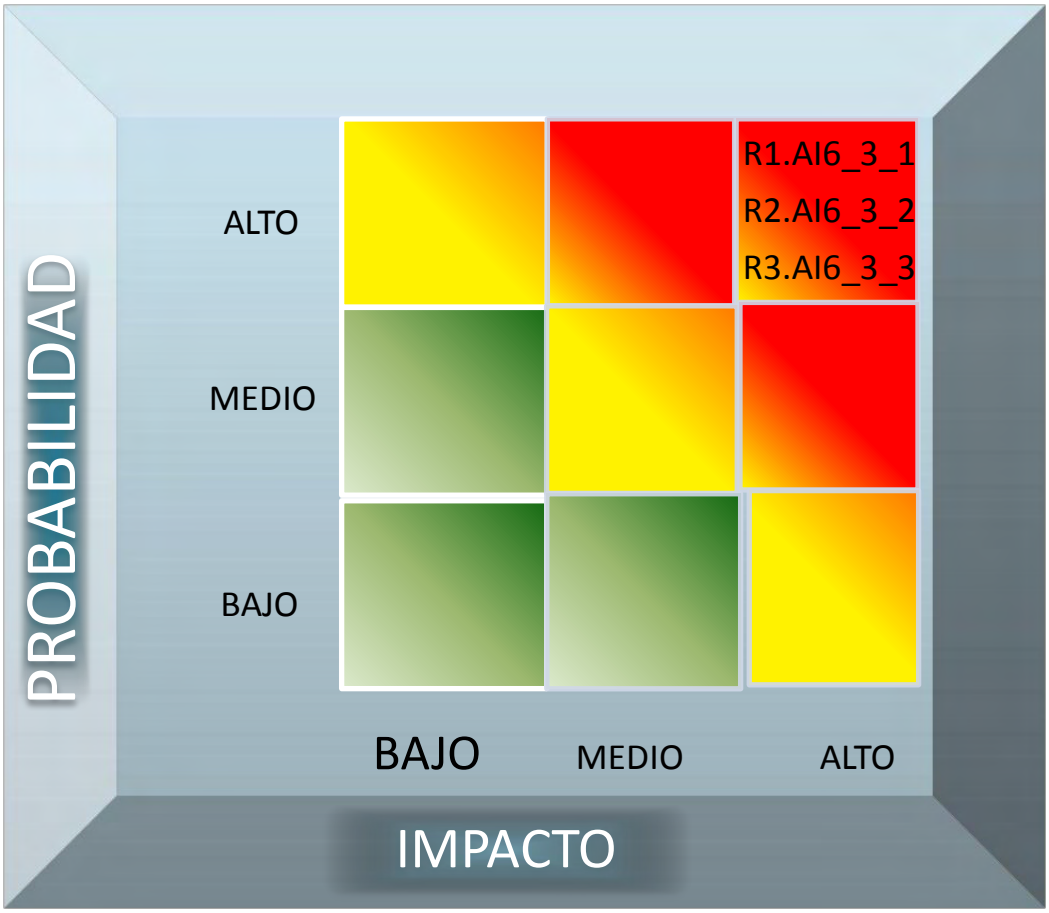
Nivel de Riesgo:

Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 3

Evidencias:

ENT_AI6_3_3

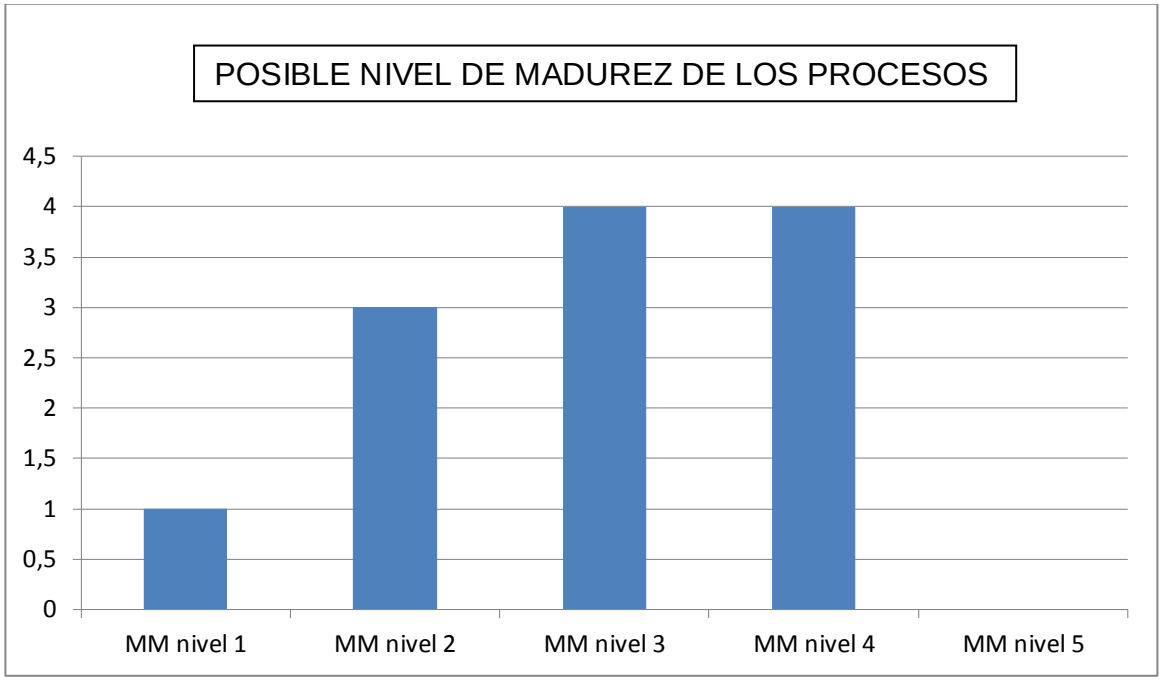
Tabla 27. Matriz de probabilidad e impacto AI6



R1PAIA Generar que los cambios alteren el buen funcionamiento del sistema, porque no se sometieron a un proceso de análisis antes de realizarlos.

R2PAIA Generar retrasos en la realización de un ajuste importante dentro del sistema.

R3PAIA Se limita la realización de procedimientos de ajustes al sistema a la celebración de contratos con terceros



Dominio – Entrega de servicios y soporte (DS): Dentro del dominio de Entrega de Servicios y Soporte (DS) del COBIT, se seleccionaron los procesos, DS5. Garantizar la seguridad de sistemas, DS9 Administración de la configuración, DS11. Administración de los datos, DS12. Administración de las instalaciones, para ser evaluados, los hallazgos o las no conformidades detectadas están clasificadas y agrupadas por cada uno de los procesos.

DS5 Garantizar la seguridad de los sistemas: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 28. Hallazgo Entrega de servicio y Soporte DS5_3_1

	HALLAZGOS			**REF** **PLAN DS5_3_1**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Hallazgo:
No existen políticas globales dentro de la Ips Indígena Guáitara, para garantizar la seguridad lógica de los Sistemas de Información que se manejan en la entidad.

Recomendaciones:
Deben existir en la Ips Indígena Guáitara políticas, estrategias o procedimientos para garantizar la continuidad de los servicios de TI para el Sistema de Información. Estas políticas deben:

_Autenticación y acceso
_Administración de perfiles de usuario y clasificación de la seguridad de datos
_Reportes y revisión de las violaciones e incidentes de seguridad.
_Aplicación de Estándares de administración de llaves criptográficas.
_Detección, resolución y comunicación sobre los virus.
_Clasificación y propiedad de los datos.
Estas políticas deben estar documentadas y ser de obligatoria cumplimiento.

	HALLAZGOS			REF PLAN DS5_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Consecuencia:

La no existencia dentro de la Ips Indígena Guáitara , de políticas orientadas a garantizar la seguridad lógica de la información, puede generar daños y perdidas de la misma, lo que afectaría el normal funcionamiento de las diferentes dependencias que utilizan Sistemas de Información como herramientas para realizar sus funciones y brindar un excelente atención a la comunidad.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 2

Evidencias:
ENT_DS5_3_1

Tabla 29. Hallazgo Entrega de servicio y Soporte DS5_3_2

	HALLAZGOS			REF PLAN DS5_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Hallazgo:
No existen políticas dentro de la Ips Indígena Guáitara para la creación y administración de las contraseñas que diariamente emplean los usuarios para acceder e interactuar con el Sistema de Información.

Recomendaciones:
Deben existir políticas dentro de la Ips Indígena Guáitara que reglamenten la creación y administración de contraseñas para acceder al Sistema de Información. Estas políticas deben contemplar:

_Cambio inicial de las contraseñas la primera vez de uso.
_Establecer una longitud adecuada mínima de las contraseñas.
_Combinaciones de alfanuméricas obligatorias en las contraseñas.
_Verificación de la contraseña en la lista de valores no permitidos
_Cambio periódico de las contraseñas.
_Protección adecuada de las contraseñas.
Estas políticas deben estar documentadas, deben ser de conocimiento de los usuarios que interactúan con el Sistema de Información y deben ser de obligatorio cumplimiento.

	HALLAZGOS			REF PLAN DS5_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Consecuencia:

La no existencia de políticas para la creación y administración de contraseñas para los usuarios que interactúan con el Sistema de Información dentro de la Ips Indígena Guáitara, puede generar que personal no autorizado descifre con facilidad las contraseñas (utilizando algunos métodos conocidos como p. ej. fuerza bruta) e ingrese al sistema, buscando sabotear o robar información.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 3

Evidencias:
ENT_DS5_3_2

Tabla 29. Hallazgo Entrega de servicio y Soporte DS5_3_3

	HALLAZGOS			**REF** **PLAN DS5_3_3**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Hallazgo:
Los procesos que actualmente utiliza el Sistema de Información para realizar la autenticidad de los usuarios, son básicos y no ofrecen altos niveles de seguridad.

Recomendaciones:
Los procesos para autenticidad de los usuarios dentro del Sistema de Información deben cumplir con:

_Uso de contraseñas que se ajusten a las políticas establecidas para la creación y administración de las mismas.
_Usuario suspendido después de 'n' intentos (valor recomendado entre 3 y 5) de entrada fallidos.
_El tiempo para realizar la autenticación de usuario se limita.
_El número de secciones concurrentes correspondientes a un mismo usuario deben estar limitadas.

	HALLAZGOS			REF PLAN DS5_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Consecuencia:

Las actuales y elementales medidas para el control del acceso al Sistema de Información, pueden ocasionar que personal no autorizado vulnere éstas y logre tener acceso con fines de sabotaje, robo o alteración de la información.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 4

Evidencias:
ENT_DS5_3_3

Tabla 30. Hallazgo Entrega de servicio y Soporte DS5_3_4

	HALLAZGOS			REF PLAN DS5_3_4
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Hallazgo:
El servidor que soporta el funcionamiento del Sistema de Información, carece de:
_Un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.).
_Un sistema de firewall físico

Recomendaciones:
Para garantizar la seguridad lógica de la información almacenada en el servidor, éste debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.

_La elección del firewall físico (de varios existentes en el mercado) debe ajustarse a las necesidades y al presupuesto de la Ips Indígena Guáitara.

	HALLAZGOS			REF
				PLAN DS5_3_4
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Garantizar la seguridad de sistemas (DS5)	

Consecuencia:

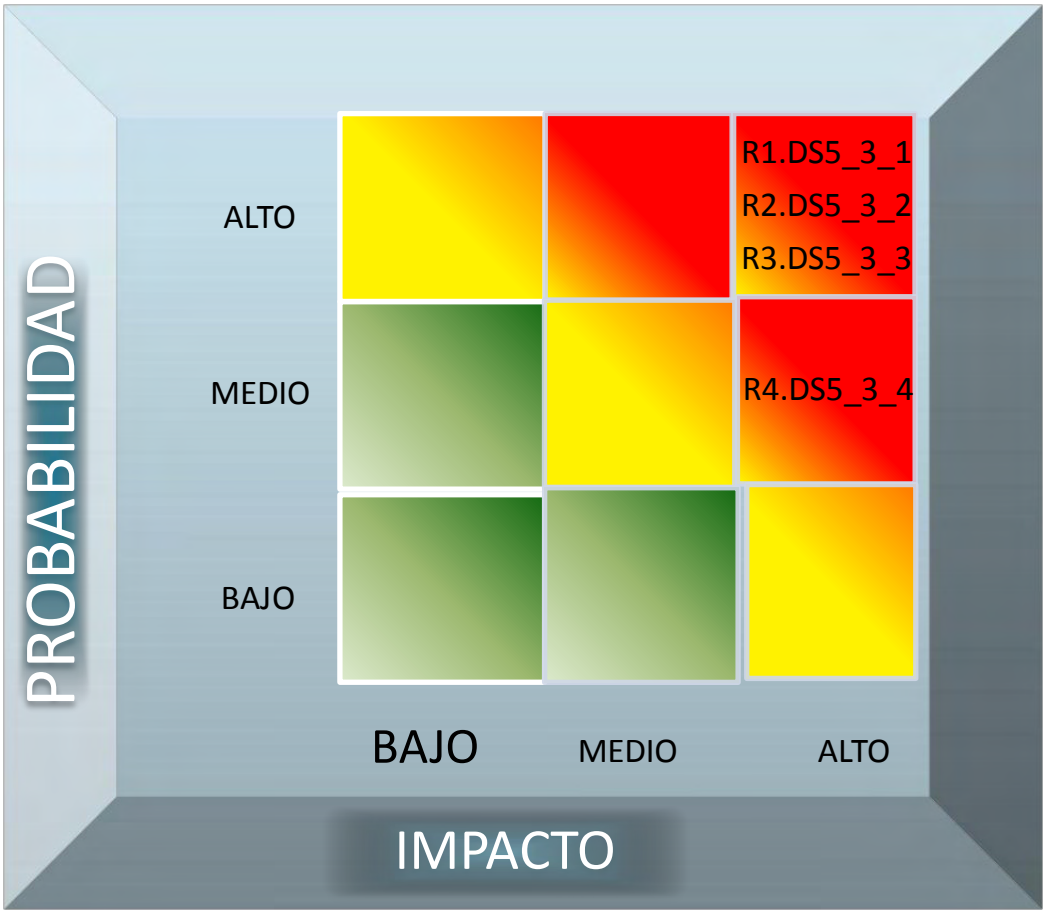
La no existencia de un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.), dentro del servidor en donde se encuentra instalado el Sistema de Información con su respectiva base de datos, genera que la información este expuesta a sufrir daños o alteraciones por la acción de uno de estos programas.

La no existencia de un sistema de firewall físico, hace más vulnerable al servidor para ser víctima de acceso no autorizado, con fines de sabotaje, alteración o robo de información.

Nivel de Riesgo:
Probabilidad: Media
Impacto: Alto
Nivel de Madurez: 0

Evidencias:
ENT_DS5_3_4

Tabla 31. Matriz de probabilidad e impacto DS5



R1PAIA Daños y perdidas de la información
R2PAIA Personal no autorizado descifre con facilidad las contraseñas e ingrese al sistema, buscando sabotear o robar información.
R3PAIA
Personal no autorizado vulnere las actuales medidas de seguridad (básicas) y logre tener acceso al Sistema de Información con fines de sabotaje, robo o alteración de la información.
R4PMIA La no existencia de un sistema de firewall físico, hace más vulnerable al servidor para ser víctima de acceso no autorizado, con fines de sabotaje, alteración o robo de información.

DS9 Administración de la configuración: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 32. Hallazgo Entrega de servicio y Soporte DS9_3_1

	HALLAZGOS			REF PLAN DS9_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de la Configuración (DS9)	

Hallazgo:
No existe un inventario detallado y completo sobre la configuración del servidor en donde se encuentra instalado el Sistema de Información y su respectiva base de datos.

Recomendaciones:
Debe existir en la Ips Indígena Guáitara, un inventario detallado de la configuración del servidor en donde se encuentra instalado el Sistema de información. Este inventario debe estar conformado por:
_Información referente a la configuración del Sistema Operativo.
_Información referente a la configuración del software de aplicación (bases de datos, servidores Web, servidores Proxy, etc.)
_Información referente a licencias de los programas instalados.
_Información referente al hardware instalado.

	HALLAZGOS			REF PLAN DS9_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de la Configuración (DS9)	

Consecuencia:

La no existencia de un inventario detallado del servidor donde se encuentra instalado el Sistema de Información, puede generar demoras en el restablecimiento de los servicios que presta en caso de tener que realizar actividades criticas de mantenimiento (formatear, reinstalar sistema operativo, reinstalar Sistema de Información, etc.)

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 1

Evidencias:

ENT_DS9_3_1

Tabla 33. Hallazgo Entrega de servicio y Soporte DS9_3_2

	HALLAZGOS			**REF** **PLAN DS9_3_2**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de la Configuración (DS9)	

Hallazgo:

No existen políticas dentro la Ips Indígena Guáitara que regulen o den pautas sobre qué tipo de software es permitido que se encuentre instalado y funcionado en las terminales de trabajo de los usuarios del Sistema de Información.

Recomendaciones:

Deben existir políticas claras en la Ips Indígena Guáitara, que regulen e identifiquen que tipo de software es permitido que se encuentre funcionando en las terminales de trabajo de los usuarios del Sistema de Información.

Estas políticas deben ser de conocimiento de todos los funcionarios de la dependencia, de obligatorio cumplimiento.

	HALLAZGOS			REF
				PLAN DS9_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de la Configuración (DS9)	

Consecuencia:

La no existencia de políticas que regulen que tipo de software se puede instalar en las terminales de trabajo, deja estas tareas a libre albedrío de los usuarios, esto puede ocasionar que los recursos del sistema este siendo usados de una manera no adecuada (p. ej. Programas para descargar música de Internet)

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 0

Evidencias:
ENT_DS9_3_2

Tabla 34. Hallazgo Entrega de servicio y Soporte DS9_3_**3**

	HALLAZGOS			**REF**
				PLAN DS9_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de la Configuración (DS9)	

Hallazgo:

No existen controles para la administración de la configuración (tanto de software como de hardware) de los equipos de computo dentro de la Ips Indígena Guáitara.

Recomendaciones:

Deben existir procedimientos de control para la administración de la configuración del software y del hardware que se encuentra instalado en las terminales de trabajo de los usuarios que interactúan con el Sistema de Información de la Ips Indígena Guáitara.

Estos controles consisten en:

_Registro en bitácoras de la configuración de los equipos y de los cambios que se realicen tanto en el software como en el hardware.

_Revisiones periódicas para comprobar que software y que hardware se encuentra instalado en las diferentes terminales de trabajo, y comparar con el tipo de elementos autorizados.

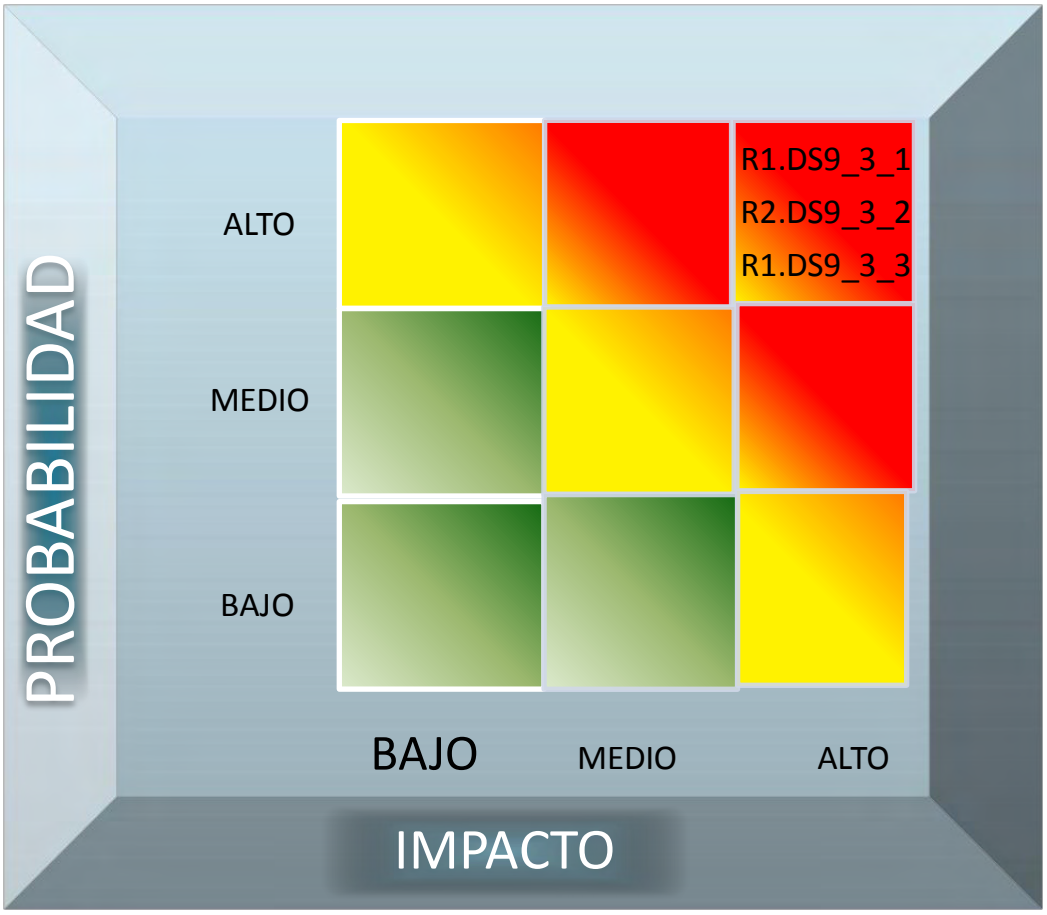
	HALLAZGOS			REF
				PLAN DS9_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de la Configuración (DS9)	

Consecuencia:
La no existencia de controles para vigilar el tipo de software y hardware que se encuentra instalado y funcionando en las terminales de trabajo, puede ocasionar varios problemas, entre ellos:
Mala utilización de los recursos de Tecnologías de la Información (p. ej. Programas para descargar música de Internet).
Robo o cambio de los elementos de tipo hardware de las diferentes terminales de trabajo.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 0

Evidencias:
ENT_DS9_3_3

Tabla 40. Matriz de probabilidad e impacto DS9



R1PAIA Generar demoras en el restablecimiento de los servicios que presta en caso de tener que realizar actividades criticas de mantenimiento (formatear, reinstalar sistema operativo, reinstalar Sistema Integral de Información, etc.)

R2PAIA Los recursos del sistema este siendo usados de una manera no adecuada (p. ej. Programas para descargar música de Internet)

R3PAIA Robo o cambio de los elementos de tipo hardware de las diferentes terminales de trabajo.

DS11 Administración de datos: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 41. Hallazgo Entrega de servicio y Soporte DS11_3_1

	HALLAZGOS			REF PLAN DS11_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de Datos (DS11)	

Hallazgo:

No existen en la Ips Indígena Guáitara documentos que soporten o den pautas sobre cómo debe llevarse a cabo el proceso de realización de las copias de seguridad para el Sistema de Información.

Recomendaciones:

Deben existir dentro de la Ips Indígena Guáitara documentos que soporten las políticas y los procedimientos para la realización de las copias de seguridad del Sistema de Información.
El administrador del Sistema de Información, deberá conocer este documento y aplicar los procedimientos que ahí se describan.

	HALLAZGOS			REF
				PLAN DS11_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indigena “GUAITARA”			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de Datos (DS11)	

Consecuencia:

La no existencia de un documento que soporte los procedimientos para la realización de copias de seguridad del Sistema de Información, genera que el administrador de éste realice procesos de forma empírica y sin seguir ningún tipo de reglas**.**

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel de madurez: 3

Evidencias:
ENT_DS11_3_1

Fuente: Esta Investigación

Tabla 42. Hallazgo Entrega de servicio y Soporte DS11_3_2

	HALLAZGOS			REF
				PLAN DS11_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de Datos (DS11)	

Hallazgo:

No existe un lugar fuera de las instalaciones de la Ips Indígena Guáitara en donde se almacenen bajo estrictas medidas de seguridad, las copias de seguridad del Sistema de Información.

Recomendaciones:

Debe existir fuera de las instalaciones de la Ips Indígena Guáitara un lugar en el cual se almacenen las copias de seguridad del Sistema de Información.

Este lugar debe contar con adecuadas medidas de seguridad, que garanticen la integridad física de los respaldos, entre estas medidas tenemos:

_Accesos únicamente de personal autorizado y debidamente identificado.

_Acceso en horarios autorizados.

_El sitio donde se guarden las copias de seguridad debe contar con personal de vigilancia.

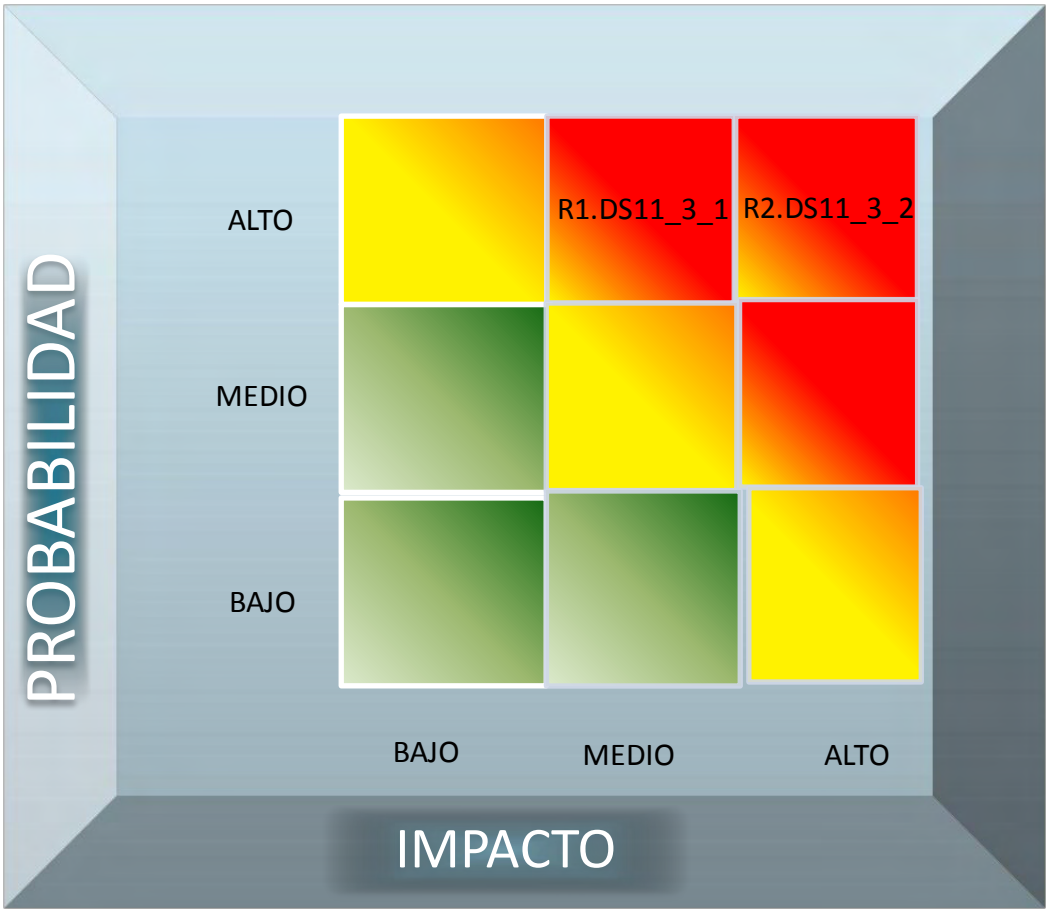
	HALLAZGOS			REF
				PLAN DS11_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indigena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de Datos (DS11)	

Consecuencia:
La no existencia de un lugar fuera de las instalaciones de la Ips Indígena Guáitara en donde se almacenen las copias de seguridad y respaldo del Sistema de Información, puede generar la pérdida parcial o total de los datos, en caso de ocurrir un evento potencialmente catastrófico que afecte la infraestructura física de esta dependencia.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Impacto: 0

Evidencias:
ENT_DS11_3_2

Tabla 43. Hallazgo Entrega de servicio y Soporte DS11



R1PAIM Los procesos de copias de seguridad se realizan de forma empírica y sin seguir ningún tipo de reglas.

R2PAIA Pérdida parcial o total de los datos, en caso de ocurrir un evento potencialmente catastrófico que afecte la infraestructura física de la Ips Indígena Guáitara.

DS12 Administración de las instalaciones: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 44. Hallazgo Entrega de servicio y Soporte DS12_3_1

	HALLAZGOS			**REF** **PLAN DS12_3_1**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:
Los procedimientos de seguridad que actualmente se lleva a cabo para controlar el acceso y la salida de las instalaciones de la entidad , brindan un buen nivel de tipo de seguridad para los activos de TI del Sistema de Información.

Recomendaciones:
Deben existir procedimientos de seguridad para controlar el acceso y la salida de las instalaciones de la Ips Indígena Guáitara. Estos procedimientos deberán asegurar que:
_Todas las personas que entran a las instalaciones de la Ips Indígena Guáitara, se identifique, sean autenticados y autorizados para entrar.
_La realización de requisas a las personas que ingresan y que salen de las instalaciones.
_El registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.
_Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.
_La realización de requisas a los vehículos que ingresan y salen de las instalaciones.

	HALLAZGOS			REF
				PLAN DS12_3_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

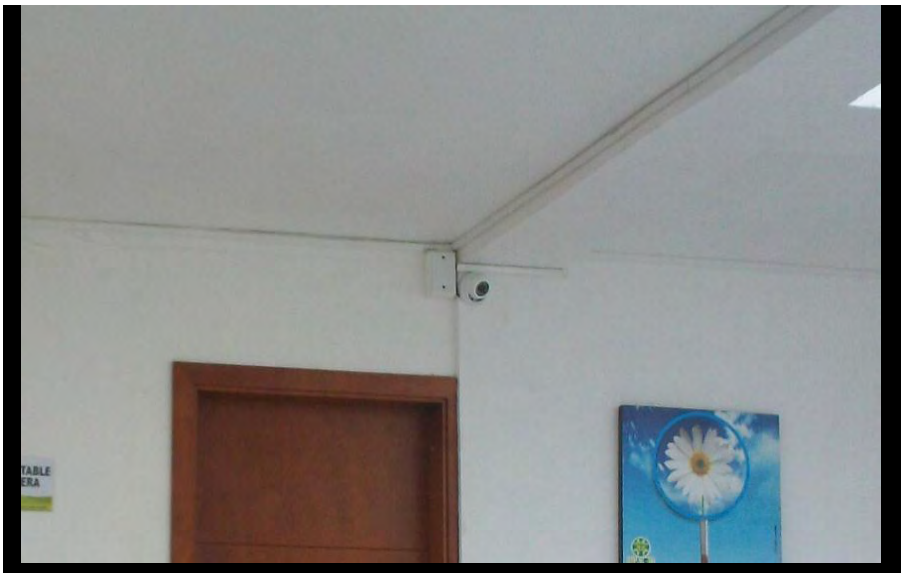
Las buenas medidas de seguridad que actualmente se evidencian en lo referente al acceso y salida de las instalaciones de la Ips Indígena Guáitara, brindan un buen tipo de seguridad para los activos de TI del Sistema de Información, aunque se pueden presentar algunos robos de elementos de tipo hardware (monitores, torres, discos duros, etc.) por falta de algunas cámaras en algunas dependencias.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Medio
Nivel de Madurez: 5

Evidencias:

ENT_DS12_3_1
IMG01_DS12_3_1
IMG02_DS12_3_1

Figura 10. Cámaras de vigilancia (IMG01_DS12_3_1)



REF	IMG03_DS12_3_1

Figura 11. Registro de vigilancia (IMG02_DS12_3_1)

REF	IMG02_DS12_3_1

Tabla 45. Hallazgo Entrega de servicio y Soporte DS12_3_2

	HALLAZGOS			REF PLAN DS12_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:
No existe en las instalaciones de la Ips Indígena Guáitara ni fuera de ellas, un lugar reservado y con las características ambientales y de seguridad para albergar los equipos que soportan el funcionamiento del Sistema de Información.

No existe el centro de cómputo.

Recomendaciones:
Los equipos de computo (servidores, patchpanel, routers, switchs, etc.) que soportan y garantizan el correcto funcionamiento del Sistema de Información deben permanecer en un lugar adecuado (centro de computo) y que satisfaga los requerimientos de:
_Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
_Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
_Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.

	HALLAZGOS			REF
				PLAN DS12_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Recomendaciones:

_Sistemas de ventilación. Las instalaciones del centro de computo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.

_Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios; los materiales del centro de computo son incombustibles (pintura de las paredes, suelo, techos, mesas, estanterías, etc.). Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a las instalaciones.

_Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

	HALLAZGOS			REF
				PLAN DS12_3_2
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				3 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

La no existencia de un centro de computo que cumpla con las características de espacio y movilidad, iluminación, tratamiento acústico, sistemas de ventilación seguridad física y suministro eléctrico, puede ocasionar daños graves en los equipos, lo que se traduciría en la parálisis parcial o total del Sistema de Información.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 2

Evidencias:
ENT_DS12_3_2

Tabla 46. Hallazgo Entrega de servicio y Soporte DS12_3_3

	HALLAZGOS			REF PLAN DS12_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:
No existen medidas de seguridad dentro de las instalaciones de la Ips Indígena Guáitara , para restringir el acceso al lugar donde se encuentran ubicados los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves que soportan y garantizan el buen funcionamiento del Sistema de Información.

Recomendaciones:
El lugar donde se encuentren los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves para el funcionamiento del Sistema de Información debe tener restringido el acceso solamente a personal autorizado.

	HALLAZGOS			REF PLAN DS12_3_3
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

El fácil acceso a los equipos de cómputo claves (servidores, patchpanel, routers, switchs, etc.) para el funcionamiento del Sistema de Información, convierte a estos elementos en un blanco fácil y susceptibles de sufrir robos, daños y sabotajes.

Nivel de Riesgo:

Probabilidad: Alta

Impacto: Alto

Nivel de Madurez: 3

Evidencias:

ENT_DS12_3_3
IMG01_DS12_3_3
ANEXO (VIDEO1_DS12_3_3.MOV)

Figura 12. Personal no autorizado (IMG01_DS12_3_3)

REF	IMG01_DS12_3_3

Tabla 47. Hallazgo Entrega de servicio y Soporte DS12_3_4

	HALLAZGOS			REF PLAN DS12_3_4
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:
Falta de extintores contra incendios dentro de las instalaciones de la Ips Indígena Guáitara.

Recomendaciones:
Dentro de las instalaciones de la Ips Indígena Guáitara se deben ubicar extintores contra incendios en lugares estratégicos y de fácil acceso.

	HALLAZGOS			REF
				PLAN DS12_3_4
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

La no existencia de algunos extintores contra incendios dentro de las Instalaciones de la Ips Indígena Guáitara, puede generar pérdida parcial o total de la información del Sistema de Información, ocasionada por los posibles daños que puedan presentar los equipos de computo después de un incendio que no se pudo controlar, por falta de los elementos de seguridad respectivos.

Nivel de Riesgo:

Probabilidad: Media
Impacto: Alto
Nivel de Madurez: 2

Evidencias:

ENT_DS12_3_4

Tabla 48. Hallazgo Entrega de servicio y Soporte DS12_3_5

	HALLAZGOS			**REF** **PLAN DS12_3_5**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:

Existe señalización en caso de presentarse un evento catastrófico, mas no se cuenta con un plan de evacuación como tal dentro de las instalaciones de la Ips Indígena Guáitara

Recomendaciones:

Algunos requisitos del plan de evacuación se observan en las instalaciones de la Ips Indígena Guáitara tales como:

_En las Instalaciones se cuenta con una señal de alarma (timbre, campana, silbato) que será muy relevante y de fácil reconocimiento por todos los actores institucionales, los cuales ante esta situación se encaminarán hacia la puerta de salida.

_ En las Instalaciones hay señalización las paredes con una flecha roja direccional acompañada de la palabra SALIDA a una altura de 2 m, en corredores, escaleras, rampas, etc.

También se deberá:

_Garantizar una salida rápida y segura hacia el exterior.

_Dar a cargo la toma de decisión de evacuación y orden a una persona responsable

_El trayecto de escape deberá estar libre de obstrucciones o entorpecimiento de circulación.

	HALLAZGOS			**REF** **PLAN DS12_3_5**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Recomendaciones:

_Se establecerán roles y responsabilidades para el personal de la Ips Indígena Guáitara, por ejemplo personal responsable de la utilización de los medios contra incendios -extintores, mangueras-, encargado del botiquín de primeros auxilios, de interrumpir los circuitos eléctricos, de la apertura de las puertas de salida.

_La concentración y desconcentración se realizará a los lugares prefijados (lugares que ofrecen medidas de seguridad aceptables) y conocidos con anterioridad.

_Se deben realizar simulacros de evacuación.

_Los extintores y otros elementos de protección se controlarán periódicamente, y se capacitará al personal acerca de su uso.

El plan de evacuación debe estar documentado y debe ser de conocimiento de todos los funcionarios de la Ips Indígena Guáitara

Tabla 49. Hallazgo Entrega de servicio y Soporte DS12_3_5

	HALLAZGOS			REF
				PLAN DS12_3_5
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indigena "GUAITARA"			**PAGINA**
				3 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

La no existencia de un plan de evacuación de las instalaciones de la Ips Indígena Guáitara en caso de una catástrofe, puede generar que el personal de esta dependencia sufra lesiones de diferentes magnitudes al presentarse un evento de este tipo.

Nivel de Riesgo:

Probabilidad: Media

Impacto: Alto

Nivel de Madurez: 1

Evidencias:

ENT_DS12_3_5
IMG01_DS12_3_5

Figura 13. Avisos de evacuación (IMG01_DS12_3_5)

REF	IMG01_DS12_3_5

Tabla 50. Hallazgo Entrega de servicio y Soporte DS12_3_6

	HALLAZGOS			REF PLAN DS12_3_6
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:
Los sistemas de detección de movimiento no existen actualmente en la Ips Indígena Guáitara.

Los sistemas de cámaras, alarmas y detección de humo se encuentran funcionando correctamente.

Recomendaciones:
Las instalaciones de la Ips Indígena Guáitara debe contar con sistemas de detección de movimiento que estén configurados y en funcionamiento, para brindar seguridad a los activos de TI del Sistema de Información.

	HALLAZGOS			REF
				PLAN DS12_3_7
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

La no existencia de sistemas de detección de moviendo en perfecto estado y funcionando dentro de las instalaciones de la Ips Indígena Guáitara, aumenta la posibilidad de que se presenten robos o sabotajes (perpetrados cuando no hay personal en las instalaciones) a los activos de TI del Sistema de Información.

Nivel de Riesgo:

Probabilidad: Alta

Impacto: Alto

Nivel de Madurez: 2

Evidencias:

ENT_DS12_3_7
IMG01_DS12_3_6

Figura 14. Sensores de humo y cámara (IMG01_DS12_3_6)

REF	IMG01_DS12_3_6

	HALLAZGOS			REF PLAN DS12_3_7
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:

No existen en la Ips Indígena Guáitara medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema de Información.

Recomendaciones:

Deben existir e implementarse medidas de seguridad en la Ips Indígena Guáitara, que garanticen la integridad física de las copias de seguridad del Sistema de Información. Algunas de estas medidas son:

_Los medios de almacenamiento físico (CD, DVD, Cintas Magnéticas, etc.) en donde se encuentran las copias de seguridad del Sistema de Información, deben guardarse bajo llave.
_Solo las personas autorizadas pueden tener acceso a las copias de seguridad.
_Debe existir un sitio fuera de las instalaciones de la Ips Indígena Guáitara, en donde se almacenen las copias de seguridad.
_Los sitios dentro y fuera de las instalaciones de la Ips Indígena Guáitara, que sirvan para almacenar las copias de seguridad, deben contar con factores ambientales (humedad, iluminación, ventilación, etc.) óptimos, que garanticen la integridad de los medios de almacenamiento.

Tabla 51. Hallazgo Entrega de servicio y Soporte DS12_3_7

	HALLAZGOS			REF PLAN DS12_3_7
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

La no existencia de medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema de Información, facilita que personal no autorizado tenga acceso a ellas, con fines de sabotaje, daño o robo.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 1

Evidencias:
ENT_DS12_3_7

Tabla 52. Hallazgo Entrega de servicio y Soporte DS12_3_8

	HALLAZGOS			REF
				PLAN DS12_3_8
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:

El sitio donde se encuentran las UPS (Sistema de Alimentación Ininterrumpida), que aseguran el funcionamiento normal de los equipos de computo claves del Sistema de Información por un determinado tiempo, en caso de presentarse cortes del suministro eléctrico en las instalaciones de la Ips Indígena Guáitara, no es adecuado, y no brinda ningún tipo seguridad para estos elementos.

Recomendaciones:

Los lugares donde se ubiquen los Sistemas de Alimentación Ininterrumpida (UPS) que dan autonomía de funcionamiento a los equipos de computo claves del Sistema de Información, durante un tiempo determinado, en caso de presentarse cortes en el suministro eléctrico, deben cumplir con las condiciones de:

_Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.

_Iluminación. El sistema de iluminación debe ser apropiado para evitar falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.

	HALLAZGOS			REF
				PLAN DS12_3_8
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA**
				2 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Recomendaciones:

_Tratamiento acústico. Los equipos ruidosos como equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.

_Sistemas de ventilación. Las instalaciones deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.

_Seguridad física. Las instalaciones donde se ubique las UPS deben contar con un sistema contra incendios; los materiales deben ser incombustibles. Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.

_Suministro eléctrico. El suministro eléctrico y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias.

	HALLAZGOS			REF
				PLAN DS12_3_8
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA**
				3 de 3
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:

La no existencia de un sitio que cumpla con condiciones optimas para albergar los Sistemas de Alimentación Ininterrumpida (UPS) puede ocasionar daños en estos equipos, lo que podría generar daños en los equipos de computo claves para el funcionamiento del Sistema de Información, en caso de presentarse cortes repentinos del suministro de energía eléctrica

Nivel de Riesgo:

Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 0

Evidencias:

ENT_DS12_3_8
IMG01_DS12_3_8

Figura 15. UPS (IMG01_DS12_3_8)

REF	IMG01_DS12_3_8

Tabla 53. Hallazgo Entrega de servicio y Soporte DS12_3_9

	HALLAZGOS			REF
				PLAN DS12_3_9
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Hallazgo:

No existen en las instalaciones de la Ips Indígena Guáitara, medidas de seguridad o aislamientos que aseguren la integridad física del cableado (UTP, eléctrico, etc.) que no se encuentra integrado a la estructura del edificio.

Recomendaciones:

El cableado (UTP, eléctrico, etc.) que no se encuentre incorporado a la estructura del edificio de la Ips Indígena Guáitara , bebe contar con medidas de aislamiento que garanticen su seguridad y su integridad. Se recomienda el uso de canaletas para proteger estos activos de TI.

				PLAN DS12_3_9
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena “GUAITARA”			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

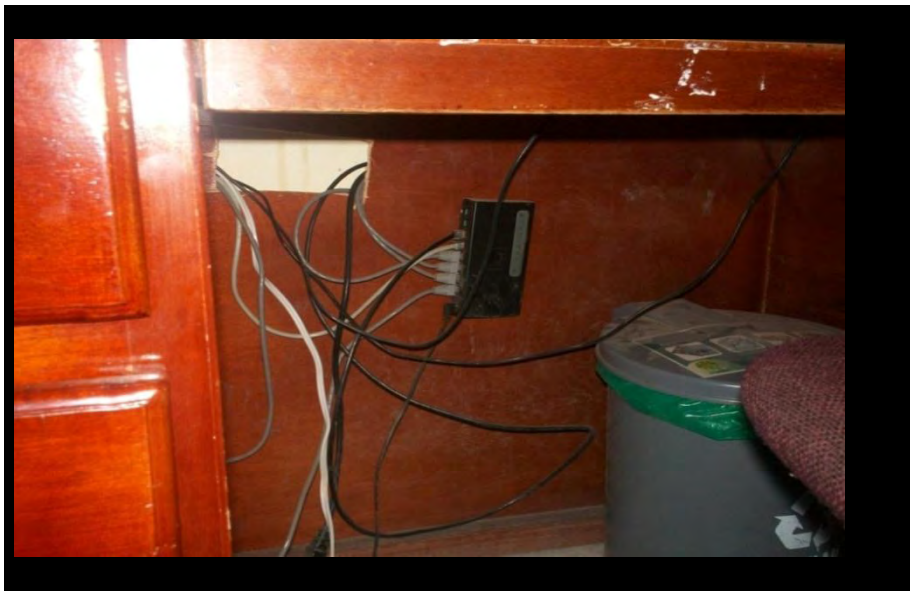
Consecuencia:
La no existencia de medidas de seguridad para proteger y garantizar la integridad física del cableado (UTP, eléctrico, etc.) dentro de las instalaciones de la Ips Indígena Guáitara, puede generar fallos en el funcionamiento del Sistema de Información, ocasionados por daños en el cableado, estos daños pueden ser no intencionados o como resultado de sabotaje.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 1

Evidencias:

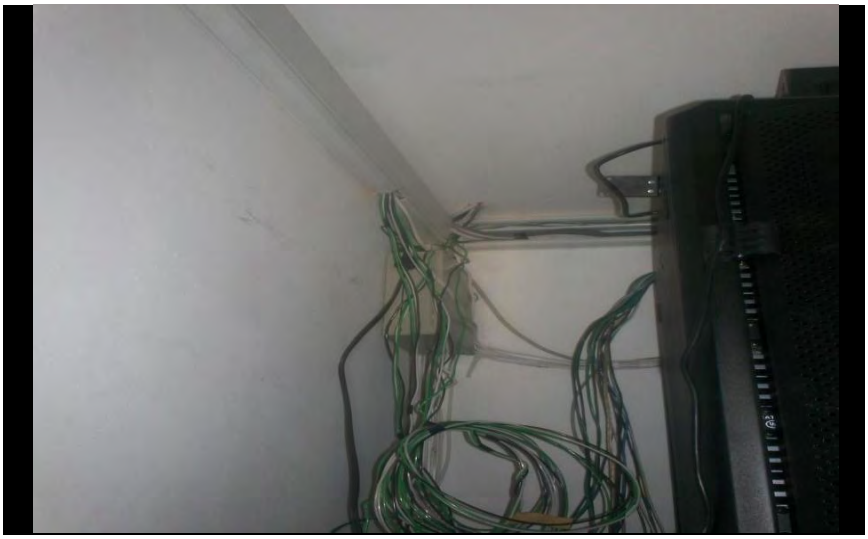
ENT_DS12_3_9
IMG01_DS12_3_9
IMG02_DS12_3_9
IMG03_DS12_3_9
IMG04_DS12_3_9
IMG05_DS12_3_9
IMG06_DS12_3_9

Figura 16. Switch (IMG01_DS12_3_9)



REF	IMG01_DS12_3_9

Figura 17. Distribución de instalaciones (IMG02_DS12_3_9)

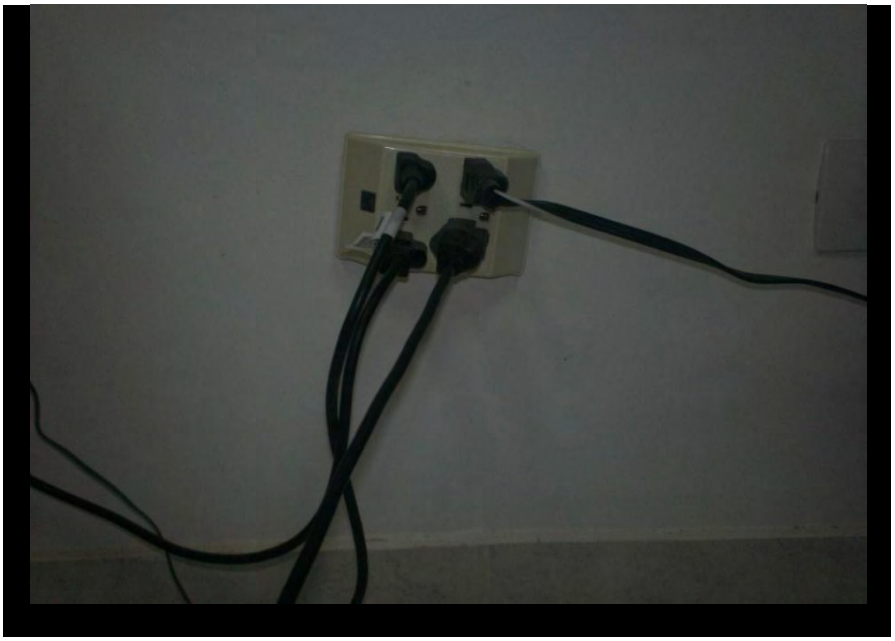


REF	IMG02_DS12_3_9

Figura 18. Conexiones (IMG03_DS12_3_9)

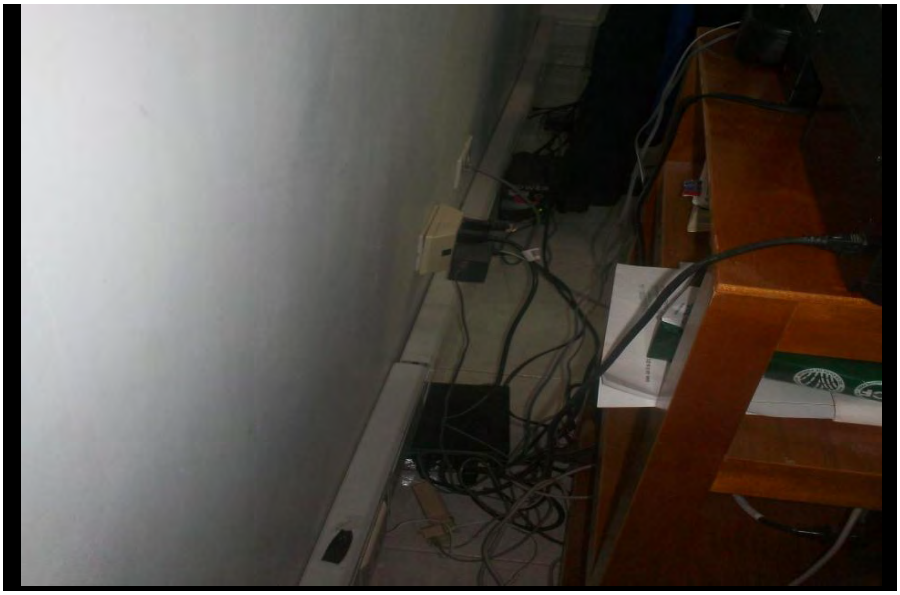
REF	IMG03_DS12_3_9

Figura 19. Conexiones (IMG04_DS12_3_9)



REF	IMG04_DS12_3_9

Figura 20. Cableado UTP (IMG05_DS12_3_9)

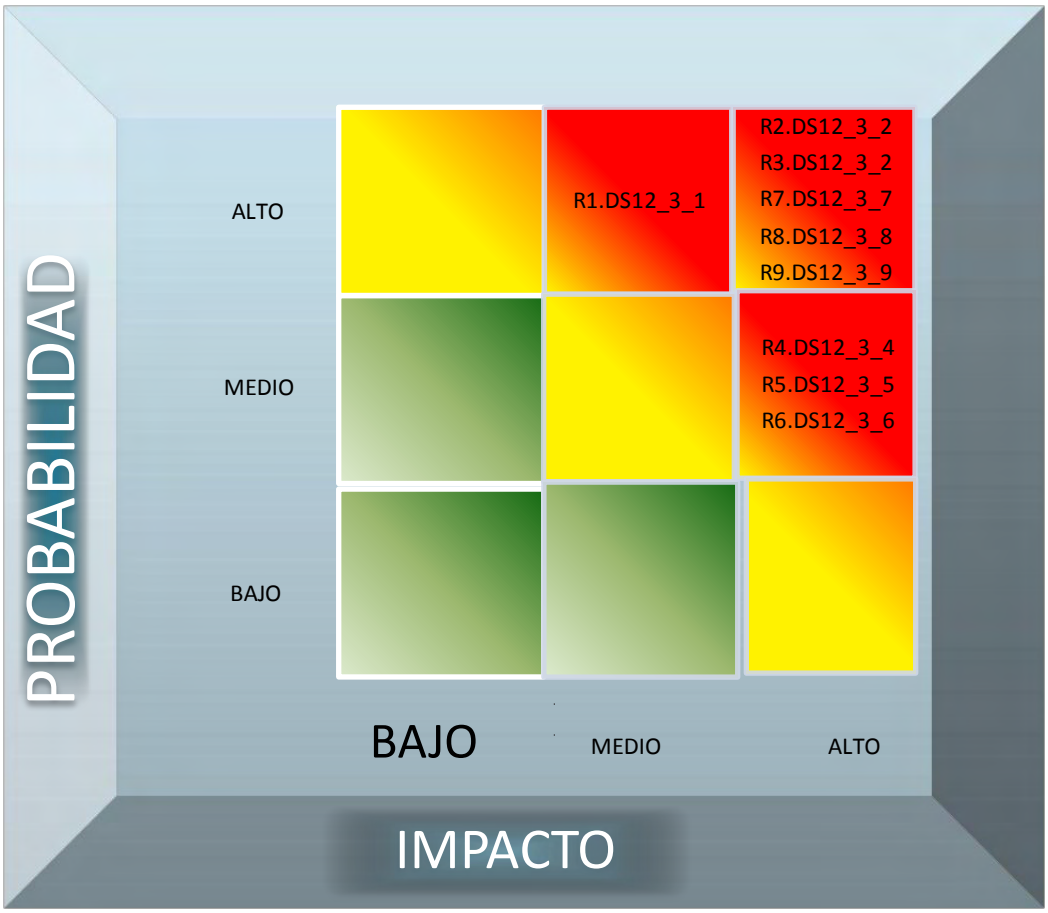


REF	IMG05_DS12_3_9

Figura 21. Canaletas (IMG06_DS12_3_9)

REF	IMG06_DS12_3_9

Tabla 54. Hallazgo Entrega de servicio y Soporte DS12



R1PAIM Se pueden presentar robos de elementos de tipo hardware (monitores, torres, discos duros, etc.).

R2PAIA La parálisis parcial o total del SI, ocasionado por daños graves en los equipos.

R3PAIA Robos, daños y sabotajes a los equipos de cómputo claves.

R4PMIA Perdida parcial o total de la información del SI ocasionada por incendios.

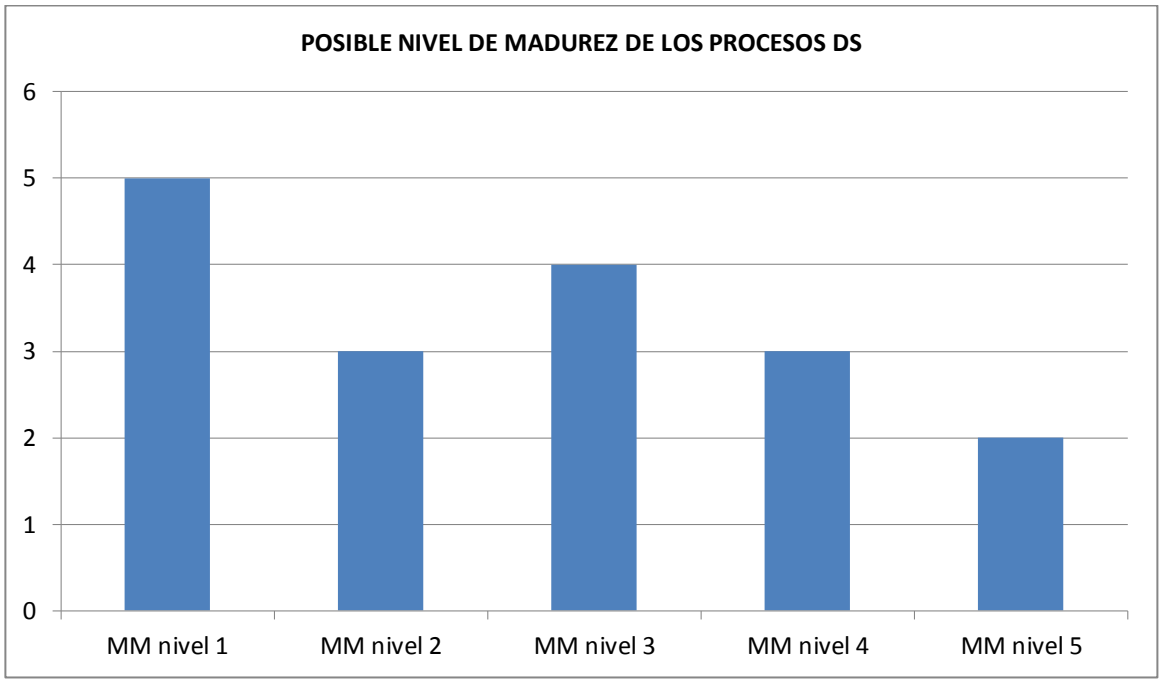
R5PMIA El personal de la Ips Indígena Guáitara está expuesto a sufrir lesiones de diferentes magnitudes al presentarse una erupción volcánica.

R6PMIA Robos o sabotajes (perpetrados cuando no hay personal en las instalaciones) a los activos de TI del Sistema de Información.

R7PAI Fácil acceso a las copias de seguridad del Sistema de Información con fines de sabotaje, daño o robo.

R8PAIA Daños en los equipos de cómputo claves para el funcionamiento del Sistema Integral de Información, en caso de presentarse cortes repentinos del suministro de energía eléctrica.

R9PAIA Fallos en el funcionamiento del Sistema de Información, ocasionados por daños en el cableado.



Dominio – Monitoreo (M): Dentro del dominio de Monitoreo (M) del COBIT, se selecciono el proceso M2. Evaluar lo adecuado del control interno, para ser evaluado, los hallazgos o las no conformidades detectadas están clasificados y agrupados.

M2 Evaluar lo adecuado del control interno: Los hallazgos o no conformidades para este proceso se muestran a partir de la siguiente página.

Tabla 55. Hallazgo Monitoreo ME2_1_1

	HALLAZGOS			REF PLAN ME2_1_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indlgena "GUAITARA"			**PAGINA** 1 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Monitoreo(M)	**PROCESO**	Evaluar lo adecuado del control interno (M2)	

Hallazgo:
No existen políticas y/o procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de TI del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones:
Deben existir políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de TI del Sistema de Información. Las características de estas políticas son:
_Debe existir una descripción detallada de los procedimientos de monitoreo que se deben aplicar dependiendo de la actividad que se desea evaluar.
_Debe existir un cronograma en donde se muestre claramente la periodicidad con que se van a efectuar los procesos de monitoreo de las diferentes actividades.
_Debe existir definición de los funcionarios responsables de realizar las actividades de monitoreo.

Estas políticas deben estar documentadas y deben ser de conocimiento de los funcionarios de TI que intervienen en los procesos de monitoreo.

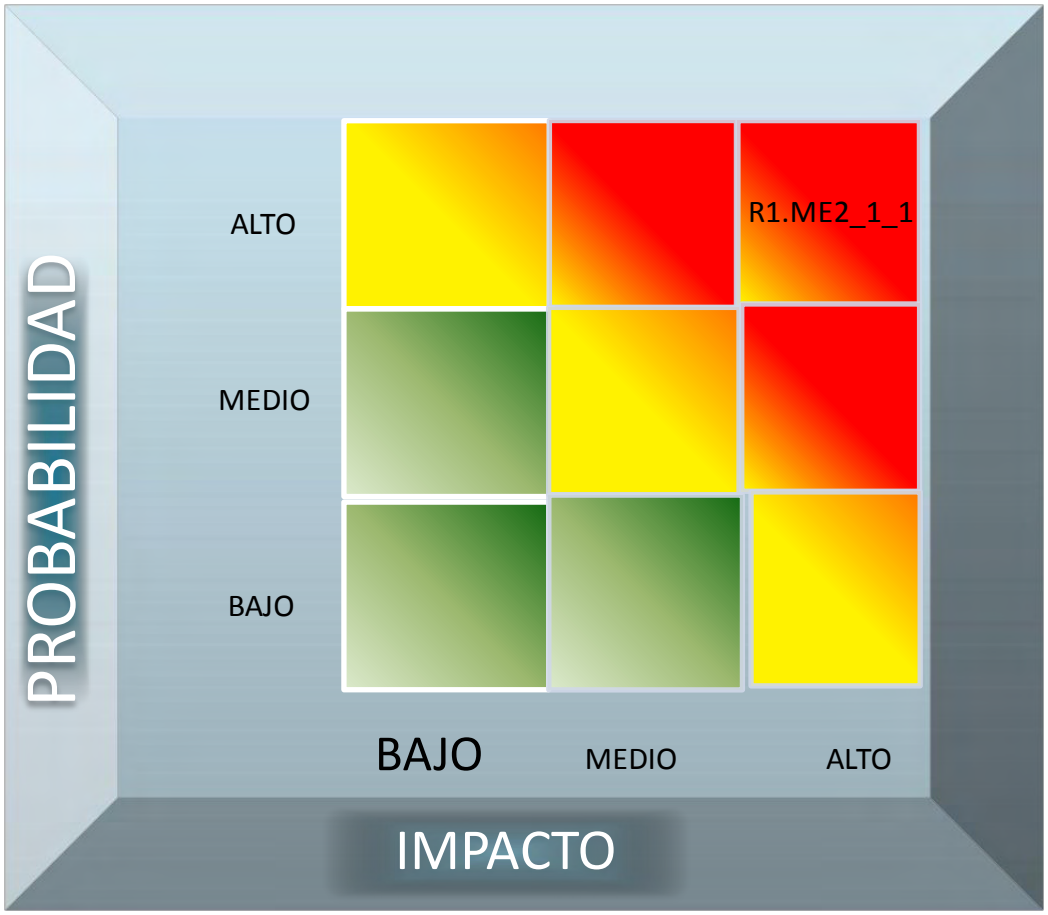
	HALLAZGOS			REF
				PLAN M2_1_1
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA**
				2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Monitoreo(M)	**PROCESO**	Evaluar lo adecuado del control interno (M2)	

Consecuencia:
La no existencia de políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de TI del Sistema de Información, hace imposible la identificación de las falencias que con respecto a estos procesos se presentan en la Ips Indígena Guáitara.

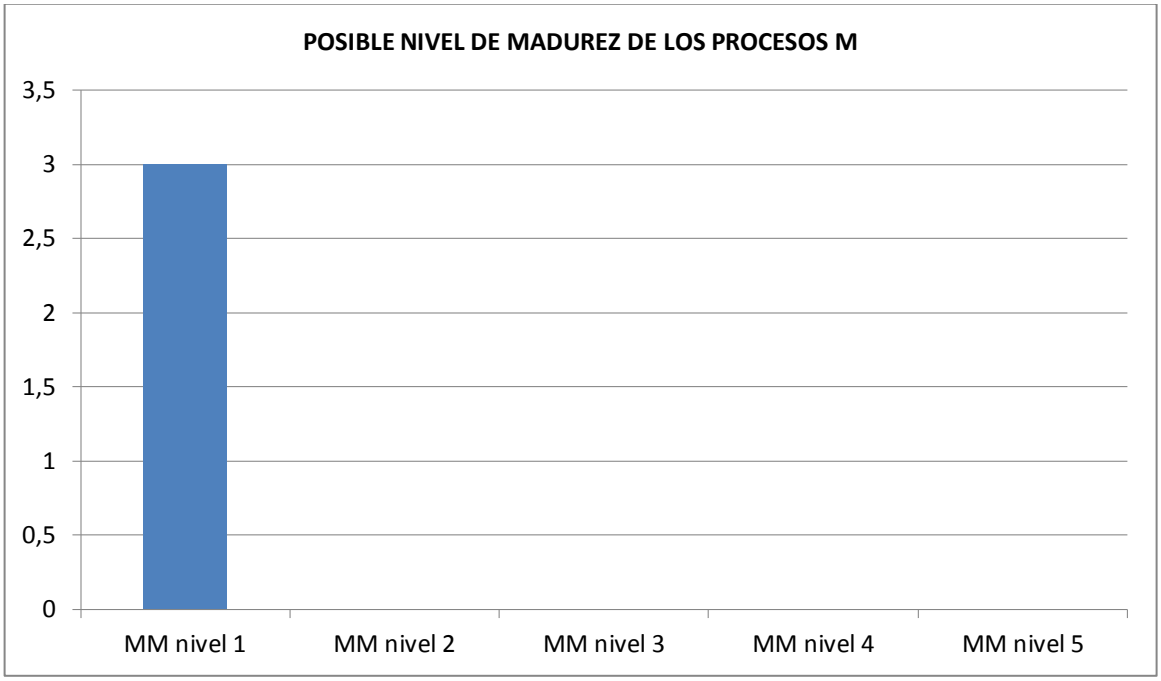
Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 1

Evidencias:
ENT_M2_1_1

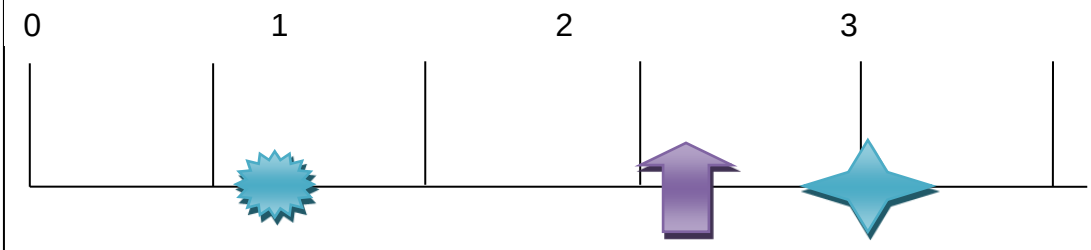
Tabla 56. Matriz de probabilidad e impacto ME



R1PAIA Identificación imposible de las falencias que con respecto a seguridad física y lógica se presentan en el Sistema de Información de la Ips Indígena Guáitara



REPRESENTACIÓN GRAFICA DE LOS MODELOS DE MADUREZ



LEYENDA PARA SÍMBOLOS USADOS

Estado actual de la institución

Promedio de la institución

Objetivo de la institución

LEYENDA PARA LA CALIFICACIÓN

0-No se aplican procesos administrativos en lo absoluto

1-Los procesos son ad-hoc y desorganizados

2-Los procesos de siguen un patrón regular

3-Los procesos se documentan y se comunican

2.3.5 Informe ejecutivo de auditoría. El informe ejecutivo de la auditoría realizada a la Institución prestadora de Salud IPS INDIGENA GUÁITARA, se encuentra en la siguiente página:

IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES

San Juan de Pasto, 05 de Marzo de 2013.

Señor:
EDWIN BASTIDAS CALDERON
Representante Legal
Ciudad

REF:
AUDITORIA DE SISTEMAS APLICADA AL SISTEMA DE INFORMACIÓNDE LA IPS INDÍGENA GUÁITARA DEL MUNICIPIO DE IPIALES

Cordial Saludo.

Como es de su conocimiento la IPS INDÍGENA GUÁITARA del municipio de Ipiales, fue sometida a una auditoría de sistemas, para detectar y evaluar vulnerabilidades de licenciamiento, seguridad física y lógica a las que se encuentra expuesta la información.

El presente informe contiene información y documentación que fue suministrada por la entidad auditada, así como también la recolección de datos y hallazgos detectados por el equipo auditor. La evaluación se realizó en el periodo comprendido entre el 15 de junio del 2011 y el 15 julio 2012. Los resultados que se obtuvieron fueron los siguientes.

En cuanto a la Seguridad Física:

Cabe resaltar que la entidad cuenta con cámaras de vigilancia que ayudan en la observación del acceso a las instalaciones, en el caso de ocurrir algún evento inesperado se tendría claras evidencias de lo sucedido. Se pudo constatar que hay ingreso de personal de la entidad a las diferentes áreas o dependencias sin

autorización, de esta manera puede que haya alteración con los sistemas y la información.

En la entidad no se cuenta con un centro de cómputo que esté equipado con las condiciones técnicas y ambientales que garanticen el óptimo funcionamiento de los equipos.

Algunos equipos de cómputo cuentan con UPS (Sistema de Alimentación Interrumpida), que aseguran el funcionamiento normal y garantizan el apagado correcto de los mismos.

En caso de haber catástrofes naturales, en la entidad no se cuenta con medidas de seguridad para los equipos de cómputo, los extintores no están bien ubicados para que se pueda acceder a ellos y dar un determinado tratamiento.

El cableado que se utiliza en la entidad está bien administrado, pero en algunas dependencias existe saturación de enchufes, por lo tanto se corre el riesgo en caso de presentarse algún corto circuito o incendio, tanto para los equipos de cómputo como para el personal y las instalaciones físicas del lugar. Se puede destacar que las canaletas existentes cuentan con las normas actuales vigentes.

La no implementación de las medidas de seguridad para corregir las falencias detectadas en cuanto a la seguridad física, puede ocasionar problemas en el funcionamiento de los Sistemas de Información (SI) y Tecnologías de Información (TI) de la entidad, se ocasionaría una mala prestación del servicio.

Las recomendaciones para mejorar la seguridad física para ésta institución son:

Mejorar las medidas de seguridad en el ingreso de personas a la entidad y a cada una de las dependencias, además, ubicar a una persona que se encargue de la respectiva vigilancia de las cámaras.

Destinar un lugar específico para el centro de cómputo equipado para proteger los distintos recursos y suministros de tecnología.

En los equipos de cómputo se deben colocar UPS (Sistema de Alimentación Interrumpida), de esta manera se podrá salvaguardar la información ante apagones inesperados o algún inconveniente que se presente.

En la entidad debe existir sitios estratégicos para la ubicación de diferentes tipos de extintores, de esta manera se podrá acceder a ellos en caso de alguna emergencia para controlar la propagación.

Tener en cuenta las normas actuales vigentes que debe cumplir el cableado

eléctrico y de redes de esta manera implementarlas.

Cabe destacar que la infraestructura de la entidad está en excelentes condiciones las chapas, cerraduras y además cuentan con antepechos en todas las ventanas que dificultan el ingreso a personas no autorizadas y garantizan la seguridad de los equipos de computo, cuentan con alarmas contra incendios, se tiene extinguidores de diferente tipo, se cuenta con personal encargado de mantener limpia la institución y vigilancia para garantizar la seguridad de las personas.

En cuanto a la Seguridad Lógica:

En algunos equipos de cómputo no se cuenta con claves de administrador, de esta manera no hay control de acceso a la información y software. Se identificó que el Sistema de Información de la Ips Indígena Guáitara maneja claves muy básicas por ejemplo la inicial del nombre de la persona que lo va a manipular, de esta manera no se ofrece altos niveles de seguridad.

No se cuenta con un manual de procedimientos que garantice la seguridad lógica de los Sistemas de Información.

No se realizan copias de respaldo (backups) por parte de la entidad que garantice la estabilidad de la información, únicamente las copias son realizadas por iniciativa de los trabajadores los cuales guardan en lugares no tan adecuados.

Algunas personas ingresan a las distintas dependencias, manipulan los equipos de esta manera pueden alterar cualquier información y hacer mal uso de archivos y programas.

Se utiliza Firewalls para la protección, en algunos equipos falta actualizaciones de antivirus y actualizaciones de Antispyware.

La información que se envía por lo red interna llega a al destinatario correctamente para realizar los distintos procesos con la información, algunos equipos comparten recursos sin el uso de claves o accesos restringidos.

El servidor en donde se encuentra instalado el Sistema Integral de Información carece de un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.), además está en constante manipulación ya que se lo utiliza en facturación

Se encuentra desactualizados algunos sistemas operativos, no se cuenta con licenciamiento.

La falta de medidas de seguridad lógica de la información, puede verse reflejada en la alteración o en la pérdida total o parcial de la misma, violando las leyes

ocasionando sanciones e impidiendo el buen funcionamiento de la entidad.

Las recomendaciones que se plantean para mejorar la seguridad lógica son:

Deben mejorarse los procesos de seguridad existentes para el ingreso al Sistema de Información, para impedir que personal no autorizado pueda tener acceso a la información.

Implementar un manual de procedimientos global y de obligatorio cumplimiento encaminadas a garantizar la seguridad lógica de los sistemas de información. Se debe realizar el diccionario de datos del Sistema de Información para facilitar los procesos de administración de la configuración.

Realizar copias de seguridad por parte de la institución periódicamente y almacenarlas en lugares adecuados para éstos.

Se recomienda que el personal de la entidad cuente con una identificación para que puedan tener acceso a distintas áreas y dependencias.

Para garantizar la seguridad lógica del servidor este debe contar con software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.

Al momento de compartir los recursos algunos equipos deben contar con claves de usuario para impedir alteración o robo de información.

El servidor debe estar libre de manipulación de personal no calificado y se lo debe utilizar para sacar copias de seguridad y para poner en funcionamiento los servicios que presta.

Comprar licencias de los sistemas operativos como de los programas ofimáticos para evitar sanciones y mantener protegido los equipos.

Atentamente,

JULIO CESAR BURGOS
Auditor

NELSON ANDRES CORTES
Auditor

2.3.6 Informe general de auditoría.

Objetivos.

Aplicar técnicas de auditoría al Sistema de Información de la IPS INDIGENA GUÁITARA, que contribuyan a evidenciar vulnerabilidades en la seguridad física y lógica a los que se encuentra expuesta.

Objetivos específicos.

- Conocer el funcionamiento del Sistemas de Información en la actualidad en cuanto los usuarios del sistema, el hardware y software, la seguridad física y lógica, entre otros.

- Realizar un análisis de riesgos para identificar y conocer la causa de los mismos para proponer alternativas de solución.

- Aplicar el proceso de auditoría a los riesgos más relevantes que afecten el funcionamiento del sistema, utilizando las técnicas apropiadas para realizar las pruebas que permitan evidenciar.

- Elaborar un informe final de auditoría con las fallas encontradas, las soluciones propuestas y los planes de mejoramiento resultado de la auditoria.

Limitaciones.

La auditoria se realizó de forma normal y adecuada, llevando a cabo entrevistas a los funcionarios de las instituciones objeto de estudio.

2.3.6.1 Resultados obtenidos de la auditoria.

IPS INDIGENA GUAITARA

A continuación se detallan hallazgos y recomendaciones para cada uno de los procesos evaluados en la IPS INDIGENA GUAITARA.

DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

Proceso PO2: definición de la arquitectura de la información
Hallazgos

No existe un Manual Técnico y de Soporte para el Sistema de Información de la Ips Indígena Guáitara.

No existe un Diccionario de Datos del Sistema de Información de la Ips Indígena Guáitara.

No se cuenta con un modelo para la arquitectura de la información del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones

El Sistema de Información de la Ips Indígena Guáitara, debe implementar un manual técnico y de soporte que contenga:

- Las características del aplicativo, para que sirve, que pretende resolver y a quien va dirigido.
- Requerimientos de software y hardware para su funcionamiento.
- Instrucciones y pasos a seguir para realizar el proceso de instalación y puesta en funcionamiento del aplicativo.
- Descripción del funcionamiento de los diferentes módulos que conforman el sistema de Información.
- Descripción de reportes del Sistema de Información.
- Descripción de logs de Sistema de Información.
- Listado de archivos y especificaciones.

El Diccionario de Datos del Sistema de Información de la Ips Indígena Guáitara debe contener:

- Estructura física y lógica de la base de datos del Sistema de Información.
- Las definiciones de los objetos de la base de datos: tablas, vistas, índices, disparadores, procedimientos y funciones.
- El espacio asignado y utilizado por los objetos.
- Información sobre las restricciones de integridad.
- Información sobre las restricciones de integridad.

El Sistema de Información debe estar documentado (arquitectura de la información) donde se indique la información clara de cómo están organizados y relacionados entre sí cada uno de los elementos que lo conforman. El modelo de la arquitectura debe contener:

- Identificación de entradas
- Identificación de procesos.
- Identificación de sitios de almacenamiento.
- Identificación de reportes.
- Identificación de la interacción con otros sistemas.
- Definición de usuarios finales.
- Los planes de Tecnologías de la Información a corto y largo plazo.

Proceso PO4: definición de la organización y de las relaciones de TI.

Hallazgos

No existe un manual de funciones para los usuarios que interactúan con el Sistema de Información de la Ips Indígena Guáitara.

No existe un manual de funciones para el personal de TI relacionado con el Sistema de Información de la Ips Indígena Guáitara.

Existe personal clave e indispensable para el funcionamiento del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones

Se debe contar con un manual de funciones para los usuarios del Sistema de Información de la Ips Indígena Guáitara donde se tenga en cuenta:

- Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
- Definición de las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan.
- Definición de responsabilidades de cada uno de los usuarios.
- Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema de Información.
- Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

Se debe contar con un manual de funciones para los usuarios de TI que interactúen con el Sistema de Información de la Ips Indígena Guáitara, donde se indique:

- Definición de las funciones que los usuarios de TI deben desempeñar de acuerdo con el rol que tengan.

- Descripción de los diferentes perfiles que deben tener el personal que desempeñe los diferentes roles dentro del Sistema de Información.
- Diagramas de flujo detallados de los procesos que deben desempeñar los diferentes usuarios.

Debe existir dentro del personal de TI por lo menos 2 funcionarios que tengan los conocimientos necesarios para proveer soporte al Sistema de Información de la Ips Indígena Guáitara. El correcto funcionamiento, no puede depender de una sola persona.

Proceso PO9: evaluación de riesgos de TI

Hallazgos

Las políticas y procedimientos para el análisis y gestión del riesgo para las TI, dentro de la Ips Indígena Guáitara y específicamente para el Sistema de Información, carecen de elementos fundamentales para garantizar la minimización del riesgo.

Recomendaciones

Se debe tener en cuenta las políticas y procedimientos para el análisis y gestión del riesgo para las TI en la Ips Indígena Guáitara, las cuales deben abarcar los siguientes temas:

- La definición del contexto de la entidad.
- El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión del riego.
- La identificación de los activos de los Sistema de Información.
- La identificación y clasificación de los riesgos a los que se encuentran expuestos los activos de los Sistemas de Información.
- La determinación del impacto que causaría la ocurrencia de los riesgos.
- La identificación de controles que mitiguen los riesgos.
- La toma de decisiones frente a los riesgos.
- La elaboración del Plan de Seguridad Informática.

DOMINIO - ADQUISICION E IMPLEMENTACION (AI)

Proceso AI2: adquisición y mantenimiento de software aplicativo

Hallazgos

No existe en la Ips Indígena Guáitara un documento que brinde soporte y sirva de guía para la realización del proceso de adquisición de software y hardware.

Recomendaciones

Debe existir en la Ips Indígena Guáitara un documento que describa cual debe ser el proceso a seguir para la adquisición de software y hardware, el proceso correcto es:

- Realización de una solicitud formal que describa las características o requerimientos que debe cumplir el software o el hardware que se va a adquirir.
- Se deben solicitar por lo menos tres cotizaciones diferentes de los productos a adquirir.
- Análisis (mediante cuadros comparativos) de las cotizaciones y elección de la propuesta (costo/beneficio) para la entidad.

Proceso AI3: adquisición y mantenimiento de la infraestructura tecnológica

Hallazgos

No existe en la Ips Indígena Guáitara un documento que brinde soporte y sirva de guía para la realización del proceso de adquisición de software y hardware.

Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios del Sistema de Información no están documentadas.

Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios del Sistema de Información no están documentadas.

No existe un documento donde se explique a los funcionarios que interactúan con el Sistema de Información, cual es el proceso que deben seguir cuando se presenta un daño en su terminal de trabajo.

No existe en la Ips Indígena Guáitara, un manual de funciones para el personal de TI encargado de realizar el mantenimiento preventivo y correctivo de los equipos de cómputo

No existe dentro del personal de TI, un funcionario experto en el manejo (configuración, reparación, etc.) de redes de datos.

Recomendaciones

Debe existir en la Ips Indígena Guáitara un documento que describa cual debe ser el proceso a seguir para la adquisición de software y hardware, el proceso correcto es:

- Realización de una solicitud formal que describa las características o requerimientos que debe cumplir el software o el hardware que se va a adquirir.
- Se deben solicitar por lo menos tres cotizaciones diferentes de los productos a adquirir.
- Análisis (mediante cuadros comparativos) de las cotizaciones y elección de la propuesta (costo/beneficio) para la entidad.

Las políticas y/o procedimientos para llevar a cabo el mantenimiento preventivo de las terminales de trabajo de los usuarios que interactúan con el Sistema de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

- Instalación, configuración y actualización de los programas antivirus.
- Revisión periódica del estado de los programas antivirus.
- Escaneo periódico de la terminales de trabajo utilizando los programas antivirus.
- Desfragmentación periódica de los discos duros de las terminales de trabajo.
- Limpieza física de los equipos de trabajo utilizando sopladora, cremas y productos químicos especializados.

Las políticas y/o procedimientos para llevar a cabo el mantenimiento correctivo de las terminales de trabajo de los usuarios que interactúan con el Sistema de Información, deben estar documentadas, además deben ser conocidas por los usuarios encargados de realizar estos procesos y su aplicación debe ser de obligatorio cumplimiento, estos procedimientos deben contemplar:

- Pruebas de funcionamiento de cada uno de los dispositivos (CPU, RAM, board, tarjeta de red, tarjeta de video, etc.) que conforman la terminal de trabajo.
- Reparación del dispositivo defectuoso.
- Reemplazo del dispositivo defectuoso.
- Pruebas de funcionamiento de la terminal una vez realizados el mantenimiento

El proceso que deben seguir los funcionarios que interactúan con el Sistema de Información, cuando se presente algún tipo de daño en sus terminales de trabajo, debe estar documentado y ser de obligatorio cumplimiento. Este proceso debe contemplar:

- Reparación del dispositivo defectuoso.
- Realización por parte del funcionario responsable del equipo, de una solicitud por escrito para la revisión del equipo.
- Entrega (mediante acta o documento) por parte del funcionario del equipo dañado al personal de mantenimiento.
- Recepción (mediante acta o documento) por parte de personal de mantenimiento del equipo a revisar.
- Revisión y arreglo de acuerdo a las políticas y procedimientos estipulados para estos fines.
- Entrega (mediante acta o documento) por parte del personal de mantenimiento y recepción por parte del funcionario que reporto el daño, del equipo de cómputo ya reparado.

Debe existir en la entidad un manual de funciones para el personal de TI, que tiene a su cargo la realización de los procesos de mantenimiento preventivo y correctivo de los equipos de cómputo. Este manual debe contener

- Descripción del cargo.
- Descripción de las funciones y responsabilidades.
- Descripción del perfil del usuario que va a desempeñar el cargo.

Debe existir dentro de la entidad debe haber un funcionario de absoluta idoneidad profesional, encargado de la red de datos que soporta el normal funcionamiento del Sistema de Información de la Ips Indígena Guáitara.

Proceso AI6: Instalación y aceptación de los sistemas

Hallazgos

No existen políticas y/o procedimientos para la administración de los cambios en el Sistema de Información de la Ips Indígena Guáitara.

No existen bitácoras de registros de cambios realizados al Sistema de Información de la Ips Indígena Guáitara.

No existe dentro del personal de TI de la Ips Indígena Guáitara, un funcionario especializado y encargado de la realizar el mantenimiento y los cambios al Sistema de Información.

No existen políticas, procedimientos y/o estrategias dentro de la Ips Indígena Guáitara para garantizar la continuidad de los servicios de TI para el Sistema de Información.

Recomendaciones

Deben existir políticas y/o procedimientos claros para la administración de los cambios dentro del Sistema de Información. El proceso que se debe realizar debe contemplar:

- Realización de una solicitud formal de cambios, por parte del interesado, esta debe contener la justificación del cambio.
- Priorización de las solicitudes de cambios.
- Acceso por parte del programador al código fuente para la realización del cambio
- Solicitudes para realización de pruebas.
- Finalización del proceso de pruebas de aceptación.
- Determinación y aceptación del impacto causado por el cambio.
- Actualización de la documentación para registrar el cambio

Deben existir bitácoras donde se registren y se lleve un control de los cambios realizados a través del tiempo al Sistema de Información de la Ips Indígena Guáitara. Estas bitácoras deben contener:

- Fecha de solicitud del cambio
- Persona que solicita el cambio.
- Soporte (motivo) para solicitar cambio.
- Cambios realizados - personal de Tecnologías de la Información.
- Aprobación de cambios realizados – usuario solicitante.
- Fecha de actualización de la documentación.

Debe existir dentro del personal de TI, un funcionario de absoluta idoneidad profesional encargado de llevar a cabo el mantenimiento del Sistema de Información y la realización de los ajustes al código fuente del mismo. Es

recomendable que este funcionario sea de carrera administrativa, para que el conocimiento adquirido continúe dentro de la entidad.

Deben existir en la Ips Indígena Guáitara políticas, estrategias o procedimientos para garantizar la continuidad de los servicios de Tecnologías de la Información para el Sistema de Información. Estas políticas deben:

- Fecha de actualización de la documentación.
- Contemplar la existencia de un marco de referencia.
- Estar alineadas con la estrategia de continuidad del negocio.
- Contemplar la identificación de los procesos críticos y el análisis del impacto estos procesos.
- Garantizar la existencia de un Plan de Continuidad, que contenga:
- Guía de cómo utilizar el plan.
- Procedimientos de emergencia para asegurar la seguridad del personal, incluyendo procedimientos de evacuación.
- Condiciones para declarar un desastre.
- Identificación de los procesos de negocio críticos y recursos de TI que deben ser recuperados
- Identificación crítica de personas afectadas y de los responsables por cada función del Plan.
- Explicación paso por paso de los procedimientos de respuesta que incluyen los procedimientos de operación en caso de emergencia.
- Identificar estrategias de continuidad.
- Garantizar que el almacenamiento de la información y los recursos críticos para garantizar la continuidad del sistema, fuera de las instalaciones de la Ips Indígena Guáitara.
- Garantizar el entrenamiento a los usuarios y la distribución del Plan de Continuidad.
- Ser de conocimiento de todos los funcionarios comprometidos en el proceso.

DOMINIO – ENTREGA DE SERVICIOS Y SOPORTES (DS)

Proceso DS5: garantizar la seguridad de sistemas

Hallazgos

No existen políticas globales dentro de la Ips Indígena Guáitara, para garantizar la seguridad lógica de los Sistemas de Información que se manejan en la entidad

No existen políticas dentro de la Ips Indígena Guáitara para la creación y administración de las contraseñas que diariamente emplean los usuarios para acceder e interactuar con el Sistema de Información.

Los procesos que actualmente utiliza el Sistema de Información para realizar la autenticidad de los usuarios, son básicos y no ofrecen altos niveles de seguridad.

El servidor que soporta el funcionamiento del Sistema de Información, carece de:

Un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.).

Un sistema de firewall físico

Recomendaciones

Deben existir en la Ips Indígena Guáitara políticas, estrategias o procedimientos para garantizar la continuidad de los servicios de TI para el Sistema de Información. Estas políticas deben:

- Autenticación y acceso
- Administración de perfiles de usuario y clasificación de la seguridad de datos
- Reportes y revisión de las violaciones e incidentes de seguridad.
- Aplicación de Estándares de administración de llaves criptográficas.
- Detección, resolución y comunicación sobre los virus.
- Clasificación y propiedad de los datos.

.

Deben existir políticas dentro de la Ips Indígena Guáitara que reglamenten la creación y administración de contraseñas para acceder al Sistema de Información. Estas políticas deben contemplar:

- Cambio inicial de las contraseñas la primera vez de uso.
- Establecer una longitud adecuada mínima de las contraseñas.
- Combinaciones de alfanuméricas obligatorias en las contraseñas.
- Verificación de la contraseña en la lista de valores no permitidos
- Cambio periódico de las contraseñas.
- Protección adecuada de las contraseñas.

Los procesos para autenticidad de los usuarios dentro del Sistema de Información deben cumplir con:

- Uso de contraseñas que se ajusten a las políticas establecidas para la creación y administración de las mismas.
- Usuario suspendido después de 'n' intentos (valor recomendado entre 3 y 5) de entrada fallidos.
- El tiempo para realizar la autenticación de usuario se limita.
- El número de secciones concurrentes correspondientes a un mismo usuario deben estar limitadas.

Para garantizar la seguridad lógica de la información almacenada en el servidor, éste debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.

- La elección del firewall físico (de varios existentes en el mercado) debe ajustarse a las necesidades y al presupuesto de la Ips Indígena Guáitara.

Proceso DS9: administración de la configuración

Hallazgos

Existe un inventario detallado y completo sobre la configuración del servidor en donde se encuentra instalado el Sistema de Información y su respectiva base de datos.

No existen políticas dentro la Ips Indígena Guáitara que regulen o den pautas sobre qué tipo de software es permitido que se encuentre instalado y funcionado en las terminales de trabajo de los usuarios del Sistema de Información.

No existen controles para la administración de la configuración (tanto de software como de hardware) de los equipos de cómputo dentro de la Ips Indígena Guáitara.

Recomendaciones

Debe existir en la Ips Indígena Guáitara, un inventario detallado de la configuración del servidor en donde se encuentra instalado el Sistema de información. Este inventario debe estar conformado por:

- Información referente a la configuración del Sistema Operativo.
- Información referente a la configuración del software de aplicación (bases de datos, servidores Web, servidores Proxy, etc.).
- Información referente a licencias de los programas instalados.

- Información referente al hardware instalado.

Deben existir políticas claras en la Ips Indígena Guáitara, que regulen e identifiquen que tipo de software es permitido que se encuentre funcionando en las terminales de trabajo de los usuarios del Sistema de Información.

- Estas políticas deben ser de conocimiento de todos los funcionarios de la dependencia, de obligatorio cumplimiento

Deben existir procedimientos de control para la administración de la configuración del software y del hardware que se encuentra instalado en las terminales de trabajo de los usuarios que interactúan con el Sistema de Información de la Ips Indígena Guáitara. Estos controles consisten en:

- Registro en bitácoras de la configuración de los equipos y de los cambios que se realicen tanto en el software como en el hardware.

- Revisiones periódicas para comprobar que software y que hardware se encuentra instalado en las diferentes terminales de trabajo, y comparar con el tipo de elementos autorizados.

Proceso DS11: administración de datos

Hallazgos

No existen en la Ips Indígena Guáitara documentos que soporten o den pautas sobre cómo debe llevarse a cabo el proceso de realización de las copias de seguridad para el Sistema de Información.

No existe un lugar fuera de las instalaciones de la Ips Indígena Guáitara en donde se almacenen bajo estrictas medidas de seguridad, las copias de seguridad del Sistema de Información.

Recomendaciones

Deben existir dentro de la Ips Indígena Guáitara documentos que soporten las políticas y los procedimientos para la realización de las copias de seguridad del Sistema de Información.

- El administrador del Sistema de Información, deberá conocer este documento y aplicar los procedimientos que ahí se describan.

Debe existir fuera de las instalaciones de la Ips Indígena Guáitara un lugar en el cual se almacenen las copias de seguridad del Sistema de Información.

Este lugar debe contar con adecuadas medidas de seguridad, que garanticen la integridad física de los respaldos, entre estas medidas tenemos:

- Accesos únicamente de personal autorizado y debidamente identificado.
- Acceso en horarios autorizados.
- El sitio donde se guarden las copias de seguridad debe contar con personal de vigilancia.

Proceso DS12: administración de instalaciones

Hallazgos

Los procedimientos de seguridad que actualmente se lleva a cabo para controlar el acceso y la salida de las instalaciones de la entidad, brindan un buen nivel de tipo de seguridad para los activos de TI del Sistema de Información.

No existe en las instalaciones de la Ips Indígena Guáitara ni fuera de ellas, un lugar reservado y con las características ambientales y de seguridad para albergar los equipos que soportan el funcionamiento del Sistema de Información.

No existen medidas de seguridad dentro de las instalaciones de la Ips Indígena Guáitara , para restringir el acceso al lugar donde se encuentran ubicados los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves que soportan y garantizan el buen funcionamiento del Sistema de Información.

Falta de extintores contra incendios dentro de las instalaciones de la Ips Indígena Guáitara.

Existe señalización en caso de presentarse un evento catastrófico, mas no se cuenta con un plan de evacuación como tal dentro de las instalaciones de la Ips Indígena Guáitara

Los sistemas de detección de movimiento no existen actualmente en la Ips Indígena Guáitara.

Los sistemas de cámaras, alarmas y detección de humo se encuentran funcionando correctamente.

No existen en la Ips Indígena Guáitara medidas de seguridad que garanticen la integridad física de las copias de seguridad del Sistema de Información.

El sitio donde se encuentran las UPS (Sistema de Alimentación Ininterrumpida), que aseguran el funcionamiento normal de los equipos de computo claves del Sistema de Información por un determinado tiempo, en caso de presentarse cortes del suministro eléctrico en las instalaciones de la Ips Indígena Guáitara, no es adecuado, y no brinda ningún tipo seguridad para estos elementos.

No existen en las instalaciones de la Ips Indígena Guáitara, medidas de seguridad o aislamientos que aseguren la integridad física del cableado (UTP, eléctrico, etc.) que no se encuentra integrado a la estructura del edificio

Recomendaciones

Deben existir procedimientos de seguridad para controlar el acceso y la salida de las instalaciones de la Ips Indígena Guáitara. Estos procedimientos deberán asegurar que:

- Todas las personas que entran a las instalaciones de la Ips Indígena Guáitara, se identifique, sean autenticados y autorizados para entrar.
- La realización de requisas a las personas que ingresan y que salen de las instalaciones.
- El registro de los equipos de computo (portátiles, PC, etc.) que ingresan a las instalaciones.
- Para los visitantes que ingresan por el parqueadero de vehículos y motocicletas, se realiza la identificación, autenticación y autorización para el ingreso.
- La realización de requisas a los vehículos que ingresan y salen de las instalaciones.

Los equipos de cómputo (servidores, patchpanel, routers, switchs, etc.) que soportan y garantizan el correcto funcionamiento del Sistema de Información deben permanecer en un lugar adecuado (centro de cómputo) y que satisfaga los requerimientos de:

- Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación. El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Tratamiento acústico. Los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.

- Sistemas de ventilación. Las instalaciones del centro de cómputo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.
- Seguridad física. Las instalaciones del centro de computo cuentan con sistema contra incendios; los materiales del centro de computo son incombustibles (pintura de las paredes, suelo, techos, mesas, estanterías, etc.). Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a las instalaciones.
- Suministro eléctrico. El suministro eléctrico a un Centro de Cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

El lugar donde se encuentren los equipos de computo (servidores, patchpanel, routers, switchs, etc.) claves para el funcionamiento del Sistema de Información debe tener restringido el acceso solamente a personal autorizado.

Dentro de las instalaciones de la Ips Indígena Guáitara se deben ubicar extintores contra incendios en lugares estratégicos y de fácil acceso.

Algunos requisitos del plan de evacuación se observan en las instalaciones de la Ips Indígena Guáitara tales como:

- En las Instalaciones se cuenta con una señal de alarma (timbre, campana, silbato) que será muy relevante y de fácil reconocimiento por todos los actores institucionales, los cuales ante esta situación se encaminarán hacia la puerta de salida.
- En las Instalaciones hay señalización las paredes con una flecha roja direccional acompañada de la palabra SALIDA a una altura de 2 m, en corredores, escaleras, rampas, etc.
- Garantizar una salida rápida y segura hacia el exterior.
- Dar a cargo la toma de decisión de evacuación y orden a una persona responsable
- El trayecto de escape deberá estar libre de obstrucciones o entorpecimiento de circulación.
- Se establecerán roles y responsabilidades para el personal de la Ips Indígena Guáitara, por ejemplo personal responsable de la utilización de los medios contra incendios -extintores, mangueras-, encargado del botiquín de primeros auxilios, de interrumpir los circuitos eléctricos, de la apertura de las puertas de salida.

- La concentración y desconcentración se realizará a los lugares prefijados (lugares que ofrecen medidas de seguridad aceptables) y conocidos con anterioridad.
- Se deben realizar simulacros de evacuación.
- Los extintores y otros elementos de protección se controlarán periódicamente, y se capacitará al personal acerca de su uso.

Las instalaciones de la Ips Indígena Guáitara debe contar con sistemas de detección de movimiento que estén configurados y en funcionamiento, para brindar seguridad a los activos de TI del Sistema de Información.

Deben existir e implementarse medidas de seguridad en la Ips Indígena Guáitara, que garanticen la integridad física de las copias de seguridad del Sistema de Información. Algunas de estas medidas son:

- Los medios de almacenamiento físico (CD, DVD, Cintas Magnéticas, etc.) en donde se encuentran las copias de seguridad del Sistema de Información, deben guardarse bajo llave.
- Solo las personas autorizadas pueden tener acceso a las copias de seguridad.
- Debe existir un sitio fuera de las instalaciones de la Ips Indígena Guáitara, en donde se almacenen las copias de seguridad.
- Los sitios dentro y fuera de las instalaciones de la Ips Indígena Guáitara, que sirvan para almacenar las copias de seguridad, deben contar con factores ambientales (humedad, iluminación, ventilación, etc.) óptimos, que garanticen la integridad de los medios de almacenamiento.

Los lugares donde se ubiquen los Sistemas de Alimentación Ininterrumpida (UPS) que dan autonomía de funcionamiento a los equipos de computo claves del Sistema de Información, durante un tiempo determinado, en caso de presentarse cortes en el suministro eléctrico, deben cumplir con las condiciones de:

- Espacio y movilidad. Características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación. El sistema de iluminación debe ser apropiado para evitar falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Tratamiento acústico. Los equipos ruidosos como equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
- Sistemas de ventilación. Las instalaciones deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento

- Seguridad física. Las instalaciones donde se ubique las UPS deben contar con un sistema contra incendios; los materiales deben ser incombustibles. Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a la instalación.
- Suministro eléctrico. El suministro eléctrico y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias

El cableado (UTP, eléctrico, etc.) que no se encuentre incorporado a la estructura del edificio de la Ips Indígena Guáitara, bebe contar con medidas de aislamiento que garanticen su seguridad y su integridad. Se recomienda el uso de canaletas para proteger estos activos de TI.

Proceso M2: Evaluar lo adecuado al control interno

Hallazgos

No existen políticas y/o procedimientos referentes al monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de TI del Sistema de Información de la Ips Indígena Guáitara.

Recomendaciones

Deben existir políticas y/o procedimientos para realizar el monitoreo de las actividades encaminadas a brindar seguridad física y lógica para los activos de TI del Sistema de Información. Las características de estas políticas son:

- Debe existir una descripción detallada de los procedimientos de monitoreo que se deben aplicar dependiendo de la actividad que se desea evaluar.
- Debe existir un cronograma en donde se muestre claramente la periodicidad con que se van a efectuar los procesos de monitoreo de las diferentes actividades.
- Debe existir definición de los funcionarios responsables de realizar las actividades de monitoreo.

3. MANUAL DE USUARIO

Para el hallazgo del Dominio: **Dar soporte y servicio (DS),** en el proceso administración de ambiente físico (DS12) tenemos el siguiente ejemplo:

	HALLAZGOS			**REF** **PLAN DS12_3_9**
ENTIDAD AUDITADA	Institución Prestadora de Servicios de Salud Indígena "GUAITARA"			**PAGINA** 2 de 2
AREA AUDITADA	Seguridad Física y Lógica	**SISTEMA**	Sistema de Información Ips Indígena Guáitara	
RESPONSABLES	Julio Cesar Burgos y Nelson Andrés Cortés			
MATERIAL DE SOPORTE	COBIT			
DOMINIO	Entrega de Servicios y Soporte (DS)	**PROCESO**	Administración de las Instalaciones (DS12)	

Consecuencia:
La no existencia de medidas de seguridad para proteger y garantizar la integridad física del cableado (UTP, eléctrico, etc.) dentro de las instalaciones de la Ips Indígena Guáitara, puede generar fallos en el funcionamiento del Sistema de Información, ocasionados por daños en el cableado, estos daños pueden ser no intencionados o como resultado de sabotaje.

Nivel de Riesgo:
Probabilidad: Alta
Impacto: Alto
Nivel de Madurez: 1

Evidencias:

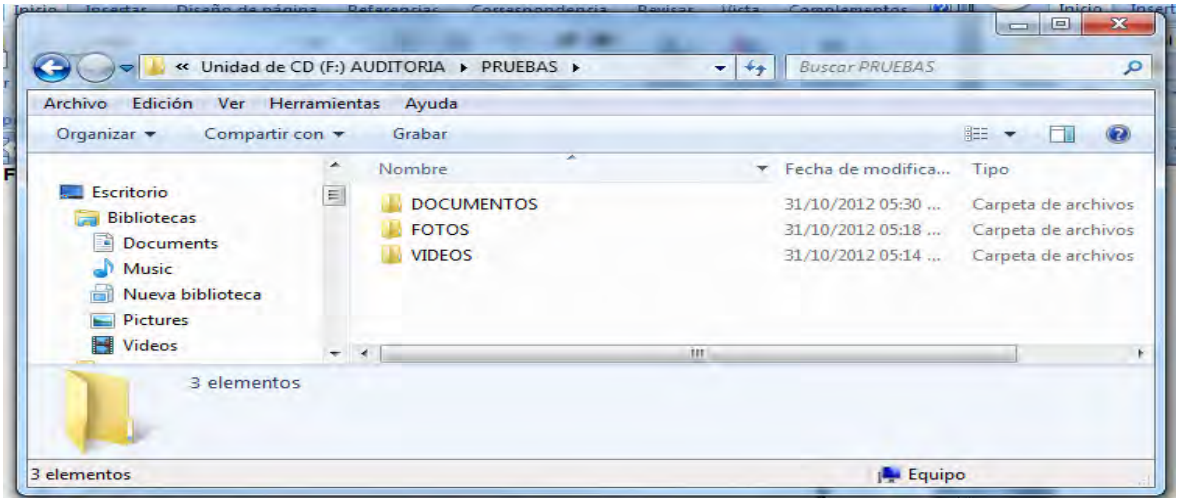
ENT_DS12_3_9
IMG01_DS12_3_9
IMG02_DS12_3_9
IMG03_DS12_3_9
IMG04_DS12_3_9
IMG05_DS12_3_9
IMG06_DS12_3_9

En el formato definido para sustentar los Hallazgos se encuentra el campo **Evidencias,** que son las pruebas que pueden ser entrevistas, cuestionarios o fotografías que sustentan la veracidad de este hallazgo.
Es importante mencionar que los nombres de las evidencias tanto en:

- Fotografía ejm: IMG01_DS12_02, los dos penúltimos números significan el subitem del proceso seguido del domino que en este caso es DS12 y tenemos IMG01 que significa imagen numero uno.

Cabe aclarar que en el DVD se encuentran dos carpetas ANEXOS y PRUEBAS, al entrar a la carpeta PRUEBAS se encuentra los siguiente (Figura 34).

Figura 22. Listado de Carpetas (PRUEBAS)



Fuente: Esta investigación

Donde se encuentran todas las pruebas que verifica toda la información recolectada en el proceso de la auditoria.

Para poder acceder a estas pruebas se debe seguir los siguientes pasos definidos así:

1. En el hallazgo **PLAN DS12** tomado como ejemplo tenemos tres evidencias donde son fotografías IMG01_DS12_02, así entonces para llegar a los documentos de prueba se debe:

- Ir a la carpeta PRUEBAS
- Dentro de la carpeta FOTOS **(PRUEBAS\FOTOS\IMG01)**, donde están numeradas todas las fotografías aplicadas en la auditoria, cabe aclarar que estas entrevistas residen también en el archivo corriente en físico firmadas por

las personas entrevistadas como prueba veraz de todos los hallazgos encontrados.

2. Las siguientes 2 evidencias de este hallazgos se encuentran en la misma ruta **(PRUEBAS\FOTOS\IMG02)** y **(PRUEBAS\FOTOS\IMG03)**, en esta carpeta **(FOTOS)** hallaran todas las fotografías que se realizaron para tener pruebas de ello, donde nos vamos a encontrar con diferentes tipos de pruebas que pueden ser videos, documentos y/o fotografías o entrevistas en físico como lo muestra la figura 34, para llegar a esta información se debe:

- Ir a la carpeta ANEXOS

- Dentro de la carpeta Anexos está el formato de la encuesta, el formato de preguntas y un formato en Excel donde se encuentran todos los cuestionarios cuantitativos aplicados en la auditoria.

4. CONCLUSIONES

- La auditoría de Sistemas de Información, hoy en día es de vital importancia para las empresas modernas con visión de futuro, sobre todo inmersas en el mundo globalizado, porque si no se prevee los mecanismos de control, seguridad y respaldo de la información dentro de una institución se verá sumida a riesgos lógicos, físicos y humanos, que conlleven a fraudes no solamente económicos sino de información, es decir, pérdidas para la empresa.

- La auditoría de sistemas se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información (SI), desde sus entradas, procedimientos, controles y salidas.

- Los Sistemas de Información (SI) constituyen uno de los aspectos estratégicos claves para el desarrollo de la empresa. Para ello es necesario que toda la organización esté concienciada de su utilidad, tanto por parte de la alta dirección, la que debe tenerlos en cuenta al realizar la planificación estratégica, como por parte de los distintos usuarios de la empresa.

- Las Tecnologías de Información (TI) hacen que se cambie la manera de realizar las operaciones respecto a la que tenía la empresa, ya que llevan consigo una propia forma de actuar, por ello los usuarios y la organización se deben adaptar a ellas.

- En la IPS INDIGENA GUAITARA existen muchas deficiencias en relación a la seguridad física y lógica de los recursos de TI, ya que los procesos que se encuentran establecidos en la entidad no son los suficientes para determinar que se encuentren en un óptimo desempeño ocasionando el no cumplimiento de los objetivos.

- En la IPS INDIGENA GUAITARA la información se encuentra expuesta a muchos riesgos a lo largo de todo su manejo, desde que es generada, hasta que es almacenada. Es por eso que la entidad debe establecer políticas de seguridad de tipo lógico y físico. Ambas de la misma importancia para conservar a la información de forma segura.

- El modelo COBIT es utilizado como marco de referencia para evaluar características como: efectividad, eficiencia, confidencialidad, integridad,

disponibilidad, cumplimiento y confiabilidad, de esta manera poder establecer hallazgos y recomendaciones para cada uno de los procesos en los cuatro dominios: Planeación y Organización (PO), Adquirir e Implantar (AI), Entregar y Dar Soporte (DS) y Monitorear y Evaluar (ME). Logrando así, determinar las posibles vulnerabilidades y problemas de seguridad que tienen las entidades en cuanto al procesamiento de la información.

5. RECOMENDACIONES

- Antes de realizar una auditoría de sistemas se aconseja analizar detalladamente el entorno organizacional de la entidad, identificar y definir claramente metas y objetivos, de esta manera se tendría una planificación inicial de la auditoría.

- Después de haber hecho la planificación inicial, se deben aplicar distintos métodos y herramientas de recolección de información como: encuestas, entrevistas, cuestionarios, etc., para luego realizar cálculos en la matriz de riesgos garantizando así que la información obtenida sea auténtica y precisa.

- Se deben realizar visitas periódicas a la entidad, ejecutar revisiones y evaluaciones continuas, según los resultados establecer planes de mejoramiento que conlleven a la certificación de calidad de los procesos.

- Al realizar una buena auditoria de sistemas se debe garantizar el buen funcionamiento de los Sistemas y las TI en las diferentes entidades sean públicas o privadas de esta manera colaborar con la toma de decisiones.

- Se deben promover la realización periódica de auditorías de sistemas en las entidades con el fin de que sirvan de instrumentos para el fortalecimiento tecnológico y sean herramientas que ayuden a lograr el cumplimiento de los objetivos.

BIBLIOGRAFÍA

ARENS, ALVIN A. Auditoria un Enfoque Integral. 6 Edición. México: Prentice Hall, 1996.

CAICEDO, Liliana. ORDOÑEZ, Claudia. Técnicas de Auditoria de Sistemas Aplicadas al Proceso de Contratación y Páginas Web en Entidades Oficiales del Departamento de Nariño. Universidad de Nariño. 2010.

ECHENIQUE GARCÍA, José Antonio. Auditoría en Informática. 2 Edición. México: Mc Graw Hill, 2001.

ESTRADA, Oscar. Auditoría de Sistemas Aplicada al Sistema Integral de Información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto. Universidad de Nariño. 2007

GUSTIN Enith, SOLARTE Francisco Javier, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, Copyright © 2011.

PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

BIBLIIOWEB

http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/auditcontxactual.htm (Consultado, Agosto 2011)

http://www.gerencie.com/auditoria-interna.html (Consultado, Agosto 2011)

http://www.gerencie.com/auditoria-externa.html (Consultado, Agosto 2011)

http://www.monografias.com/trabajos16/auditoria-fiscal/auditoria-fiscal.shtml (Consultado, Agosto 2011)

http://www.mitecnologico.com/Main/DiferenciaEntreAuditoriaAdministrativaYFinanciera (Consultado, Septiembre 2011)

http://www.mitecnologico.com/Main/DiferenciaEntreAuditoriaAdministrativaYFinanciera (Consultado, Septiembre 2011)

http://www.gestiopolis.com/recursos6/Docs/Fin/auditoria-concepto-funciones.htm (Consultado, Octubre 2011)

http://www.auditsoftware.net/documents/TopCAATs.pdf (Consultado, Octubre 2011)

http://www.dspace.espol.edu.ec/bitstream/123456789/4158/ 1/6686.pdf (Consultado, Noviembre 2011)

http://www.megapuntes.com.ar/auditoria/ALUMNOS2008/ISACA.doc (Consultado, Diciembre 2011)

http://www.isacabogota.net/metodologias/cobit.aspx (Consultado, Enero 2012)

http://www.itsor.net/pdf/ITSOR_COBIT_Brochure_VE.pdf. (Consultado, Enero 2012)

http://www.datasec- oft.com/archivos/sp/folletos/acl/ACL_Desktop_Data_Sheet-es.pdf (Consultado, Enero 2012)

http://es.wikipedia.org/wiki/COBIT (Consultado, Febrero 2012

ANEXOS

DEFINICIÓN_PLANEACION Y ORGANIZACIÓN

ANEXO 1. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - Proceso PO2: definición de la arquitectura de la información

ANEXO 2. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - PO3. Determinar la Dirección Tecnológica.

ANEXO 3. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - PO4. Definición de la organización y las relaciones de TI

ANEXO 4. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - PO9. Evaluación de riesgos.

DEFINICIÓN_ADQUISICION E IMPLEMENTACION

ANEXO 5. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - AI3. Adquisición y Mantenimiento de la Infraestructura Tecnológica.

ANEXO 6. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - AI4: facilitar la operación y el uso
.
ANEXO 7. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - AI5. Adquirir recursos.

DEFINICIÓN_ENTREGA DE SERVICIOS Y SOPORTE

ANEXO 8. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS5: garantizar la seguridad de sistemas

ANEXO 9. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS9: administración de la configuración

ANEXO 10. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS12. Administración de Instalaciones

ANEXO 11. Definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría - DS13: administrar las operaciones.