AUDITORIA A LA SEGURIDAD DEL SISTEMA DE INFORMACION SIVIGILA DE LA ALCALDÍA DE SAN ANDRÉS DE TUMACO BASADA EN EL ESTÁNDAR ISO 27001.

YURANI ALEJANDRA LANDAZURI GUEVARA

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2015

AUDITORIA A LA SEGURIDAD DEL SISTEMA DE INFORMACION SIVIGILA DE LA ALCALDÍA DE SAN ANDRÉS DE TUMACO BASADA EN EL ESTÁNDAR ISO 27001.

YURANI ALEJANDRA LANDAZURI GUEVARA

Trabajo de grado presentado como requisito parcial para optar el título de Ingeniera de Sistema

Esp. JOSE JAVIER VILLALBA ROMERO
Director

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2015

NOTA DE RESPONSABILIDAD

“Las ideas y conclusiones aportadas en la tesis de grado, son responsabilidad exclusiva de la autora”.

Artículo 1° del acuerdo N° 324 de Octubre 11 de 1966, emanado por el Honorable Concejo Directivo de la Universidad de Nariño.

Artículo 2° del acuerdo N° 005 de 2010, emanado por el Honorable Concejo Directivo de la Universidad de Nariño.

Nota de aceptación

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

_____
Firma del asesor del proyecto

San Juan de Pasto, Septiembre de 2015

DEDICATORIA

Dedico este trabajo de forma muy especial a Jesucristo Dios todo Poderoso que en todo momento me dio sabiduría de lo alto y salud para desarrollar este proyecto estando en cada instante llenándome de fuerza y de dominio propio para culminar lo iniciado.

A mis padres, Nuris Alicia Guevara y William Teófilo Landázuri, por darme a manos llenas su amor, paciencia y apoyo en cada camino que he emprendido a lo largo de mi vida personal y estudiantil.

A mi hermano Sergio Cifuentes quien desde hace más de dos años vivo extrañando su presencia, pero estoy segura que de donde este él está feliz por la culminación de un camino que nos pertenece a los dos, debo confesar que el después de Dios fueron mis más grandes pensamientos reconfortadores en momentos de desesperación, donde te encuentres hermano esto va por ti y para ti.

A mis demás hermanos Jimena, William y Yulieth Landázuri porque cada vez que los miro siento más ganas de ser mejor por ellos para que puedan tener un espejo donde reflejarse. A todos mis familiares a quienes amo profundamente y que siempre confiaron en mí, a mi novio Diego Ocoro por su apoyo y ayuda en momentos que en su tiempo fueron críticos.

AGRADECIMIENTOS

Agradezco a Dios porque sin él estar escribiendo estas líneas no sería posible, ya que en todo tiempo sentí su ayuda y amor que permitió llegar hasta aquí.

A mis padres, a quienes amo en gran manera porque siempre he tenido su apoyo económico, moral y sobre amoroso haciéndome sentir lo importante que es la familia en tu desarrollo como persona y profesional.

Al ingeniero José Javier Villalba Romero, quien se llenó de paciencia y de ganas de ayudar para colaborar con este proceso y hacerlo posible, a quien además de mi asesor considero mi amigo el cual me supo guiar y dirigir para desarrollar un buen trabajo.

Al ingeniero Manuel Bolaños quien ayudo a facilitar todos los procesos a nivel administrativo para poder llegar a esta etapa del trabajo presente además de hacer el papel de revisor de la propuesta inicial.

Al ingeniero Francisco Solarte, quien actuó de forma dedicada y rápida para la revisión y aprobación de la propuesta inicial.

A todos los docentes de la gran Universidad de Nariño, que me acompañaron en mi proceso de formación a lo largo de la carrera dándome sus conocimientos y ayudando a despejar todas las dudas que tuve durante el proceso de estudio.

A mis compañeros, quienes con su compañía hicieron más amenas desde sus inicios las horas de clase, de forma especial a Nolys Prado Y Tatiana Castro por haberse convertido en grandes amigas que espero conservar el resto de mi vida.

A la honorable Universidad de Nariño, por dar a la sociedad profesionales íntegros y la mejor prueba de esto son los docentes egresados de la misma que en su gran mayoría compartieron secciones de clases conmigo.

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Para asegurar la fácil comprensión en el transcurso de este proyecto es necesario conceptualizar varios términos claves que son utilizados en el desarrollo del presente trabajo, estos se describen enseguida.

Activo: relacionado con la seguridad de la información es cualquier elemento informático o elemento relacionado con el tratamiento de la misma es decir sistemas, soportes, edificios, personas, que tengan un valor para la organización.
Los activos es todo aquello que represente ganancias para la entidad y que a su vez si son mal administrado representan pérdidas y a su vez dependiendo del nivel de gravedad será el grado de complejidad los controles para aplicar para la búsqueda de una solución.

Control: Es también utilizado como sinónimo de salvaguarda o contramedida. Permite a las políticas, procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos por debajo del nivel asumido.
En toda organización se necesita tener controles para evitar que riesgos y amenazas no permitan que se cumpla el objetivo del negocio, y colocando de esta forma a la entidad en riesgo, los controles permiten si son bien aplicados un equilibrio en toda la organización.

Confidencialidad: Es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

No divulgar información a no autorizados es lo ideal en las entidades, la confidencialidad es el atributo que permite que se guarde la privacidad de los datos que se tengan que forman información de gran importancia para una organización.

Disponibilidad: Es la propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. En otros términos es el atributo en una empresa que permite que todo lo que se necesite este siempre ahí para asegurar rapidez en la ejecución de los procesos dentro de la organización.

Evidencia: Es aquella prueba determinante e irrefutable a instancia de cualquier proceso. Por lo general se emplea para designar aquello que permite demostrar la realidad de un hecho.
En la informática este término es de gran importancia para desarrollar procesos en cualquier identidad ya sea de seguimiento, a un proceso o algún empleado de una organización.

Integridad: se define como la pureza original y sin contacto o contaminación con un mal o un daño, ya sea físico o moral. Es el estado de lo que está completo o tiene todas sus partes, es la totalidad, la plenitud. En informática la información integra tiene todo completo y no han sido manipulados por personal no autorizado.
Para que una empresa refleje confianza y se sustente sobre bases sólidas debe existir esta propiedad en cada proceso y en los resultados de los mismo, porque de esta forma toda la información que se manipule será contada como un activo y no como una perdida, ya que en el momento que un dato es manipulado por personal que no es correcto se pierde la esencia y lo intacto de la información.

Monitoreo: Se define como el desarrollo del control constante que pretende detectar defectos y anomalías, para tomar medidas necesarias para subsanar los daños que se hayan causado o que estén por suceder.
Cuando las organizaciones están interesadas en descubrir falencias y fortalecer todos los aspectos positivos el monitoreo es una actividad propia de ellas porque de esta forma se están observando y procurando avanzar.

Riesgo: Es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en activo de información. Suele relacionarse la probabilidad de un evento y sus consecuencias combinados.
Que no existan riesgos en una entidad es imposible pero evitarlos si es posible o al menos estar preparados por si estos se llegan a presentar, ya que una vez presentes en la realidad de una organización puede poner en problemas la ejecución de los procesos.

Programas utilitarios: Son los programas que resuelven problemas relacionados con la administración del sistema de un equipo de cómputo, estos realizan tareas de mantenimiento, revisión de software, recuperación de datos y la eliminación de software malicioso.
Estos están diseñados para realizar tareas específicas en el sistema de una computadora, como por ejemplo, un editor, un depurador de código.

Escritorio despejado: Es el tipo de política que permite en una empresa que todos los escritorios estén limpios y todas las áreas de la compañía estén libres de papeles, que la oficina se vea atractiva y refleje a un profesional eficiente.
Hace que los empleados se sientan en control en un entorno bien organizado y que la parte externa a la entidad se lleve una buena impresión de las misma.

Pantalla despejada: Es aquella política que permite conservar la pantalla libre de acceso directos a información clasificada como confidencial, verifica que en los equipos asignados o bajo la responsabilidad de algún empleado de una entidad se bloquee la sesión de trabajo, cuando estos no estén.

Este tipo de política evita riesgos de pérdida o deterioro de la información que reposa en equipos de una oficina determinada.

Controles criptográficos: estos se encargan de estudiar algoritmos, protocolos y todo tipo de sistemas que se utilizan para dotar de seguridad a la información de una entidad.
Estos tienen como objetivo conservar propiedades que debe tener la información como la confidencialidad e integridad en busca que esta esté lo más disponible para los funcionarios de una entidad en particular.

Sistema de gestión de llaves: son aquellos que periten controla quien puede acceder a un sistema, este también si se lo configura es capaz de monitorizar y asegurar el acceso de cada llave individual estando estas llaves disponibles solo para `personal autorizado.

RESUMEN

El presente trabajo tuvo como objetivo Proponer planes de mejoramiento que redunden en la gestión de la información mediante la aplicación de procesos de auditoría a la seguridad basada en el estándar ISO 27001 en el sistema de información SIVIGILA de la Secretaria de Salud de la alcaldía de Tumaco. De esta la como primera meta es identificar el lugar a auditar que permita desarrollar una investigación completa y verídica que dé lugar a un plan de auditoria completo y acorde con las necesidades de la entidad que se está evaluando, seguido del desarrollo de un plan de auditoria acorde con la investigación hecha en el lugar a auditar, una vez hecho esto desarrollar herramientas, técnicas y procedimientos para la recolección de información y obtención de evidencias en el proceso de auditoría, las cuales permitieron obtener evidencias mediante la ejecución del plan de auditoria, sintetizar y sistematizar los hallazgos del resultado del proceso de auditoría, haciendo posible la socialización del informe final de auditoria a la alcaldía de Tumaco.

De esta manera, tuvo como referencia varios entandares reconocidos internacionalmente como COBIT, MAGERIT y la norma ISO/IEC 27001 siendo esta la más importante ya que es la base del presente proyecto permitiendo trabajar los controles y sus objetivos en el sistema de información Sivigila y su entorno estableciendo para el auditor grados de cumplimiento de los mismos dentro de la entidad reconocida como el entorno auditable.

Fue necesario también hacer gestión de riesgo ya que toda entidad posee unos activos y estos a su vez estarán expuestos a posibles amenazas y este tipo de estudio lo hace posible la Metodología de Gestión de Riesgos llamada también MAGERIT, donde se tuvo la frecuencia de las amenazas sobre los activos el impactos de las mismas desarrollando un cruce de ambas que dejó como resultado una tabla que muestra la situación de riesgo de los activos relacionados con el Sivigila.

Como resultado obtenido de los hallazgos y evidencia del proceso de auditoria se propuso unas recomendaciones y también el cuerpo de una Política de Seguridad de la información para la Alcaldía de San Andrés de Tumaco ya propuesta en un documento que se adiciona en la entrega, además de la propuesta de divulgación de la política antes mencionada.

ABSTRACT

This paper aims to propose improvement plans that result in information management processes by applying the safety audit based on ISO 27001 standard in the information system SIVIGILA health secretary of the mayor of Tumaco. Thus as the first goal to identify the place to audit that allows to develop a complete and truthful investigation resulting in a complete audit plan and meets the needs of the entity being evaluated, followed by development of an audit plan accordingly with the research done in place to audit, once that is done to develop tools, techniques and procedures for gathering information and obtaining evidence in the audit process, which allowed to obtain evidence by executing the audit plan, synthesize and systematize the findings of the outcome of the audit process, enabling the socialization of the final audit report to the mayor of Tumaco.

This way I had the reference number entandares internationally recognized COBIT, MAGERIT and ISO / IEC 27001 being the most important because it is the basis of this project allowing to work the controls and objectives in the information system SIVIGILA and environment establishing for the auditor degree of compliance with them within the entity known as the auditable environment.

It was also necessary to risk management and that every entity has few assets and these in turn be exposed to potential threats and this type of study makes it possible Methodology Risk Management also called MAGERIT, where the frequency of threats had the impact on the assets of these developing a crossing that left both result in a table showing the risk of assets related SIVIGILA.

As a result of the findings and evidence of the audit process and recommendations about the body of a Security Policy Information for mayor of San Andrés de Tumaco proposal in a document it is added to the proposed delivery plus the proposed disclosure of the aforesaid policy.

INTRODUCCIÓN

La información es el activo que hace a las organizaciones en la actualidad, porque es esta que le da valor a las cosas, siendo una serie de conjuntos de datos muy bien organizados que finalmente producen un mensaje sobre algún tema. En estos momentos se puede decir que la información es la columna vertebral de una empresa puesto que es esta la que maneja todos los registros que hacen que dicha entidad crezca o fracase; es necesario destacar que las malas o buenas decisiones que se tomen en un entorno empresarial depende de la información que en este se esté manejando ya que según lo que se sabe es lo que hace una determinación acertada o fallida.

Si en una empresa se tiene claro que uno de los bienes más importantes es la información, entonces llegara el momento de pensar en protegerla puesto que en algún instante de emergencia si esta se encuentra segura dicha entidad volverá a levantarse sin problema, porque ha sabido guardar muy bien los datos que maneja, se sabe que en estos momentos de la historia de la humanidad todo es absolutamente vulnerable y por esta razón se han creado controles, planes que eviten que todo lo que se maneje sea amenazado o dañado, como un bien importante que son los datos los cuales constituyen la información siempre sufren daños y son amenazados con ser modificados o eliminados, para ello existen estándares y personal debidamente autorizado para evitar situaciones en las empresas que resulten desagradables en cuanto al manejo de la información.

La Alcaldía de Tumaco es la entidad que vela por el bienestar de la comunidad tumaqueña, teniendo en cuenta que el bien común es el que prima entre sus funciones, desde este lugar se expiden las decisiones que sean necesarias para el municipio en conformidad con las leyes de la constitución, también se administran, coordinan, todos los bienes que pertenecen al municipio; siendo este el lugar que maneje asuntos importantes, es el sitio justo para demostrar que el flujo de información es enorme y de proporciones algo sorprendentes y que podría ser considerado como blanco de ataque para robar o dañar información.

Actualmente la Alcaldía de Tumaco no tiene un conducto regular de manejo de la seguridad de la información, no se ha contemplado realizar auditorías donde se evalué la seguridad de los datos, SIVIGILA es uno de los sistemas de información que maneja esta entidad en la secretaria de salud es una aplicación de escritorio que hace reportes q son enviados al departamento, sobre el estado epidemiológico del municipio de Tumaco.

Este trabajo busca auditar la seguridad apoyado en la norma ISO 270001 en la secretaria de salud de la alcaldía de Tumaco con el fin establecer y unificar que controles de seguridad manejan en esta parte de la entidad antes expuestos y en base a esto establecer recomendaciones que ayuden y hagan una diferencia en el manejo de la información en comparación con los otros sistemas de información manejados en esta institución.

Una auditoria busca conservar la confiabilidad, integridad y sobre todo confidencialidad de los datos, buscando de esta forma que toda la información que se maneje en una entidad sea veraz y que siempre este a tiempo cuando esta se necesite.

Por lo dicho anteriormente este trabajo expone los riesgos de seguridad identificados a los que se encuentra expuesto el sistema de información SIVIGILA de la secretaria de salud en la Alcaldía de San Andrés de Tumaco.

ELEMENTOS DE INVESTIGACIÓN

TEMA DE INVESTIGACIÓN

Política de Seguridad de Información en las instituciones públicas del Gobierno basados en norma ISO/IEC 27001.

ÁREA DE INVESTIGACIÓN

Política de Seguridad de Información para la alcaldía de San Andrés de Tumaco se ubica dentro del área de investigación de Auditoría de Sistemas Computacionales definido por el comité curricular del Programa de Ingeniería de Sistemas de la Universidad de Nariño.

LÍNEA DE INVESTIGACIÓN

El proyecto pertenece a la línea de investigación: GESTIÓN, SEGURIDAD Y CONTROL. Esta línea tiene como objetivo planificar, analizar, diseñar e implantar sistemas de control de información, con el propósito de brindar seguridad de la información en las organizaciones.

DESCRIPCIÓN DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

SIVIGILA es un sistema de información estatal es decir que desde el Estado se hace un manejo general, pero en cada gobernación y alcaldía se tiene una aplicación personal para el manejo de datos locales, esto ha ocasionado que en la alcaldía exista la poca gestión por cuidar de la información que este maneje, de cierta forma delegan todo el trato de la información a terceros y no cuidan de forma local también dichos datos. No existen controles locales autónomos que den fe que la información que tenga este sistema esté bien cuidada, es decir se han limitado a optar por el papel de usuarios finales el cual maneja mecánicamente la aplicación sin saber a ciencia cierta si esta guarda bien los datos ingresados, si es verdad que la información está siendo manejada por el personal adecuado y demás situaciones que no dan grado de confianza sobre la seguridad e integridad de los datos.

La Alcaldía de Tumaco hasta el momento no ha realizado una auditoria de seguridad por esta razón no se ha dispuesto lineamientos que ayuden a proteger la información como activo que es en la entidad; en el manejo del Sistema de información SIVIGILA la documentación que se tiene es la que reposa en la web dada de forma general para todas las entidades locales, pero no se tiene documentos de tipo personal como institución local. Es preocupante el trato y el poco orden que se está dando a la información el punto es que no se tiene claro es si tan maltrato de la información es por falta de educación al personal en cuanto a la importancia de la seguridad de los datos o es que el talento humano no está interesado en seguir normas que estén acorde para la protección de la información; si se tiene un personal que vigile la seguridad de la información no se sabe a ciencia cierta en estos momentos en que actividades se está ocupando dicho talento humano, según lo antes dicho es de suma importancia al menos empezar a evaluar cuál es el motivo que causa el manejo tan pobre que se le da a la seguridad de la información y aún más concientizar al personal de que esta es de suma importancia para una entidad de este tipo donde se supone que se tienen datos, proyectos y todo tipo de información importante que involucra a todo un municipio es una obligación tener controles de manejo de la misma, y para saber que se tiene a favor y en contra en el aspecto de seguridad es necesario evaluar para establecer planes de mejora.

SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cuál es el tipo de información que maneja el área secretaria de salud de la alcaldía de Tumaco?
- ¿Cuáles son los recursos informáticos disponibles en la secretaria de salud para el manejo de la información?
- ¿Qué inconvenientes ha presentado el manejo de la información en el área de la secretaria de salud de la alcaldía de Tumaco?
- ¿Qué actividades de mejoramiento se pueden implementar en la seguridad de la información en la secretaria de salud de la alcaldía de Tumaco?

FORMULACIÓN DEL PROBLEMA

¿Cómo la auditoria a la seguridad basada en el estándar ISO 27001 al sistema de información SIVIGILA de la secretaria de salud ayudará a proponer políticas de mejoramiento que redunden en una gestión de la información en la alcaldía del municipio de Tumaco?

OBJETIVOS

OBJETIVO GENERAL

Proponer políticas de mejoramiento que redunden en la gestión de la información mediante la aplicación de procesos de auditoría a la seguridad basada en el estándar ISO 27001 en el sistema de información SIVIGILA de la secretaria de salud de la alcaldía de Tumaco.

OBJETIVOS ESPECÍFICOS

- Identificar el lugar a auditar que permita desarrollar una investigación completa y verídica que dé lugar a un plan de auditoria completo y que valla acorde con las necesidades de la entidad que se está evaluando.
- Desarrollar un plan de auditoria acorde con la investigación hecha en el lugar a auditar.
- Desarrollar herramientas, técnicas y procedimientos para la recolección de información y obtención de evidencias en el proceso de auditoría.
- Obtener evidencias mediante la ejecución del plan de auditoria.
- Sintetizar y sistematizar los hallazgos del resultado del proceso de auditoría
- Socializar el informe final de auditoria a la alcaldía de Tumaco

JUSTIFICACIÓN

El presente trabajo se hace con el fin de mejorar falencias que pueda tener el manejo de la información en el Sistema de Información SIVIGILA manejado en la secretaria de salud de la alcaldía de Tumaco, busca evaluar los controles de seguridad, con la finalidad de actualizar la forma como se trata a la información en esta entidad, ya que el hecho de que Tumaco este pasando por problemas de orden público y demás situaciones que dañan la imagen del municipio ante el exterior no quita el derecho y deber que este tiene para mejorar, y hacer que este al día en el desarrollo de sus procesos, debe quedar claro que como organización que manipula información que puede beneficiar o perjudicar a toda una comunidad esta tiene la obligación de mantener a salvo todos los datos que se encuentren en su poder, porque esta es la única forma de asegurar éxito en la ejecución de sus funciones; es el momento de mirar hacia afuera y tomar ejemplo de otras entidades con las mismas funciones donde estas ya se dieron cuenta que si tienen a salvo un activo tan importante como es la información tendrán a salvo el poder,

por esta razón, se necesitan controles que dejen claro roles y responsabilidades, compromiso de la administración con la seguridad de la información, conductos regulares que se deben seguir para acceder a información delicada, clasificación de la información, quienes pueden manejar información confidencial y quienes no deben hacerse cargo de una tarea como esta además de otros controles que se contemplan como limitante de este proyecto.

Los beneficiados inicialmente será todo el personal que maneja el sistema de información que se está auditando porque ellos son parte de los usuarios finales del SIVIGILA y si ellos ponen en práctica actividades que vayan en pro del cuidado de la información generarían un ambiente de concientización con respecto al personal que en inicios no está contemplado en el trabajo; la alcaldía en general como entidad empezaría un proceso serio de seguridad de la información generando en los habitantes de Tumaco un ambiente de confianza sobre los procesos que se manejan desde esta haciéndose en orden y siguiendo un conducto regular exacto.

Auditar es importante porque es la única forma de saber que se tiene a favor y que se tiene en contra, y aquello que es ventaja como se puede hacer mejor si es posible y lo que resulte una desventaja como volver esto una fortaleza, y el tiempo de tomar conciencia sobre la seguridad de la información es ahora y dicha actividad es proporcionada por un plan de auditoria serio y verídico.

DELIMITACIÓN

El presente trabajo permitirá revisar, analizar y evaluar el sistema de información SIVIGILA de la secretaria de salud en la Alcaldía de San Andrés de Tumaco, con la finalidad de identificar debilidades y amenazas en cuanto a la seguridad, a la que este se encuentre expuesto, y determinar si existe un sistema de control y a que estándar este se encuentra sujeto.

Del sistema de información SIVIGILA, se evaluará:

- Documentos de política de seguridad del sistema de información
- Bitácoras de revisión de la política de seguridad de la información
- Compromiso de la administración con las políticas de seguridad de la información.
- Coordinación de la seguridad de la información
- Asignación de responsabilidades para la protección de la información.
- Acuerdos sobre confidencialidad.
- Directrices de clasificación de la información.

- Etiquetado y manejo de la información.
- Proceso disciplinario si hay mal manejo de la información.
- Monitoreo y revisión de servicios dados por terceros al sistema de información.
- Controles contra códigos maliciosos.
- Respaldo de información.
- Seguridad de la documentación.
- Políticas y procedimiento para el intercambio de la información.
- Monitoreo del uso del sistema de información.
- Registro de fallas.
- Registro de usuarios.
- Gestión de privilegios.
- Gestión de contraseñas
- Políticas de escritorio despejado y de pantallas despejadas.
- Uso de contraseñas.
- Aislamiento de información sensible, dentro del sistema de información.
- Validación de datos.

1 MARCO REFERENCIAL

1.1 ANTECEDENTES

En el ámbito regional.

La Universidad de Nariño ya ha tenido trabajos relacionados con auditoria de sistemas de los cuales se destaca:

- "DEFINICION DE POLITICAS DE SEGURIDAD INFORMATICA PARA EL CENTRO DE INFORMATICA DE LA UNIVERSIDAD DE NARIÑO" desarrollada por los estudiantes [María Constanza Torres B. y Efraín Fajardo Guevara]. Este trabajo realizo los procesos de auditoría a la seguridad del Centro de Informática de la Universidad de Nariño. Servirá de base para trazar algunas pautas de tareas de auditoria.

- AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARÍA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO" desarrollado por el estudiante [Oscar Julián Estrada Obando]. Este proyecto ejecuto una auditoría de sistemas tendiente a identificar las vulnerabilidades de seguridad física y lógica que presentaba el sistema integral de información (SII) en la Secretaría de Planeación Municipal de la alcaldía de Pasto. Servirá como ejemplo para saber cómo se maneja la auditoria a sistema de información.

- "AUDITORÍA APLICADA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN DINÁMICA GERENCIAL HOSPITALARIA DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO" desarrollada por las estudiantes [Edith Friney Diaz Fuelantala Y Maira Alejandra Mora Enríquez]. Este trabajo identificó de los diferentes riesgos y vulnerabilidades de seguridad lógica, a las cuales se encuentra expuesto el Sistema de Información Dinámica Gerencial Hospitalaria. Es una ayuda importante porque contempla la evaluación de la seguridad a un sistema y es una base que se tendrá en cuenta para trazar ítems de análisis para el presente trabajo.

1.2 MARCO TEÓRICOS.

Para el desarrollo satisfactorio de la investigación es necesario tener un marco conceptual y teórico que sustente cada procedimiento que se llevó a cabo. Por esta razón es necesario abordar los siguientes temas.

Auditoria. Para Echenique García José Antonio[1] la auditoria es un examen crítico que se realiza con objetivo de evaluar la eficiencia y la eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos. Igualmente Muños Razo Carlos[2] define la auditoria como la revisión independiente de alguna o de algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoria, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.

De la misma forma Sánchez Gabriel Curiel[3] define la auditoria como el examen integral sobre la estructura, las transacciones y el desempeño de una entidad económica para contribuir a la oportuna prevención de riesgos, la productividad en la utilización de los recursos y el acatamiento permanente de los mecanismos de control implantados por la administración. Las anteriores definiciones permiten concluir que auditoria es aquel trabajo de evaluación que se realiza a una entidad con la finalidad de mejorar y fortalecer sus procesos.

Tipos de auditoria. La clasificación de auditoria varía por autor, algunos la clasifican por su naturaleza, otros por el lugar de aplicación, en esta ocasión se analizara la opinión de Carlos Muños Razo[4] quien las clasifica de la siguiente manera:

- **Por su lugar de aplicación:** se refiere a la forma en que se realiza el tipo de trabajo, y también a como se establece la relación laboral en las empresas donde se llevara a cabo la auditoria, en esta categoría se tiene.

[1] ECHENIQUE GARCÍA, José Antonio. Auditoria En Informática: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág.11.
[2] RAZO MUÑOZ Carlos . Auditoria en Sistemas Computacionales: Pearson Educacion Mexico 2002. Pág. 11,12.
[3] SANCHEZ CURIEL Gabriel. Auditoria de Sistemas Financieros: Pearson Educacion Mexico 2006. Pág. 2.

- Auditoria externa
- Auditoria interna

❖ **Por su área de aplicación:** se refiere al ámbito específico donde se llevan a cabo las actividades y operaciones que serán auditada, ubicando a cada tipo de auditoria de acuerdo con el área de trabajo e influencia de la rama o especialidad que será evaluada, según lo anterior se tiene.

- Auditoría financiera
- Auditoria administrativa
- Auditoria operacional
- Auditoría integral
- Auditoria gubernamental
- Auditoria de sistemas

❖ **Especializadas en áreas específicas:** estos tipos de auditorías están enfocadas a satisfacer las necesidades concretas de revisión y dictamen, según la especialidad que se trate, en este grupo están.

- Auditoria al área médica(evaluación médica-sanitaria)
- Auditoria al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría fiscal
- Auditoria laboral
- Auditoria de proyectos de inversión
- Auditoria a la caja chica o caja mayor(arqueos)
- Auditoria al manejo de mercancías(inventarios)
- Auditoría ambiental
- Auditoria de sistemas

❖ **De sistemas computacionales:** estas se aplican para las diferentes áreas y disciplinas de ambiente informático.

- Auditoria informática
- Auditoria con la computadora
- Auditoria sin la computadora
- Auditoria a la gestión informática
- Auditoria al sistema de cómputo
- Auditoria alrededor de la computadora

- Auditoria de la seguridad de sistemas computacionales
- Auditoria a los sistemas de redes
- Auditoría integral a los centros de computo
- Auditoria ISO-9000 a los sistemas computacionales
- Auditoria outsourcing
- Auditoria ergonómica de sistemas computacionales

El trabajo en cuestión por su finalidad y objeto de estudio se enfocara en la seguridad de la informática basada en la norma ISO/IEC 27001, de esta manera se ubica en el tipo auditoria de la seguridad de sistemas computacionales, haciendo posible evaluar aspecto de la seguridad del sistema de información Sivigila en la alcaldía de Tumaco.

Auditoria informática. Piattini Velthuis Mario[5], define la auditoria informática como el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

A su vez para Muñoz Razo Carlos[6], la auditoria informática es la revisión técnica, exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos, y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.

Igualmente Echenique José Antonio[7] define la auditoria informática como la revisión y evaluación de controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización eficiencia y seguridad de la organización que participa en el procedimiento 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. Según los anteriores aportes se puede decir que la auditoria informática se enfoca en la revisión y evaluación de la parte tecnológica de las organizaciones, buscando la mejora y continuación de los objetivos de negocio de las entidades.

[5] PIATTINI Marco. Auditoria de Tecnologia y Sistemas de Informacion: Spanish Edition 2008. Pág. 7

[6] RAZO MUÑOZ Carlos . Auditoria en Sistemas Computacionales: Pearson Educacion Mexico 2002. Pág. 23

[7] ECHENIQUE GARCÍA, José Antonio. Auditoria En Informática: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág. 2

Todo proceso de auditoría para un posterior análisis de información requiere unas técnicas que permitan que el desarrollo del trabajo sea satisfactorio y de acuerdo con las necesidades de la situación que se esté tratando, por esta razón es vital conocer teóricamente que son y cuáles son las técnicas de auditoria las cuales se describen a continuación.

Técnicas de auditoria. Según el IMCP[8] (Colegio de Contadores Públicos de México), para realizar una auditoria es necesario apegarse a ciertos lineamientos que son normativos y algunos meramente sugerencias, para ellos las técnicas son el medio por el cual auditor obtiene evidencia y así puede fundamentar su opinión estrictamente profesional, siendo estas los métodos prácticos de investigación y prueba que el profesional utiliza para lograr la información y comprobación necesaria para sustentar su opinión.

De igual forma Muñoz Razo Carlos, aborda diciendo que las técnicas de auditoria son las herramientas que el auditor utiliza para llevar a cabo su trabajo, ubicándola en tres grupos grandes, considerando a las herramientas tradicionales y otras herramientas específicas aplicables a los sistemas computacionales, mostrándolas de esta forma.

Instrumentos de recopilación de datos aplicables en la auditoria de sistemas.

En este grupo se encuentran:

- Entrevista
- Cuestionario
- Encuesta
- Observación
- Inventarios
- Muestreo
- Experimentación

Técnicas de evaluación aplicables en la auditoria de sistemas

Aquí se encuentran:

- Examen
- Inspección
- Confirmación
- Comparación
- Revisión documental

[8]ICMP. [en línea]. <http://www.ccpm.org.mx/avisos/boletines/boletinauditoria12.pdf > [citado en 19 de octubre de 2015]

Técnicas especiales para la auditoria de sistemas computacionales
Las cuales son:

- Guía de evaluación
- Ponderación
- Simulación
- Diagrama del circulo de sistemas
- Diagrama de sistemas
- Matriz de evaluación
- Programas de verificación
- Seguimiento de programación

Las técnicas usadas globalmente para el proceso de auditoria son:

- Estudio general
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaración
- Certificación
- Observación

Mencionar y tener en cuenta las técnicas de auditoria es necesario para el marco de este trabajo porque, se necesitan bases para saber cómo obtener información que se lleve a la culminación positiva del proyecto y deje resultados satisfactorios para las partes involucradas.

Tomando lo dicho por los autores mencionados acerca de las técnicas de auditoria el presente trabajo tendrá en cuenta estudio general, análisis, investigación y observación del funcionamiento y manejo de la seguridad de la información del sistema Sivigila de la secretaria de salud de la alcaldía de Tumaco bajo la orientación de la norma ISO/IEC 27001 quien es el marco de referencia principal para el desarrollo de este trabajo.

Estándares internacionales

❖ COBIT (control objetives of information and related technology)

COBIT[9] es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma. Siendo su misión investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

Según COBIT, para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios, se llaman:

- ❖ Planear y Organizar (PO) – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- ❖ Adquirir e Implementar (AI) – Proporciona las soluciones y las pasa para convertirlas en servicios.
- ❖ Entregar y Dar Soporte (DS) – Recibe las soluciones y las hace utilizables por los usuarios finales.
- ❖ Monitorear y Evaluar (ME) -Monitorear todos los procesos para asegurar que se sigue la dirección provista.

Para el trabajo COBIT fue un marco de referencia para visualizar que en todo negocio se tienen procesos y que llegado el momento de auditar los mismos es importante investigar para conocer cuáles son las partes débiles de la entidad para poder hablar de un desarrollo de un proceso de auditoría.

[9] COBIT 4.1, 2007, pág. 9

Según lo antes dicho todo proceso de auditoría requiere tener estándares reconocidos y aprobados que sirvan de referencia y soporte que permita desarrollar un trabajo serio y confiable.

- **MAGERIT**

MAGERIT[10] es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es un método de carácter público elaborado por el Consejo Superior de Informática (CSI), órgano del Ministerio de Administraciones Públicas (MAP), encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno Español.

Este método nace para minimizar los riesgos asociados al uso de Sistemas Informáticos y Telemáticos, garantizando la autenticación, confidencialidad, integridad y disponibilidad de dichos sistemas y generando de este modo confianza en el usuario de los mismos.

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información, persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Persigue los siguientes objetivos:

- Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

- Indirectos:

1. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

[10] MAGERIT Metodologia de Analsis y Gestion de Riesgos. pág. 7

Para el trabajo MAGERIT, permitió gestionar riesgos, haciendo de esta manera que identificarlos como amenazas para el sistema de información Sivigila y su entorno tuvieran una base y una razón lógica haciendo posible proponer planes de mejoramiento para los mismos.

En un trabajo de este tipo siempre será de gran importancia tener varios marcos de referencia que ayuden a que su desarrollo sea rápido y confiable. Por lo antes dicho a continuación se hace mención y descripción de la norma ISO/IEC 27001 siendo esta la principal herramienta utilizada en este proceso de auditoría.

- **ISO/IEC 27001**

La ISO/IEC 27001[11] ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple. Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas.

Promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización. Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un “enfoque basado en procesos”.
El enfoque basado en procesos para la gestión de la seguridad de la información, presentado en esta norma, estimula a sus usuarios a hacer énfasis en la importancia de:

a) Comprender los requisitos de seguridad de la información del negocio, y la necesidad de establecer la política y objetivos en relación con la seguridad de la información;

[11] NORMA TECNICA COLOMBIANA NTC-ISO/IEC 27001, 2006

b) Implementar y operar controles para manejar los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización;
c) El seguimiento y revisión del desempeño y eficacia del SGSI, y
d) La mejora continua basada en la medición de objetivos.

Esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI.
La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002) que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

Esta norma está alineada con la NTC-ISO 9001:2000 y la NTC-ISO 14001:2004, con el fin de apoyar la implementación y operación, consistentes e integradas con sistemas de gestión relacionados. Un sistema de gestión diseñado adecuadamente puede entonces satisfacer los requisitos de todas estas normas. Está diseñada para permitir que una organización alinee o integre su SGSI con los requisitos de los sistemas de gestión relacionados.

Una vez descritos y analizados los anteriores estándares ya mencionados para el sentido y fin del proyecto se decide trabajar con la norma ISO/IEC 27001 ya que esta permite el análisis por controles haciendo más fácil la comprensión de los sistemas de información y la seguridad de los mismo permitiendo.

Auditoria de la seguridad informática

Para Castello Ricardo[12] la auditoria de la seguridad informática en una organización se debe abordar considerando tres situaciones básicas.

1. Cuando la organización tiene planes y/o políticas de seguridad informática formalizados (escritos, implementados, explícitos).
2. Cuando la organización no cuenta con planes formalizados pero tiene implementadas medidas de seguridad para proteger sus sistemas y equipamiento. Si estas prácticas no están documentadas ni fueron seleccionadas luego de un proceso formal de análisis forman parte de una

[12] CASTELLO, Ricardo. Auditoria de Entornos Informaticos: Segunda edición - Diciembre de 2006 I.S.B.N. 950-33-0199-8 2006. Pág. 225

política de seguridad informal; además, están operativas y protegen eficazmente las preocupaciones básicas de la empresa.

3. Cuando la organización carece de cualquier política de seguridad, actúa con la "política de bombero", es decir reaccionando ante situaciones consumadas de daños y/o perjuicios relacionados con los servicios informáticos.

- Según Castello, el mejor caso para auditar es el primer caso porque el auditor tiene la oportunidad de contrastar la práctica y situación de los servicios de sistemas contra los planes y políticas de seguridad informática. En este caso la documentación que se sugiere evaluar es: Planes y Proyectos de Seguridad Informática, Planes de Contingencia, procedimientos relacionados con seguridad, contratos con proveedores de seguridad informática, etc.

- En el segundo caso, el auditor debe relevar las prácticas vigentes, sugerir su formalización y por ultimo puede hacer consideraciones respecto a la eficacia de las mismas

- En la última situación Castello refiere que el auditor carece prácticamente de "cuadro de referencia" para hacer consideraciones, salvo situaciones obvias que detecte, como carencia de copias de seguridad, acceso irrestricto a sistemas y archivos.

Seguridad informática

Jesús Rodea[13] (1994), definió la seguridad como un estado de cualquier sistema que indica que ese sistema está libre de peligro, daño o riesgo; peligro o daño se entiende como todo aquello que pueda afectar el funcionamiento directo o los resultados que se obtienen del mismo. Los expertos en su mayoría consideran el significado de seguridad informática es utópico porque a decir verdad sistema 100% seguro no existe.

Para que un sistema se pueda definir como seguro debe tener:

1. Integridad: La información sólo puede ser modificada por quien está autorizado.
2. Confidencialidad: La información sólo debe ser legible para los autorizados.
3. Disponibilidad: Debe estar disponible cuando se necesita.
4. Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

[13] RODEA, Jesus. Seguridad Informatica. Pág. 26

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en seguridad lógica y seguridad física.

Sistemas 100% seguros no los hay pero es tarea de las organizaciones alcanzar el máximo de seguridad que sea posible en cada una de sus áreas.

Política de seguridad de la información.

La Política de Seguridad es la demostración de la Dirección sobre el propósito y compromiso de la seguridad de la información en la organización. La Política debería girar en torno a la criticidad de la información identificada en las anteriores tareas. La Política deberá reflejar cuestiones como:

- ¿Por qué la información es importante y estratégica para la Organización?
- ¿Qué son los requisitos legales y de negocio para la seguridad de la información?
- ¿Cuáles son las obligaciones contractuales relativas a procesos de negocio, clientes, empleados, etc.?
- Qué pasos debe tomar la organización para garantizar la seguridad de la información

La política que se presente debe tener como mínimo:

- Una definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información
- El establecimiento del objetivo de la Dirección como soporte de los objetivos y principios de la seguridad de la información
- Una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la Organización, por ejemplo:

    1. Conformidad con los requisitos legislativos y contractuales
    2. Requisitos de formación en seguridad
    3. Prevención y detección de virus y otro software malicioso
    4. Gestión de la continuidad del negocio
    5. Consecuencias de las violaciones de la política de seguridad
    6. Requisitos de uso de los Sistemas de Información como gestión de contraseñas, acceso a internet, uso de e-mail
    7. Controles técnicos.
        - Controles de cambio de software
        - Controles de versión
        - Seguridad de bases de datos
        - Seguridad de redes y telecomunicaciones

- Seguridad de Sistemas operativos
- Seguridad de Firewalls
- Respuesta ante incidentes
- Seguridad de servidores web
- Seguridad de Intranet
- Seguridad de comercio electrónico
- Cifrado de datos

8. Controles establecidos sobre empresas externas o teletrabajo

- ❖ Una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad
- ❖ Las referencias a documentación que pueda sustentar la política como por ejemplo políticas y procedimientos mucho más detallados para Sistemas de Información específicos o las reglas de seguridad que los usuarios deberían cumplir

Se asignará un propietario responsable del mantenimiento y revisión de la política conforme a un proceso de revisión definido. Este proceso asegurará que la revisión responde a todo cambio que afecte a las bases de la evaluación original del riesgo como incidencias de seguridad significativas, nuevas vulnerabilidades y cambios organizativos o técnicos. Igualmente se definirán las revisiones periódicas de:

- ❖ La efectividad de la política (demostrada por el número e impacto de las incidencias de seguridad)
- ❖ El coste y el impacto de los controles en la eficiencia del negocio Los efectos de los cambios tecnológicos.

Según lo antes tratado el sistema de información Sivigila de la Secretaria de Salud de la Alcaldía de Tumaco no solo requiere de políticas de seguridad sino de todo un SGSI (SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN) que se profundiza a continuación, el cual se diseña para asegurar controles de seguridad suficientes que protejan los activos de información y brinden confianza a las partes involucradas.

SGSI sistemas de gestión de la seguridad de la información

La ISO-IEC 27001 lo define como parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizacional,

políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta. Para los propósitos de esta norma, el proceso usado se basa en el modelo PHVA

Modelo PHVA

- **Planificar (establecer el SGSI).** En esta etapa se establece la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
- **Hacer (implementar y operar el SGSI).** Durante esta etapa se Implementa y opera la política, los controles, procesos y procedimientos del SGSI.
- **Verificar (hacer seguimiento y revisar el SGSI)** Aquí se evalúa, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
- **Actuar (mantener y mejorar el SGSI).** En este momento se emprende acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

1.3 MARCO LEGAL.

El presente trabajo está sustentado en un contexto legal el cual contemplas tres normas ley 1273 del 2009 o de delitos informáticos, ley de protección de datos personales y la ley de derechos de autor, las cuales se describen a continuación

Ley 1273 del 2009. Esta Ley planteo nuevos tipos penales en relación con los delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. El sentido de esta ley está en que al mismo tiempo que crecen los avances tecnológicos a su vez aumenta los bienes de aquellos que se apropian de forma ilegal de los patrimonio de otros por medio de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para hacer posible las transferencias electrónicas de fondos mediante la manipulación de programas y afectación de los cajeros automáticos. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

Esta adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

Para el presente trabajo esta ley deja claro que en cada avance tecnológico que se dé habrá un ataque para el mismo, y que llegado el momento es comprensible tener presente en una auditoria todos los hallazgos que se encuentren y que de cierta forma no sean agradables para terceros estos pueden ser violados pero que a su vez una acción de este tipo tiene su penalización correspondiente.

En todo desarrollo de una auditoría habrán datos que serán delicados y privados para la empresa, por esta razón es necesario conocer que ley penaliza la violación de los datos personales la cual se describe a continuación.

Ley 1581 de 2012. Esta Ley busca dar protección a los datos personales registrados en cualquier base de datos que permite realizar operaciones, como recolección, almacenamiento, uso, circulación o supresión en cualquier entidad ya se pública o privada. Contempla los principios que deben seguirse en todo tratamiento de datos personales en los cuales se encuentran:

- Legalidad: el tratamiento es una actividad reglada por lo tanto debe sujetarse a lo establecido en ella y en las demás disposiciones.
- Finalidad: debe obedecer el tratamiento a una finalidad legítima de acuerdo con la constitución y la ley, la cual deber ser informada al titular.
- Libertad: solo puede ejercerse el tratamiento con el consentimiento, previo, expreso e informado del titular.
- Veracidad o calidad: la información que esté sujeta al tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Transparencia: se debe garantizar el derecho del titular en el tratamiento en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- Acceso y circulación restringida: el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y de la constitución.
- Seguridad: los datos personales deben tratarse con medidas técnicas, humanas y administrativas para dar seguridad a los registros de las bases de datos personales.
- Confidencialidad: todas las personas que participen en el tratamiento de datos personales deben garantizar la reserva de la información.

Esta Ley complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación, se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

Para el auditor del trabajo presente fue importante conocer que los datos que conoció en la empresa, son de esta y por lo tanto divulgarlos tiene una penalización, esto según la ley 1581 descrita anteriormente.

Todo trabajo con su autor respectivo debe ser respetado y no plagiado, en caso de violación a los derechos de autor la ley colombiana tiene unos parámetros de penalización que se mencionan en la siguiente ley de Derechos de Autor.

Ley de derechos de autor. Determina que todo autor desde el momento de la creación, dispone de unos derechos patrimoniales. Esto significa que todo creador o quien lo haya contratado o quien sea que haya adquirido derechos de explotación sobre una obra, dispone del derecho exclusivo de autorizar o prohibir cualquier forma de explotación. Mientras alguien sea titular o propietario de unos derechos, puede administrar y explotar su obra como a bien tenga. El problema es que pesar de que esto en teoría es viable, en la práctica y ante diversas formas de explotación, le queda absolutamente imposible a un creador titular de sus derechos, hacer esa gestión individual.

Respetar el trabajo de otros haciendo mención de ellos en caso de necesitarlo es una forma de respeto por quien hizo el trabajo y aun para el que pretende hacer algo nuevo o una mejora.

2 METODOLOGÍA

Tipo de investigación

El presente trabajo sigue una investigación descriptiva-aplicativa, descriptiva ya que según Sampieri[14], los estudios descriptivos permiten detallar situaciones y eventos, diciendo como es y cómo se manifiesta un determinados fenómeno, buscando especificar propiedades importantes de cualquier detalles sometido a un análisis; de la misma forma ya que según lo dicho por Sampieri el tipo de investigación aplicativa permite que de la información y el análisis obtenido se utilizará todo el conocimiento consolidados para desarrollar un manual de política de seguridad de la información para la secretaria de salud de la alcaldía de Tumaco, el cual sirva como iniciativa de protección al sistema Sivigila donde se procesa información desde las oficinas ante mencionadas permitiendo de esta manera que todo lo que emita sea manejado con orden y por medio de controles ya previamente establecidos.

Paradigma

De acuerdo con lo antes dicho es necesario mencionar que para el desarrollo de la auditoria se tuvo en cuenta el siguiente paradigma:

Porque por todo lo antes mencionado en los tipos de la investigación este permite trazar datos que son más sencillos de demostrar en gráficas y tablas fáciles de explicar y por consiguiente de interpretar.

Enfoque empírico analítico

Este busca la explicación, la determinación de causas y efectos cuantitativamente comprobables y repetibles en contextos diversos con variables de control en este la realidad se desagrega por variables cuantificables se buscan regularidades que permitan proposiciones, permitiendo que su interés es técnico: ambiciona predecir y controlar los hechos que estudia para modificarlos.

[14] SAMPIERI, Hernández. Metodología de la investigación, México, D.F. McGrawHill de México. Pag 185.

Población

Para el desarrollo de este trabajo la población fue de 23 UPGD (Unidades Primarias Generadoras de Datos) del Sivigila, la UNM (Unidad Notificadora Municipal) la señora Yamileth Ramos y el Coordinador de Sistemas de la Alcaldía de Tumaco el señor Jhon Javier Mininderos.

Las UPGD (Unidades Primarias Generadoras de Datos) que notifican al Sivigila, son:

- Batallón.
- CDIN
- Clínica Miramar
- Confamiliar
- IPS los Ángeles Coomeva
- Comité Magisterio
- Comité Puerto
- Centro Hospital Divino Niño
- Puesto de Salud las Flores
- Puesto de Salud la Coordialidad
- Puesto de Salud las Palmas
- Puesto de Salud Viento Libre
- Puesto de Salud Llorente
- Puesto de Salud Imbili
- IPS Emsanar
- IPS Global Salud
- Hospital San Andrés de Tumaco
- INPEC
- IPS los Ángeles
- IPS Puente del Medio
- IPS Unipa
- Policía
- Corporación Nariño.

Muestra

La muestra para el desarrollo de este trabajo fue la UNM del Sivigila y el Coordinador de Sistemas de la Alcaldía. La UNM porque es quien tiene todo el consolidado del Sivigila y además porque es la que está autorizada para dar

código de configuración del sistema, en tal caso que ella no esté disponible para notificar al departamento no hay hasta el momento otro funcionario que lo haga, en conclusión es la UNM quien tiene toda la información dada por el Sivigila. Al coordinador de sistemas porque es el quien configura los sistemas de información y porque como ingeniero de sistemas podrá dar aportes enfocado al tema y sentido de este trabajo.

Instrumentos de recolección de la información

Para llegar a una conclusión y dar recomendaciones sobre algún tema en especial, es necesario tener bases y en este caso hay instrumentos de recolección de la datos que permiten tener un consolidado de toda la información para desarrollar un trabajo responsable y real, en el presente proyecto se utilizaron los siguientes.

- **Entrevista.**

Según Muñoz Razo la entrevista permite obtener guías que serán importantes para su trabajo, e incluso, muchas veces se entera de tips que le permitirán conocer más sobre los puntos que puede evaluar o debe analizar y mucha más información forma directa, cara a cara y a través de algún medio de captura de datos, es decir, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que está auditando; en la aplicación de esta técnica, el auditor utiliza una guía de entrevista, la cual contiene una serie de preguntas preconcebidas que va adaptando conforme recibe la información del entrevistado, de acuerdo con las circunstancias que se le presentan y en busca de obtener más información útil para su trabajo. Este instrumento fue tenido en cuenta para el proceso de la auditoria porque se tiene entendido que los funcionarios que tiene un cargo administrativo de alto rango como en este caso la Jefe de Epidemiologia municipal siempre tienen ocupaciones y disponen un tiempo para este tipo de situaciones donde el auditor debe buscar las preguntas más concisas y claras para evitar intervenir en las actividades del entrevistado, además de la oportunidad de estar cara a cara con el principal usuario del sistema de información que en este caso es el Sivigila.

- **Observación directa.**

Muñoz Razo[15] la define como la inspección hecha directamente en el contexto donde se presenta el hecho o fenómeno observado, a fin de contemplar todos los aspectos inherentes al comportamiento, conducta y características de ese ambiente. En este caso, el observador (el auditor de sistemas) entra en contacto directo con el fenómeno observado, analizando su comportamiento de dos maneras; por un lado permanece aislado al observar el comportamiento del hecho o fenómeno (sistema) que va a estudiar, y por otro lado participa en dicho fenómeno al observarlo. Lo importante es observar en forma directa lo que acontece en el sistema o área de sistemas auditada. A continuación, se presenta algunos ejemplos de observación:

- La forma en que ingresan los usuarios al centro de cómputo, a fin de conocer las medidas de seguridad establecidas para el acceso a esta área.
- Observar el comportamiento de los usuarios de un sistema, a fin de evaluar su forma de utilizarlo.
- El trabajo que están realizando los usuarios del sistema, a fin de validar las bases de datos que éste está utilizando, sus privilegios y restricciones en el sistema, siempre que la observación no sea oculta, es decir, que el usuario sepa lo que hacen él y el administrador. En caso contrario, sería una observación oculta.

Este tipo de observaciones se aplica espontánea e intuitivamente en cualquier tipo de auditoría; hay que recordar que la principal función del auditor es observar el funcionamiento de lo que evalúa; en este caso, lo que observa del ambiente de sistemas en forma franca, abierta y concisa.

En el caso actual de la evaluación y revisión de la seguridad del Sivigila se optó por este instrumento porque es la mejor forma para que el auditor valide la información obtenida en la entrevista y las listas de chequeo, ya que lo que no se contempló en estas se puede visualizar directamente. Observar como el usuario maneja el Sivigila y como hacen la recepción de la información dejó para el auditor el aprendizaje para tener la autonomía, de manejar el sistema cuando ingresó para hacer las pruebas de funcionamiento. Además la mejor forma de darse cuenta como cada funcionario que tiene que ver con el sistema maneja y cuida la información que se obtiene.

[15] RAZO MUÑOZ, Carlos . Auditoria en Sistemas Computacionales: Pearson Educacion Mexico 2002. Pág. 359.

- **Lista de chequeo**

Llamada también en ingles checklist es una herramienta que se utiliza para extraer ciertas propiedades de aquello que somete a estudio, son presentadas de forma general en preguntas que se responden de manera binaria es decir lo tiene o no lo tiene, está presente o no está presente, cumple o no cumple, se pueden dar más de dos opciones de respuesta pero siempre de forma cerrada, si se quiere dejar un espacio para comentarios se lo puede hacer pero las respuestas siempre serán en modo cerrado.

Conocidas también como lista de verificación siendo una de las formas más objetivas para valorar el estado de aquello que se somete a control, el carácter cerrado de las preguntas proporciona objetividad, pero a su vez elimina información que no es útil, esta se utiliza con finalidades de evaluación, de control, de análisis y de verificación.

Del resultado de las listas de chequeo se puede deducir el valor de un indicador, o se puede utilizar para comparar entre varias opciones o establecer una foto fija de la situación actual que se vive en una entidad especifica.

El presente trabajo tomó como instrumento la lista de chequeo porque están proporciona información que se puede analizar gráficamente de forma más sencilla, además de permitir que el auditor tenga a su disposición la información que necesita y no tenerla de forma redundante y que no atrase el proceso de evaluación.

3 RESULTADOS DE LA INVESTIGACION.

3.1 ENTORNO AUDITABLE

3.1.1 ALCALDÍA DE TUMACO

Descripción general de la alcaldía de Tumaco

- **Misión**

El Municipio de Tumaco es una entidad territorial comprometida con la satisfacción de las necesidades básicas y la convivencia pacífica de su población, que aprovechando su ubicación geográfica, sus ecosistemas y su riqueza étnica y cultural, busca a través de la permanente interacción con la comunidad, la Nación y la comunidad internacional, con eficiencia, con efectividad y honestidad en su gestión, posicionarse como el Municipio líder del territorio región del Pacífico Sur Colombiano y punto de encuentro de la comunidad internacional.

- **Visión**

En el 2015 Tumaco será el mejor Territorio del Pacifico, con un modelo de desarrollo endógeno a escala humana en marcha que genera las condiciones que permitan a su población vivir con dignidad; una Entidad Territorial Incluyente y participativa, un pueblo socialmente desarrollado, con mayor formación en educación acorde con su cultura, más productivo, más competitivo, con mejor seguridad y convivencia ciudadana, ambiental y naturalmente sostenible, con mayor desarrollo deportivo y una mejor calidad de vida para la población en general.

- **Funciones**

Están contenidas en la Ley 136 de 1994 y sus Decretos Reglamentarios. ARTICULO 3º FUNCIONES: corresponde al municipio:

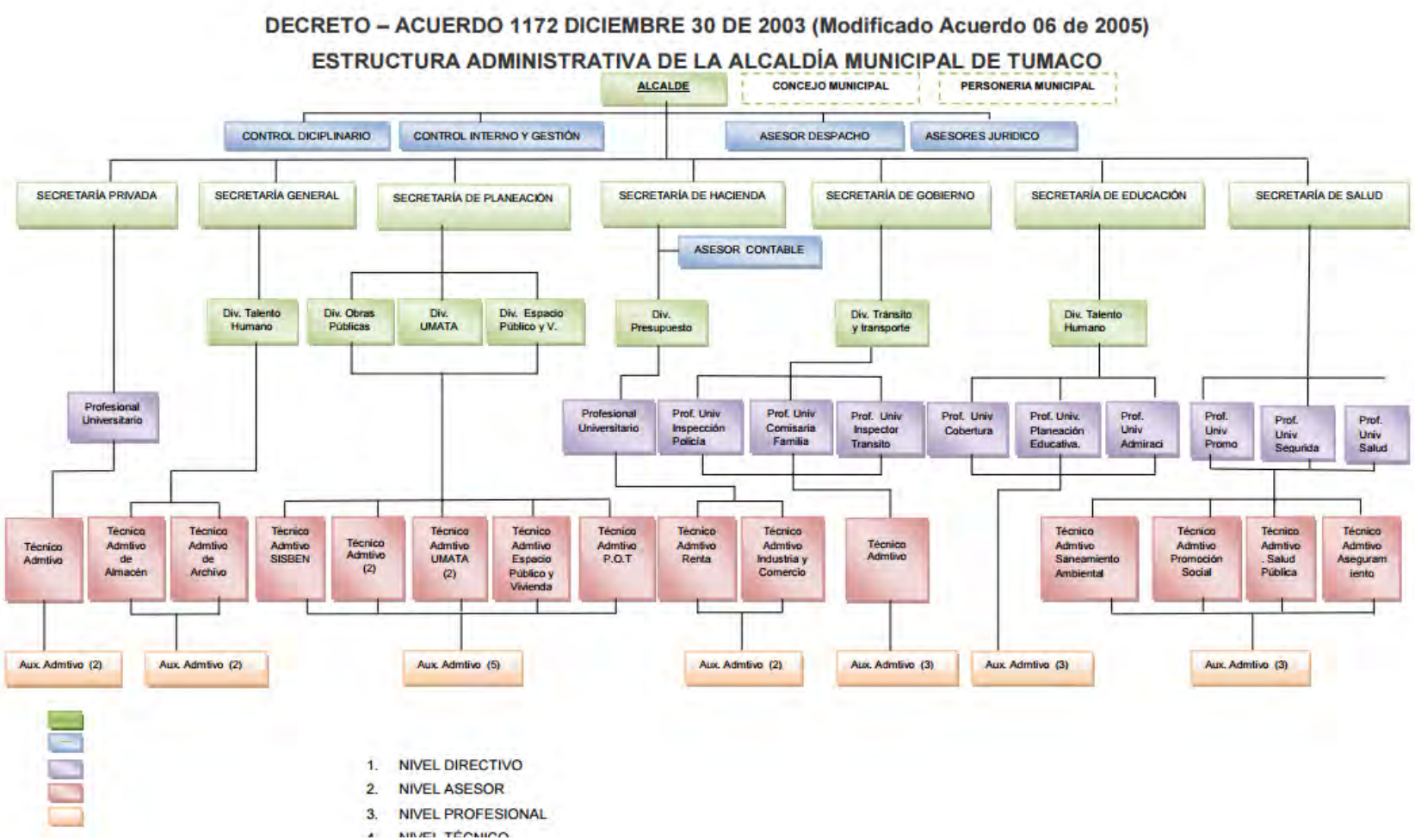
1) Administrar los asuntos municipales y prestar los servicios públicos que determine la ley.
2) Ordenar el desarrollo de su territorio y construir las obras que demande el progreso municipal.
3) Promover la participación comunitaria y el mejoramiento social y cultural de sus habitantes.
4) Planificar el desarrollo económico, social y ambiental de su territorio, de conformidad con la ley y en coordinación con otras entidades.
5) Solucionar las necesidades insatisfechas de salud, educación, saneamiento ambiental, agua potable, servicios públicos domiciliarios, vivienda recreación y deporte, con especial énfasis en la niñez, la mujer, la tercera edad y los sectores discapacitados, directamente y en concurrencia, complementariedad y coordinación con las demás entidades territoriales y la Nación, en los términos que defina la ley.
6) Velar por el adecuado manejo de los recursos naturales y del medio ambiente, de conformidad con la ley.
7) Promover el mejoramiento económico y social de los habitantes del respectivo municipio.
8) Hacer cuanto pueda adelantar por sí mismo, en subsidio de otras entidades territoriales, mientras éstas proveen lo necesario.
9) Las demás que le señale la Constitución y la ley.

- **Objetivos**

Los objetivos de Tumaco-Nariño, son todos aquellos inscritos en sus normas municipales, además de los que se encuentran detallados en el Plan de Desarrollo 2012 - 2015.

A continuación se muestra en la figura No 1 el organigrama de la Alcaldía de San Andrés de Tumaco.

Figura 1. Organigrama de la Alcaldía de Tumaco



Fuente: Sitio Web Oficial Alcaldía de Tumaco.

Despacho del Alcalde

❖ Misión

Representar legalmente al Municipio y cumplir con funciones de dirección general, formulación de políticas institucionales, adopción de planes, programas y proyectos, para promover el desarrollo, crecimiento económico y social del Municipio de Tumaco, conforme la Constitución, la Ley, las Ordenanzas, los Acuerdos, el Plan de Ordenamiento Territorial y el Plan de Desarrollo Municipal.

❖ Objetivos

- Representación legal del Municipio.
- Dirección y coordinación de la gestión interna y externa.
- Coordinación de la comunicación interna y externa.
- Gerencia de la Administración Municipal.

❖ Funcionario responsable

Víctor Arnulfo Gallo Ortiz
Alcalde Municipal
Fecha de posesión: Enero 02 de 2012

Despacho de Secretaria Privada

❖ Misión

Ofrecer a la comunidad del municipio de Tumaco espacios de participación ciudadana a través de estrategias que involucren el sano esparcimiento y optimización de los momentos de ocio.

La secretaria privada se identifica con el desarrollo de actividades, lúdicas, recreativas, de entretenimiento, culturales, turística y de conmemoración con el objetivo de preservar la identidad cultural, activar el turismo en la región, aprovechar el deporte como un estilo de vida, festejar fechas que para la comunidad hacen parte de su identidad y desarrollo como los carnavales.

Fortalecer la imagen de la administración municipal con la comunidad a través de la información diaria que se genera desde todas las dependencias de las diferentes secretarias de despacho para los medios de comunicación.

❖ **Objetivo**

Prestar los servicios asistenciales que requiere directamente el Alcalde como Jefe de la Administración y Representante Legal del Municipio, y el control en cuanto a la ejecución y desarrollo de las políticas, planes, programas y proyectos autorizados por el Alcalde Municipal a las dependencias internas del Municipio.

Despacho de Secretaria General

❖ **Misión**

Propiciar un ambiente organizacional adecuado entre la Administración Municipal y la comunidad, la satisfacción ciudadana con el gobierno y la satisfacción de los servidores públicos municipales con su ambiente laboral para que garantice el funcionamiento de la Alcaldía Municipal mediante la planificación logística de la Administración del Talento Humano, los recursos del software, hardware y el adecuado suministro de los elementos necesarios para su funcionamiento y el mantenimiento de su infraestructura.

❖ **Objetivos**

- Instaurar una estructura institucional moderna, eficaz y transparente.
- Implementar el sistema de control interno Distrital.
- Elevar el nivel de motivación y productividad de los servidores del distrito.
- Ofrecer una mejor organización a través del diseño de una nueva estructura administrativa.
- Ampliar la comunicación y relaciones con la comunidad, con el propósito de retroalimentar el ejercicio del gobierno social e incluyente.
- Mejorar la atención al público.

Despacho de Gobierno

❖ **Misión**

Garantizar la convivencia pacífica y la seguridad ciudadana en el Municipio, mediante la formulación y ejecución de planes, programas, proyectos y acciones en relación con seguridad, orden público, protección del consumidor, resolución pacífica de conflictos, ejercicio de las facultades y atribuciones de policía,

prevención y protección de la familia y apoyo a los organismos de seguridad y justicia.

- **Objetivo**

Proyectar, dirigir, implementar y controlar las políticas en materia de Gobierno, seguridad, orden público, asuntos electorales, participación ciudadana, desarrollo comunitario, atención en prevención de desastres, atención y ejercer el control sobre precios pesas, medidas, rifas, juegos y espectáculos, y aplicar las normas de Policía para promover el bienestar social de la comunidad.

Secretaria de Hacienda

- **Misión**

Garantizar la convivencia pacífica y la seguridad ciudadana en el Municipio, mediante la formulación y ejecución de planes, programas, proyectos y acciones en relación con seguridad, orden público, protección del consumidor, resolución pacífica de conflictos, ejercicio de las facultades y atribuciones de policía, prevención y protección de la familia y apoyo a los organismos de seguridad y justicia.

- **Objetivo**

Proyectar, dirigir, implementar y controlar las políticas en materia de Gobierno, seguridad, orden público, asuntos electorales, participación ciudadana, desarrollo comunitario, atención en prevención de desastres, atención y ejercer el control sobre precios pesas, medidas, rifas, juegos y espectáculos, y aplicar las normas de Policía para promover el bienestar social de la comunidad.

Secretaria de Planeación

- **Misión**

La Secretaría de Planeación Municipal de Tumaco cumple a cabalidad con las funciones de planificación, coordinación, asesoría, control y seguimiento de planes, programas y proyectos de desarrollo del municipio, para lograr un crecimiento armónico y equilibrado que mejore la calidad de vida de la población urbana y rural, manteniendo activos y fortalecidos los espacios e instancias de planificación participativa, garantizando la interacción continua entre la administración y los ciudadanos.

❖ **Objetivos**

- Preparar y actualizar los planes y programas de desarrollo económico y social, de obras públicas y ordenamiento territorial, efectuando el seguimiento y evaluación de resultados y determinar el logro de las metas propuestas para el desarrollo y cambio social del municipio.
- Formular y Elaborar el plan de Desarrollo Municipal para la vigencia de los años 2012 – 2015.
- Garantizar el efectivo cumplimiento y gestión en el seguimiento y evaluación de planes, programas y proyectos a nivel municipal.
- Identificar y valorar oportunidades de desarrollo económico, social, ambiental, tecnológico e institucional.
- Implementar y poner en funcionamiento modernas técnicas de gerencia administrativa, que permitan dinamizar y mejorar los niveles de competitividad y productividad de la Secretaría de Planeación, mediante la optimización de procesos, calidad del servicio y empoderamiento de talento humano para los desarrollos de la gestión de programas y proyectos.
- Orientar, dirigir y coordinar la formulación de políticas públicas, planes, programas y proyectos en asocio con entidades públicas y privadas, para integrar y focalizar el portafolio de inversiones de la región.
- Coordinar esfuerzos interinstitucionales con organismos departamentales, regionales, locales, nacionales e internacionales, sector privado y ONG'S, con el fin de fortalecer la capacidad económica y financiera de la región, para lograr el cumplimiento del plan de desarrollo Municipal.

Secretaria de Educación

❖ **Misión**

La Secretaría de Educación de Tumaco, tiene como misión, garantizar el acceso y la permanencia de los niños, niñas, jóvenes y adultos en el sistema educativo mediante la planeación, dirección y control de la educación, con calidad, eficiencia y pertinencia, promoviendo la implementación y ejecución de proyectos educativos; apoyado por personal altamente capacitado y regidos por el principio de equidad.

❖ **Objetivos**

Acompañar a las Instituciones y Centros Educativos del Distrito de Tumaco en el fortalecimiento y desarrollo de una política educativa que responda las necesidades del Distrito, con un sentido humano e incluyente, para el aporte al desarrollo de una sociedad productiva, dinámica y cultural respetando el medio ambiente.

Secretaria de Salud de la Alcaldía de Tumaco.

❖ **Misión**

Formular, ejecutar y evaluar actividades de dirección y control de los planes, programas y proyectos de salud del ámbito municipal, en armonía con las políticas y disposiciones del orden departamental y nacional, que permitan garantizar la prestación de los servicios de salud a la comunidad del Municipio de Tumaco. Dirigir el sistema general de salud en el municipio, conforme a lo prescrito en las leyes 10 de 1990 y 715 de 2001.

❖ **Funciones**

1. Planear, dirigir, coordinar, supervisar, controlar y ajustar los procesos y actividades en materia de Salud del municipio, de acuerdo a los lineamientos trazados por el ministerio de Salud
2. Gestionar el recaudo, flujo y ejecución de los recursos con destinación específica para salud del municipio, y administrar los recursos del Fondo Local de Salud
3. Ejercer las funciones establecidas en el artículo 12 de la ley 10 de 1990 y la ley 715 de 2001
4. Gestionar y supervisar el acceso a la prestación de los servicios de salud para la población del Municipio
5. Impulsar mecanismos para la adecuada participación social y el ejercicio pleno de los deberes y derechos de los ciudadanos en materia de salud y de seguridad social en salud
6. Adoptar, administrar e implementar el sistema integral de información en salud, así como generar y reportar la información requerida por el Sistema
7. Adoptar, implementar y adaptar las políticas y planes en salud pública de conformidad con las disposiciones del orden nacional y departamental, así como formular, ejecutar y evaluar el plan de atención básica municipal.

8. Gestionar la financiación y cofinanciación de la afiliación al Régimen Subsidiado de la población pobre y vulnerable y verificar la ejecución eficiente de los recursos destinados a tal fin
9. Dirigir el Sistema Municipal de Salud y Seguridad Social
10. Realizar las acciones de fomento de la salud, prevención de la enfermedad, asegurar y financiar la prestación de los servicios de tratamiento y rehabilitación del nivel de atención de la salud de la comunidad
11. Coordinar las actividades de salud entre el municipio, el hospital local, Centro Hospital Divino Niño y demás I. P. S. que funcionen en la jurisdicción municipal
12. Supervisar y controlar el recaudo de los recursos locales que tienen destinación específica para salud y administrar el Fondo Local de Salud
13. Impulsar, implantar y garantizar los mecanismos necesarios para lograr la participación social y el ejercicio pleno de los deberes y derechos de los ciudadanos en materia de salud
14. Reportar la información que solicite la Nación y el departamento
15. Cumplir y hacer cumplir en la jurisdicción de Tumaco, las políticas y normas trazadas por el Ministerio de Protección Social, la Superintendencia de Salud y el Consejo Nacional de Seguridad Social en Salud, y apoyar en forma complementaria las acciones de salud a cargo del departamento
16. Cumplir y hacer cumplir en la jurisdicción de Tumaco, las políticas y normas trazadas por el Ministerio de Protección Social, la Superintendencia de Salud y el Consejo Nacional de Seguridad Social en Salud, y apoyar en forma complementaria las acciones de salud a cargo del departamento
17. Velar por el cumplimiento de las normas sobre seguridad industrial y salud ocupacional
18. Orientar y coordinar las acciones de todas las dependencias de la Secretaría
19. Llevar a efecto los contratos y convenios administrativos por delegación del Alcalde, necesarios para el funcionamiento de la Dirección
20. Adelantar campañas de nutrición y complementación alimentaría para los niños, ancianos y menesterosos en coordinación con el I. C. B. F.
21. Identificar a la población pobre y vulnerable del municipio y seleccionar a los beneficiarios del Régimen Subsidiado, atendiendo las disposiciones que regulan la materia
22. Realizar sondeos para establecer las necesidades guarderías y jardines infantiles
23. Adoptar, implementar y adaptar las políticas y planes en salud pública de conformidad con las disposiciones del orden nacional y departamental, así como formular, ejecutar y evaluar el plan de atención básica municipal
24. Adoptar, administrar e implementar el sistema integral de información en salud, así como generar y reportar la información requerida por el Sistema
25. Realizar las acciones de fomento de la salud, prevención de la enfermedad, asegurar y financiar la prestación de los servicios de tratamiento y rehabilitación del nivel de atención de la salud de la comunidad

26. Establecer la situación de salud en el municipio y propender por el mejoramiento de las condiciones determinantes de dicha situación. De igual forma, promover la coordinación, cooperación e integración funcional de los diferentes sectores para la formulación y ejecución de los planes, programas y proyectos en salud pública.
27. Ejercer el autocontrol en todas las funciones que le sean asignadas
28. Ejercer vigilancia y control sanitario sobre los factores de riesgo para la salud, en los establecimientos y espacios que puedan generar riesgos para la población, tales como establecimientos educativos, hospitales, cárceles, cuarteles, albergues, guarderías, ancianatos, puertos y transporte público, piscinas, estadios, coliseos, gimnasios, bares, tabernas, supermercados y similares, restaurantes, hoteles, moteles, casa de citas, droguerías, plazas de mercado, de abasto público y plantas de sacrificio de animales, entre otros
29. Ejercer control y seguimiento a la prestación de los servicios de agua potable, alcantarillado, soluciones de tratamiento de agua, aseo urbano y saneamiento básico urbano y rural
30. Velar por la implementación y mejoramiento continuo de los Sistemas de Control Interno y Gestión de la Calidad
31. Ejercer control y seguimiento a las políticas nacionales y departamentales del sistema de seguridad social en salud y relacionadas con la inspección, vigilancia y control de sanidad, se efectúen acorde a las disposiciones legales, estatutarias y reglamentarias vigentes

Descripción general del sistema de información Sivigila.

Su nombre completo es Sistema Nacional de Vigilancia en Salud Pública - SIVIGILA[16], que se ha creado para realizar la provisión en forma sistemática y oportuna, de información sobre la dinámica de los eventos que afecten o puedan afectar la salud de la población colombiana, con el fin de:

- Orientar las políticas y la planificación en salud pública
- Tomar las decisiones para la prevención y control de enfermedades y factores de riesgo en salud
- Optimizar el seguimiento y evaluación de las intervenciones

[16]SITIO OFICIAL SISTEMA NACIONAL DE VIGILANCIA EN SALUD PÚBLICA [en línea] <http://www.ins.gov.co/lineas-de-accion/Subdireccion-Vigilancia/sivigila/Paginas/sivigila.aspx> [citada en 19 de octubre de 2015]

- Racionalizar y optimizar los recursos disponibles y lograr la efectividad de las acciones en esta materia, propendiendo por la protección de la salud individual y colectiva.

El Sivigila tiene como objetivo disponer de una guía práctica y sencilla para que todos los funcionarios responsables de los procedimientos involucrados en el subsistema de información en salud pública estén en capacidad de operar el software Sivigila escritorio, versión 2015, diseñado para facilitar el procesamiento, reporte y análisis de los datos generados por las fichas de notificación de los casos de eventos objeto de vigilancia y control en salud pública.
Está dirigido a todos los actores del territorio nacional, encargados de la gestión y operación del sistema de vigilancia y control en salud pública, desde el ámbito local: prestadores de servicios de salud (Unidades primarias generadoras de datos), Unidades notificadoras municipales, distritales y departamentales, y las entidades de carácter nacional.

Actores

Figura 2. Actores del Sivigila

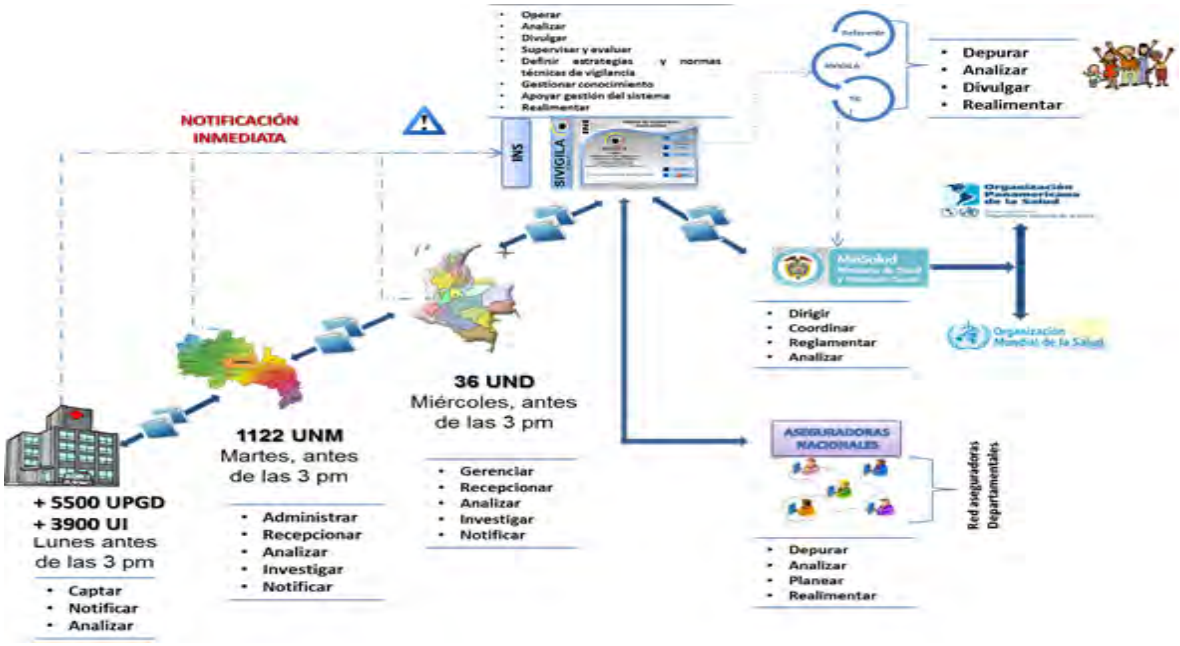
Fuente: Manual Sivigila 2015.

Flujo de información en el Sivigila.

En el siguiente esquema se muestra el flujo de información entre los actores del sistema de vigilancia en salud pública, que asciende desde el ámbito local hacia el ámbito nacional.

Esta característica en el flujo de información, hace que cada uno de los actores tenga definidas funciones particulares en el sistema de vigilancia en salud pública Nacional y en relación con el uso de los datos y la operación del aplicativo.

Figura 3. Flujo de Información en el Sivigila



Fuente: Manual Sivigila

Tipos de Rol en el Sivigila

En el Sivigila cada actor tiene asociadas actividades particulares.

Tabla 1. Rol de actores en el Sivigila

Actividad	UI	UPGD	UNM	UND*	UN**
Instalar actualizar Sivigila	X	X	x	x	X
Configurar Sivigila	X	X	X	X	
Migrar información de años anteriores	X	X			X
Caracterizar UPGD	X	X	X	X	
Digitar información	X	X			

Notificar	X	X	X	X	X
Consolidar			X	X	X
Realizar ajustes	X	X			
Generar reportes	X	X	X	X	X
Retroalimentar			X	X	X

Fuente: Manual Sivigila.

Unidades notificadoras del Sivigila.

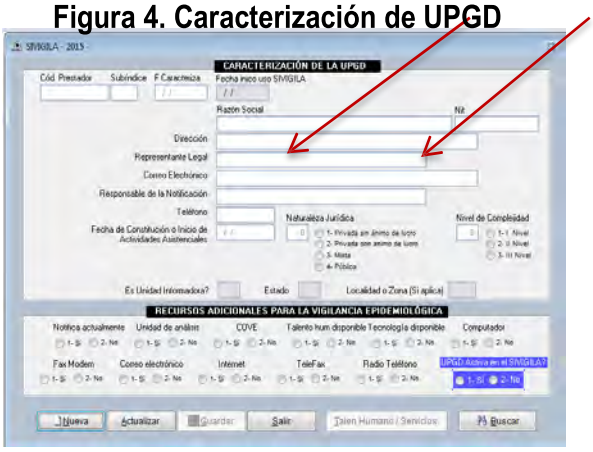
Para el procesamiento en el sistema de información Sivigila se tienen establecidos unos roles y unas responsabilidades ya antes mencionados a continuación se describe quienes son cada una de las unidades.

- **Unidad notificadora:** es la entidad pública responsable de la investigación, confirmación y configuración de los eventos de interés en salud pública, con base en la información suministrada por las Unidades Primarias Generadoras de Datos y cualquier otra información obtenida a través de procedimientos epidemiológicos. En este grupo se tiene:
- **UND:** unidad notificadora departamental. Esta consolidad la información de todo el departamento y reporta la unidad nacional.
- **UNM:** unidad notificadora municipal .consolida la información del municipio y la reportan a la unidad departamental.
- **Unidad primaria generadora de datos – UPGD:** es la entidad pública o privada que capta la ocurrencia de eventos de interés en salud pública y genera información útil y necesaria para los fines del Sistema de Vigilancia en Salud Pública, Sivigila.
- Cuando las unidades informadoras y las UPGD no cuenten con la capacidad instalada suficiente, la unidad Notificadora deberá asumir por complementariedad las funciones que no puedan ser cubiertas por las UPGD.
- **UN:** es la unidad nacional quien recibe la información de los eventos de salud ya consolidados de todo el país.

Condiciones Generales del Software Sivigila

Este software cuenta con ventanas o formularios de captura, que presentan unas casillas o espacios que tiene cada variable para la digitación de valores (números) o texto.

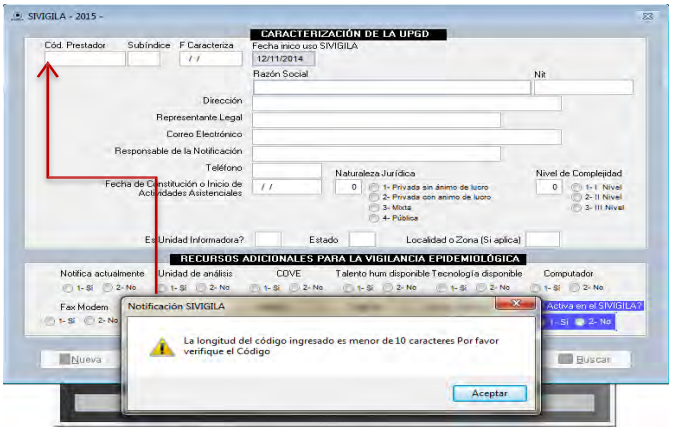
Figura 4. Caracterización de UPGD



Fuente: Software Sivigila

Al ser digitado un valor o texto en cada una de estas casillas, se ejecuta una regla de validación que sólo permite digitar ciertos datos, si se digitó adecuadamente en el espacio de cada variable se continúa con la siguiente, de lo contrario se impide continuar con la digitación, hasta ingresar lo permitido. Cuando el dato digitado en la casilla se valida como error, aparecerá un aviso de advertencia y dicho dato estará sombreado para reingresarlo nuevamente, no hay necesidad de borrar el dato y digitarlo, si es un campo de un sólo carácter de captura, este no aparecerá sombreado, y de esta manera se reingresa sin borrarlo.

Figura 5. Caracterización UPGD 1



Fuente: Software Sivigila

Cada variable tiene unos valores o rangos de datos permitidos, estos se presentan como ayuda al Digitador en:

- La barra de estado que se encuentra ubicada en la parte inferior de cada ventana o formulario, cada vez que el cursor se ubica en una variable. Una cajita de fondo amarillo y texto negro que se presenta al ubicar el puntero del mouse en la variable, donde además se encuentra la descripción del dato que captura la variable

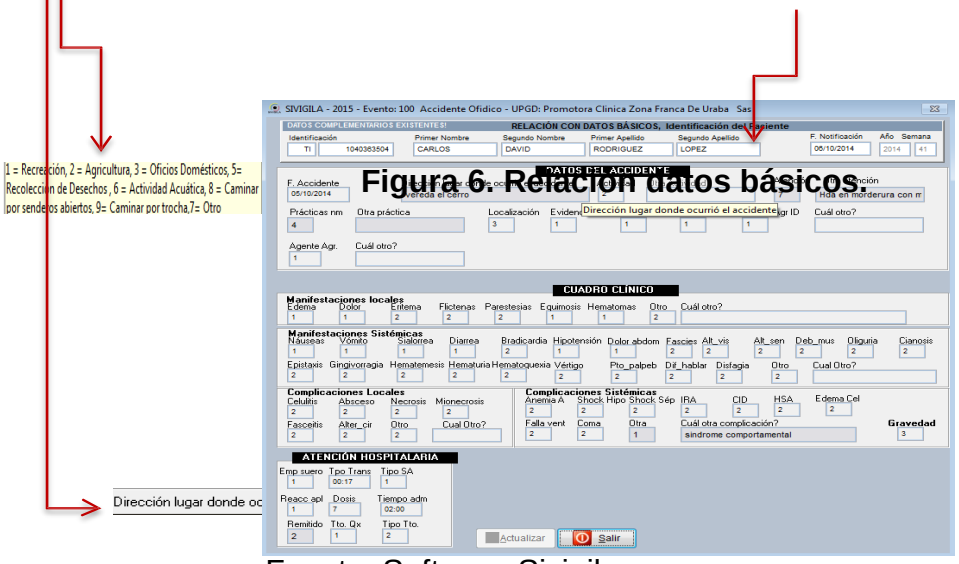


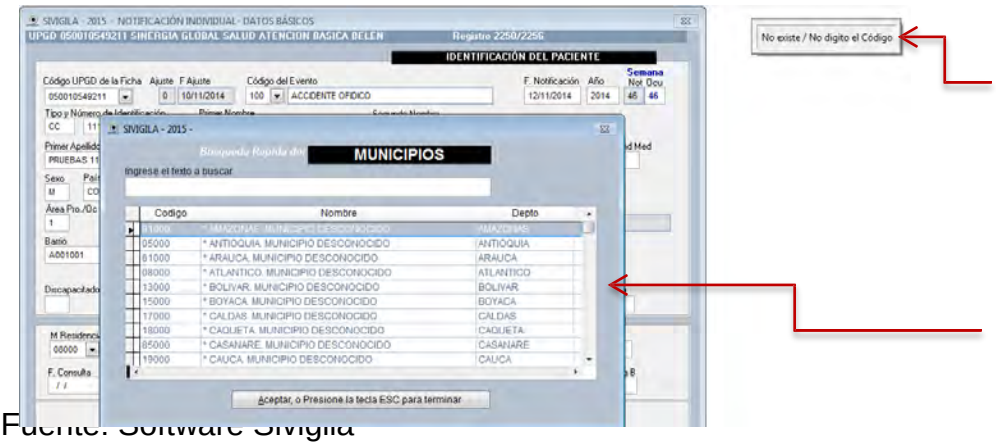
Figura 6. Relación datos básicos

Fuente: Software Sivigila

Existen variables que ameritan búsquedas de varios o muchos criterios, estas variables cuentan con una tabla que se despliega al presionar la tecla Enter, permitiendo realizar búsqueda y seleccionar del listado de opciones posibles haciendo Clic sobre una de ellas para seleccionarla y posteriormente en el botón aceptar para pasar el dato a la casilla en el formulario.

El sistema cuenta con unas tablas de uso general, que se encuentran en variables como municipios, ocupaciones, aseguradoras, etc. Cuando en algún formulario se solicite el ingreso de uno de estos códigos y al ingresarlo éste no corresponda con ninguno de los valores precargados en la tabla de referencia, se presentará un mensaje informando que el código ingresado no se encuentra, a su vez aparece un aviso que le pregunta si desea consultar en la tabla, al hacer clic en Sí se presenta la pantalla de búsqueda.

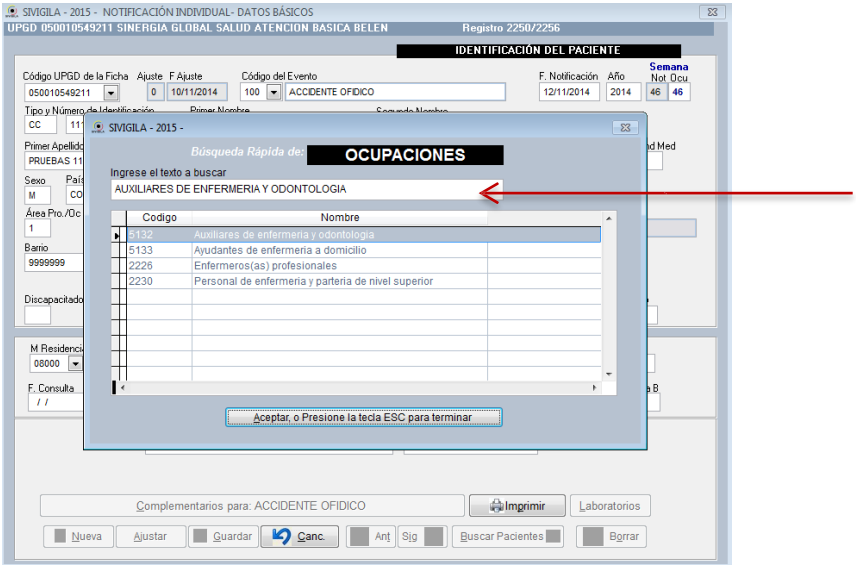
Figura 7. Descripción municipios



Fuente: Software Sivigila

Digite un fragmento del texto en la casilla en blanco que aparece en la parte superior del formulario y presione la tecla entre para ver el resultado de la búsqueda que se presentará en la tabla, al realizar esta acción, aparecerá sombreado el nombre ingresado y otras opciones que presentan similitud en la búsqueda. Una vez verifique que se trata del mismo texto buscado, presione la tecla enter o esc o el botón que se encuentra en la parte inferior de la tabla de búsqueda.

Figura 8. Descripción ocupación



Fuente: Software Sivigila

Requerimientos Del Sistema Aplicativo Sivigila 2015

Para que el programa funcione adecuadamente se requieren los siguientes elementos mínimos:

Computador: Procesador: 1 GHz o superior Memoria RAM: 512 MB o superior
Disco Duro: 1GB libre de espacio en disco.
Sistema operativo: Windows 2000, XP, Vista, 7, 8, 8.1.
Video con resolución mínima de 1024*768 píxeles a 512 colores.

3.2 INVENTARIOS DE RECURSOS SECRETARIA DE SALUD ALCALDÍA DE TUMACO

3.2.1 ACTIVOS INFORMÁTICOS USADOS EN EL PROCESAMIENTO DE INFORMACION DEL SIVIGILA EN LA ALCALDIA DE TUMACO.

Los activos son los recursos necesarios para que la recepción de información en el Sivigila o relacionados con este, alcance los objetivos propuestos. Estos activos pueden ser: recurso humano, recurso tecnológico, recursos físicos, información. A continuación se describe la lista de activos tecnológicos y de software que permiten el procesamiento de información en el Sivigila.

Actualmente se consideran activos los correspondientes al servicio del Sivigila a todos los equipos donde se encuentra instalada la aplicación de escritorio del sistema de información, además de la descripción del sistema operativo de los equipos los programas que se encuentran instalados, las ups y sus detalles, a continuación se describen estos activos en las siguiente tabla.

Tabla 2. Activos relacionados al Sivigila.

Activo	Valoración	Observación
Copias de seguridad	5	Son de suma importancia no solo por tener un segundo plan en caso de pérdida de la información primaria, sino porque en caso de perdida y caer en manos equivocadas se tendría información extraviada de suma importancia porque al divulgarse de forma mal intencionada podría causar daños irreversibles en la comunidad de Tumaco
Equipos de computo	5	Si no se tienen equipos de cómputos donde se pueda instalar el sistema de información, no será posible el procesamiento de los datos por parte de los usuarios del Sivigila.
Fluido eléctrico	5	Sin energía no es posible acceder al sistema.
Ups	4	En el caso de no haber fluido eléctrico, estas permiten que los equipos donde se esté haciendo la recepción de la información del Sivigila no se dañen y así no sufrir situaciones que lamentar por el mal manejo del equipo.

Internet	3	Es importante para el proceso de reporte de las unidades, pero si el temporalmente las unidades notificadoras del Sivigila pueden trabajar en el sistema.
Programas	3	Ayudan de cierta forma para tener facilidad en el momento de generar reportes, cuando se comprime la información, se descarga en formato plano y se permite la manipulación de las tablas, pero los usuarios del Sivigila estando en el sistema son capaces de trabaja sin utilizarlos hasta que puedan necesitarlos.
Sistemas operativos	5	Un equipo sin software no funciona, entonces no será posible el proceso de reportes ni de recolección de información en el Sivigila.

4 PLAN DE AUDITORIA

Constituye la guía para la ejecución de las actividades para la auditoria a desarrollar, por el responsable que lleve realice la elaboración, ejecución, evaluación y seguimiento significativos que se realicen durante el ejercicio ue deberán ser conocidas y aprobadas por el comité que este encargado de su revisión posterior.

Objetivo del plan de auditoria

Verificar el cumplimento de los procesos de seguridad de la información según la ISO/IEC 27001 en el sistema de información Sivigila de la secretaria de salud alcaldía de San Andrés de Tumaco.

Alcance del plan

El presente plan tiene como propósito revisar cada uno de los pasos a seguir en los procesos de seguridad en la recesión de información en el sistema Sivigila y su entorno, de esta manera verificar la eficiencia y eficacia en el desarrollo de cada tarea relacionada con la seguridad.

Justificación

La alcaldía de San Andrés de Tumaco es el lugar donde nunca antes se ha hecho un auditora de ningún tipo y por lo tanto no se tienen bases para dar inicio a un proceso similar con mayor rapidez, además se debe tener en cuenta que en la actualidad la información es un activo importante que en toda entidad es necesario tener lineamientos y normas que conduzcan a su cuidado.

Teniendo en cuenta lo antes dicho para desarrollar de forma correcta un proceso de evaluación y revisión como lo es una auditoria se debe trazar un plan que le diga al responsable que hacer, cuando y como, que le permita seguir un orden y culminar de forma satisfactoria su proceso y tener resultados rápidos y veraces, por tal razón un plan de auditoria se contempla en todo actividad de este tipo que servirá a la larga como guía para un trabajo bien hecho y que deje buenas recomendaciones para la entidad donde se lleve a cabo.

Metodología

La herramienta de apoyo que se utilizó durante el desarrollo de este proyecto es la NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Esta norma ha sido

elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de información. Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas.

Para realizar el proceso de evaluación se cuenta con fuentes para la recolección de datos las cuales se han clasificado como primarias y secundarias.

- Primarias
    - El administrador de SIVIGILA la señora Yamileth Ramos quien tiene el conocimiento del manejo del sistema de información, además de ser la que tiene los manuales de procesos y manejos del sistema.
    - El ingeniero Javier Mindineros Satizabal quien posee conocimiento del sistema de información y del personal que permitirán llevar a cabo las actividades de la auditoria.
    - Todo el personal de la secretaria de salud, los cuales serán de gran ayuda para todo el proceso de recolección de información porque son ellos quienes al final tienen una visión a nivel de experiencia del manejo del sistema.

- Secundarias

    - Internet
    - Libros de investigación.
    - Documentos de auditorías que ya se han realizado en la universidad.

- Es necesario mencionar que se desarrolló:

    - Entrevistas a directivos de las áreas involucradas en el proceso de evaluación, con la finalidad de obtener información detallada que ayudo enriquecer el trabajo de evaluación.
    - Observación directa, porque fue preciso tener una visión más cercana con todo el personal que interviene en estas dependencias.
    - Listas de chequeo que dieron un punto de vista neutro de los procesos de las áreas antes mencionadas y además de las diferentes investigaciones que se puedan llevar acabo para mostrar un trabajo completo.

❖ Para el análisis de datos se tuvo en cuenta:

- Tabulación
- Representación gráfica de los resultados.

❖ Las herramientas que se tuvieron en cuenta fueron:

- Backup y copias espejos de discos duros y medios removibles.
- Software de Recuperación de archivos borrados.
- Análisis de la Actividad del equipo.

Recursos humanos

El proyecto fue desarrollado por la estudiante Yurani Alejandra Landázuri Guevara bajo la dirección del Ingeniero José Javier Villalba Romero y la colaboración del personal de la Secretaria de Salud de la Alcaldía.

Tabla 3. Recursos humanos

Participante	Yurani Alejandra Landázuri Guevara
Organización	Universidad de Nariño
Rol	Auditora

Participante	José Javier Villalba Romero
Organización	Universidad de Nariño
Rol	Asesor

Participante	Javier Mindinero Satizabal
Organización	Alcaldía de Tumaco
Rol	Ingeniero de Sistemas
Es cliente	Si

Participante	Personal De Administración y Presupuesto
Organización	Alcaldía de Tumaco
Rol	Usuario del SI
Es usuario	Si

Recursos tecnológicos

Hardware

Tabla 4. Recursos tecnológicos

Descripción	Cantidad
Portátil HP Intel Core i3, memoria RAM 4GB, disco duro 500MB	**1**

Software

Descripción	Cantidad
Paquete ofimática	**1**
Herramienta de Modelado UML	**----------**
Herramientas de testing	**1**

Recursos materiales

Descripción	Cantidad
Fotocopias, resmas de papel	**----------**
USB	**2**
CD	**5**

Pasos en la ejecución de la auditoria

Según lo mencionado la metodología del trabajo fue divida en las siguientes etapas.

❖ **Primera etapa**: **conocimiento**

- Identificar el sistema a auditar.
- Determinar finalidad y límite de la auditoria.
- Identificar los activos informáticos
- Identificar los procesos de manejo de información
- Identificar los usuarios del sistema

❖ **Segunda etapa: planificar.**

Durante esta etapa se estableció los procedimientos para desarrollar la evaluación del SI SIVIGILA de la alcaldía.

- Diseñar el plan de pruebas.
- Determinar herramientas a realizar durante el proceso de auditoría.
- Realizar la investigación pertinente referente a la seguridad del SI SIVIGILA
- Crear plan de trabajo.

❖ **Tercera etapa: hacer**

Esta etapa comprendió el desarrollo de la auditoria.

- Realizar entrevista al personal de secretaria de salud de la alcaldía.
- Aplicar instrumentos diseñados anteriormente para la recolección de la información.
- Realizar análisis de riesgo.
- Ejecutar pruebas a la aplicación de escritorio del sistema SIVIGILA.
- Determinar la existencia de controles ISO/IEC 27002.

❖ **Cuarta etapa: presentación del informe final.**

- Elaborar informe final.

Durante esta etapa se presentó el informe final con las respectivas observaciones y recomendaciones.

5 DISEÑO DE INSTRUMENTOS DE RECOLECCIÓN DE EVIDENCIAS

Se describe a continuación el diseño de los instrumentos de recolección de evidencias donde se contempló en la lista de chequeo el cumplimiento de los controles de la norma ISO 27001 que se consideraron necesario para este trabajo; la observación directa se hizo con la finalidad de conocer el campo donde se trabaja con el sistema de información, establecer acercamiento con los usuarios, funcionarios de las oficinas y conocer funcionamiento de la entidad, la secretaria de salud y del mismo sistema Sivigila, la entrevista se realizó a dos funcionarios claves para este procedimiento de evaluación a la señora Yamileth Ramos que es la UNM (Unidad Notificadora Municipal) del Sivigila y la Jefe de Epidemiologia de la Secretaria de Salud a ella porque es la encargada de asignar códigos a las UPGD (Unidades Primarias Generadoras de Datos) del Sivigila quienes únicamente con el permiso de la UNM en este caso Yamileth Ramos pueden ser usuarias del sistema de información y hacer los reportes de la EPS correspondiente, también porque es la única que tiene información de cómo se hacen los manejos con el sistemas ya que los demás usuarios solo saben generar y recibir reportes y la ultima y no menos importante razón es porque a las UPGD no se le permitió a la auditora acceder para mirar cómo estas tratan al sistema y la información que este genera, la señora Yamileth Ramos en conclusión maneja toda los datos del Sivigila y a ella le llega todos los reportes del municipio. El otro funcionario es el señor Javier Mininderos el Coordinador de Sistemas a él porque es quien hizo la configuración y acompañamiento inicial para la instalación del Sivigila y como jefe de sistemas de la entidad se intuyó que podría manejar información sobre el funcionamiento de la seguridad de la información de la alcaldía de Tumaco y servir de guía para el desarrollo de la auditoria. (Ver Anexos 1, 2, 3)

6 EVIDENCIAS Y HALLAZGOS DEL PROCESOS DE AUDITORIA

6.1 IDENTIFICACIÓN DE CONTROLES Y OBJETIVOS DE CONTROL SEGÚN ISO-IEC/27001

Esta norma en busca de mejorar la seguridad y tratamiento de información en las entidades públicas y privadas ha divido el análisis por procesos y cada uno de estos con sus respectivos controles y objetivos. Una vez en el contexto del sistema Sivigila de la alcaldía de Tumaco, se puede observar altos niveles de fallas en el cumplimiento de estos controles, por esta razón a continuación se describe el listado de controles que en la alcaldía de Tumaco se deben implementar en busca de la seguridad del sistema auditado, lo ideal sería que estos se asumieran para toda la entidad pero ya es decisión de las administración la decisión que puedan tomar. (Ver Anexo 4).

La ISO/IEC 27001 está dividida en objetivos de control que a su vez están enumerados como se muestra en el (Anexo 4), estos se han obtenido directamente de los de la NTC-ISO/IEC, con numerales 5 a 15, y están alineados con ellos. Las listas de estas tablas no son exhaustivas, y para el presente trabajo se consideró que controles se necesitan y objetivos de control y controles adicionales. La norma NTC- ISO/IEC, numerales 5 a 15, proporciona asesoría y orientación sobre las mejores prácticas de apoyo a los controles especificados en el literal A.5 a A.15, mostrados en el anexo ya mencionado.

VALORACIÓN DE LOS ACTIVOS

Una vez identificados los activos que están relacionados con el Sivigila es necesario valorar el nivel de importancia que tienen estos en el procesamiento de la información, para ello se debe definir las dimensiones o criterios bajo los cuales se van a evaluar. En la tabla 5 se describe la valoración cualitativa de los activos asociados al Sivigila.

La escala de valoración se ha definido de la siguiente manera:

- 1: Muy bajo (MB).
- 2: Bajo (B)
- 3: Medio (M)
- 4: Alto (A)
- 5: Muy alto (MA)

Tabla 5. Activos relacionados al Sivigila

Activo	Valoración	Observación
Copias de seguridad	5	Son de suma importancia no solo por tener un segundo plan en caso de pérdida de la información primaria, sino porque en caso de perdida y caer en manos equivocadas se tendría información extraviada de suma importancia porque al divulgarse de forma mal intencionada podría causar daños irreversibles en la comunidad de Tumaco
Equipos de computo	5	Si no se tienen equipos de cómputos donde se pueda instalar el sistema de información, no será posible el procesamiento de los datos por parte de los usuarios del Sivigila.
Fluido eléctrico	5	Sin energía no es posible acceder al sistema.
Ups	4	En el caso de no haber fluido eléctrico, estas permiten que los equipos donde se esté haciendo la recepción de la información del Sivigila no se dañen y así no sufrir situaciones que lamentar por el mal manejo del equipo.
Internet	3	Es importante para el proceso de reporte de las unidades, pero si el temporalmente las unidades notificadoras del Sivigila pueden trabajar en el sistema.
Programas	3	Ayudan de cierta forma para tener facilidad en el momento de generar reportes, cuando se comprime la información, se descarga en formato plano y se permite la manipulación de las tablas, pero los usuarios del Sivigila estando en el sistema son capaces de trabaja sin utilizarlos hasta que puedan necesitarlos.
Sistemas operativos	5	Un equipo sin software no funciona, entonces no será posible el proceso de reportes ni de recolección de información en el Sivigila.

IDENTIFICACIÓN DE AMENAZAS ASOCIADAS A LOS ACTIVOS.

Ya detectados los activos importantes relacionados con el Sivigila se da inicio con la identificación de las posibles amenazas a los que estos están expuesto, teniendo como referencia el análisis de los controles según la norma ISO/IEC 27001 . Según lo antes dicho se describen en las siguientes tablas.

Tabla 6. Amenazas naturales.

ACTIVO	AMENAZA			
	Fuego	Daños por agua	Desastres humanos	Desastres naturales
Copias de seguridad	**X**	**X**	**X**	**X**
Equipo de computo	**X**	**X**	**X**	**X**
Fluido eléctrico	**X**	**X**	**X**	**X**
Internet	**X**			**X**
Programas				
Sistemas operativos				

Esta tabla (Tabla 6), muestra a qué tipo de amenazas naturales están expuestos los activos relacionados con el Sivigila, esta clasificación permite que tipo de amenazas incidan más para los activos.

Tabla 7. Amenazas de origen industrial

ACTIVO	AMENAZA				
	Derrumbes	Contaminación mecánica	Avería de origen físico o lógico	Corte suministro eléctrico	Condiciones de humedad
Copias de seguridad	**X**		**X**		
Equipo de computo	**X**	**X**	**X**	**X**	**X**
Fluido eléctrico				**X**	**X**
Internet				**X**	
Programas			**X**		
Sistemas operativos				**X**	

La tabla anterior (tabla 7) refiere las amenazas de origen industrial a las que están expuestos los activos del sistema Sivigila y a su vez muestra cuales son esos activos que se encuentran más en peligro siendo de todos ellos los equipos de cómputo que se encuentran más vulnerables ante estas amenazas.

Tabla 8. Amenazas Y Fallos No Intencionados.

ACTIVO	AMENAZA								
	Error de usuarios	Error de administrador	Error de configuración	Deficiencia de organización	Difusión sw maligno	Divulgación de información	Escape de información	Introducción de información	Indisponibilidad del personal
Copias de seguridad	**X**	**X**		**X**	**X**	**X**	**X**		
Equipo de computo	**X**	**X**	**X**	**X**	**X**				
Fluido eléctrico									
Internet									
Programas					**X**				
Sistemas operativos					**X**				

La tabla 8, refiere aquellas amenazas causadas por fallos no intencionados a los que los activos relacionados a la Sivigila están expuestos siendo estas amenazas las que los usuarios causan sin querer, siendo según lo que se refleja las copias de seguridad las que están más vulnerables ante este tipo de situaciones.

Tabla 9. Amenazas De Ataques Intencionados.

ACTIVO	AMENAZA								
	Suplantación de identidad	Uso no previsto	Acceso no autorizado	Repudio	Modificación de la información	Introducción falsa de información	Destrucción de información	Divulgación de información	Robo
Copias de seguridad		X	X	X	X		X	X	X
Equipo de computo		X	X	X	X	X	X	X	X
Fluido eléctrico		X							X
Internet		X							
Programas	X	X							
Sistemas operativos					X				X

La tabla 9, hace mención a los ataques intencionados que causan los usuarios al sistema de información Sivigila, siendo estos de gran daño porque son los funcionarios conscientes de que lo están haciendo y que de alguna forma afectan al sistema, siendo el equipo de cómputo y las copias de seguridad los activos que están más expuestos a este tipo de ataque.

IDENTIFICACIÓN Y VALORACIÓN DE LAS VULNERABILIDADES

Una vulnerabilidad se define en este método de Gestión del Riesgo, como un estado de debilidad o incapacidad para resistir un fenómeno amenazante y que al ser explotado afecta el estado de los activos del proyecto, dicho en otras palabras es la potencialidad o 'cercanía' previsible de la materialización de la Amenaza en Agresión.

Al igual que los activos las vulnerabilidades deben valorarse y priorizarse, pero antes deben describirse claramente y evaluarla tomando como criterios la frecuencia de ocurrencia. A continuación se describen la valoración de las vulnerabilidades asociada a los activos que se han contemplado en relación con el Sivigila.

Para efectos del siguiente análisis se ha tomado el valor cualitativo de las vulnerabilidades la cual se describe en la siguiente tabla.

Tabla 10. Valor cualitativo de vulnerabilidades

Valor	**Description**	**Probabilidad de Ocurrencia**
Muy Frecuente **(MF)**	A diario	75-100%
Frecuente **(F)**	Una vez al mes	50% -75%
Frecuencia Normal **(FN)**	Una vez al año	25% -50%
Poco Frecuente **(PF)**	Cada varios Años	0-25%

La siguiente tabla 10, muestra la ocurrencia de las vulnerabilidades respecto a los activos asociados al Sivigila, las casillas en blanco quieren decir que no se consideró relación entro los ítems analizados.

Tabla 11. Valoración de vulnerabilidad

AMENAZA	ACTIVO					
	Copias de seguridad	Equipo de computo	Fluido eléctrico	Internet	Programas	Sistemas operativos
Fuego	**PF**	**PF**	**PF**	**PF**	**PF**	**PF**
Daños por agua	**PF**	**PF**	**FN**	**PF**	**PF**	**PF**
Desastres humanos	**F**	**F**	**PF**	**PF**	**F**	**F**
Desastres naturales	**PF**	**PF**	**PF**	**PF**	**PF**	**PF**
Derrumbes	**PF**	**PF**	**PF**	**PF**	**PF**	**PF**
Contaminación mecánica		**MF**	**MF**	**F**		
Avería de origen físico o lógico	**F**	**F**	**F**	**F**	**F**	**F**
Corte suministro eléctrico	**F**	**F**	**F**	**F**	**F**	**F**
Condiciones de humedad		**FN**	**FN**			
Error de usuarios	**FN**	**FN**	**FN**	**FN**	**FN**	**FN**
Error de administrador	**PF**	**PF**	**PF**	**PF**	**PF**	**PF**
Error de configuración	**PF**	**PF**	**F**	**PF**	**F**	**F**
Deficiencia de organización	**FN**	**F**	**FN**	**FN**	**FN**	**FN**
Difusión sw maligno	**FN**	**F**		**F**	**F**	**F**
Divulgación de información	**FN**	**F**			**FN**	**FN**
Escape de información	**FN**	**F**		**FN**	**FN**	**FN**
Introducción de información	**FN**	**F**		**FN**	**FN**	**FN**
Indisponibilidad del personal	**PF**	**F**	**FN**	**FN**	**F**	**F**
Suplantación de identidad	**PF**	**PF**				**PF**
Uso no previsto	**FN**	**FN**	**FN**	**MF**	**MF**	**MF**
Acceso no autorizado	**PF**	**FN**	**PF**	**MF**	**F**	**F**
Repudio	**FN**	**FN**	**F**	**FN**	**FN**	**FN**
Modificación de la información	**FN**	**FN**		**FN**	**MF**	**MF**
Destrucción de información	**FN**	**FN**		**FN**	**FN**	**FN**
Divulgación de información	**FN**	**FN**		**FN**	**FN**	**FN**
Robo	**FN**	**F**	**PF**	**MF**	**F**	**F**

La Tabla 11, demuestra la frecuencia de las amenazas a las que están expuestos los activos relacionados con el sistema Sivigila, reflejando que la incidencia de frecuencia es alta para desastres humanos, averíos de origen físico y lógico, suministro de energía y uso no previsto, sin dejar de lados otros como divulgación de información, robo, modificación de la información y repudio dejando al sistema vulnerable en partes importantes para poder decir que se tiene segura la información o al menos que se están identificando controles para ello.

IDENTIFICACIÓN Y VALORIZACIÓN DE IMPACTOS

Un impacto es el daño que causa o puede causar sobre el activo derivado de la materialización de una amenaza.

La tipificación de los impactos puede variar de acuerdo al trabajo. Para efectos de esta del presente se evalúan los impactos de acuerdo al tipo de perdida técnica.

La siguiente tabla (Tabla 12), muestra el rango que se ha tomado para el análisis del presente trabajo.

Tabla 12. Valoración cualitativa de impacto

5	Muy alto **(MA)**	Daño muy grave para el sistema
4	Alto **(A)**	Daño grave al sistema
3	Medio **(M)**	Daño importante al sistema
2	Bajo **(B)**	Daño menor al sistema
1	Muy Bajo **(MB)**	Daño despreciable

La siguiente tabla (Tabla 13) muestra el impacto de las vulnerabilidades respecto a los activos asociados al Sivigila, las casillas en blanco quieren decir que no se consideró relación entro los ítems analizados o que se consideran redundantes ya que pueden estar explícitamente incluidos en otro análisis.

Tabla 13. Impacto de vulnerabilidades

AMENAZA	ACTIVO					
	Copias de seguridad	Equipo de computo	Fluido eléctrico	Internet	Programas	Sistemas operativos
Fuego	**MA**	**MA**	**MA**	**B**	**MA**	**MA**
Daños por agua	**MA**	**MA**	**MA**	**B**	**A**	**A**
Desastres humanos	**A**	**A**	**A**	**B**	**A**	**A**
Desastres naturales	**MA**	**MA**	**MA**	**MA**	**MA**	**MA**
Derrumbes	**A**	**MA**	**MA**	**MA**	**A**	**A**
Contaminación mecánica		**M**	**M**	**M**		
Avería de origen físico o lógico	**MA**	**MA**	**MA**	**M**	**A**	**MA**
Corte suministro eléctrico	**M**	**M**	**M**	**B**	**M**	**M**
Condiciones de humedad	**A**	**A**	**A**	**B**		
Error de usuarios	**A**	**MA**	**A**	**B**	**M**	**MA**
Error de administrador	**MA**	**MA**	**A**	**B**	**MA**	**MA**
Error de configuración	**A**	**MA**	**MA**	**M**	**M**	**MA**
Deficiencia de organización	**MA**	**MA**	**MA**	**M**	**M**	**MA**
Difusión sw maligno	**MA**	**MA**	**A**	**A**	**A**	**MA**
Divulgación de información	**MA**	**MA**		**A**	**A**	**MA**
Escape de información	**MA**	**MA**		**A**	**A**	**A**
Introducción de información	**MA**	**MA**				**M**
Indisponibilidad del personal		**A**		**M**		**A**
Suplantación de identidad		**MA**		**A**		**A**
Uso no previsto	**A**	**M**	**M**	**M**	**M**	**M**
Acceso no autorizado	**MA**	**MA**		**A**		**MA**
Repudio	**A**	**A**	**A**	**B**	**B**	**A**
Modificación de la información	**MA**	**MA**			**B**	**A**
Destrucción de información	**MA**	**MA**		**B**	**A**	**A**
Divulgación de información	**MA**	**MA**		**B**	**B**	**B**
Robo	**MA**	**MA**	**A**	**B**	**A**	**MA**

La tabla, demuestra el impacto que tiene las vulnerabilidades al sistema dejando así al mismo débil en caso de ocurrir alguno de ellos, se muestra que los desastres naturales, las fallas de la organización, los daños causados por agua y el fuego serian de gran impacto de forma negativa para el Sivigila, y que además estos dejarían en muy mal estado la información que se maneja el sistema en caso de ocurrir.

6.1.1 ESTIMACIÓN DEL RIESGO

El valor de la Vulnerabilidad y su Impacto sobre el Activo determinan conjuntamente el valor del Riesgo.

Esto se puede ver con facilidad cuando se representa el riesgo con una sencilla técnica matricial. En esta técnica se relacionan los niveles de Vulnerabilidad (puestos en filas) y los de Impacto (puestos en columnas). En las casillas correspondientes, los valores del nivel de Riesgo, como es lógico, son crecientes con los niveles de ambos factores, pero serán sistemáticamente mayores por debajo de la diagonal, pues se considera que el Impacto influye más en el nivel de Riesgo que la Vulnerabilidad.

En el trabajo que se está desarrollando se ha cruzado la tabla de identificación y valoración de las vulnerabilidades (puestos en filas) y la tabla identificación Y valorización de impactos (puestos en columnas) y se analizó mediante la siguiente combinación, descrita en la tabla que se muestra.

Tabla 14. Valor cualitativo de impactos

RIESGO		**VULNERABILIDAD**			
		PF	FN	F	MF
IMPACTO	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Donde el valor cualitativo es el siguiente:

Clase	Valoración Cualitativa
Crítico	Muy Alto
Grave	Alto
Moderado	Medio

Fuente: Esta investigación

Tabla 15. Valoración de impactos

AMENAZA	ACTIVO					
	Copias de seguridad	Equipo de computo	Fluido eléctrico	Internet	Programas	Sistemas operativos
Fuego						
Daños por agua						
Desastres humanos						
Desastres naturales						
Derrumbes						
Contaminación mecánica						
Avería de origen físico o lógico						
Corte suministro eléctrico						
Condiciones de humedad						
Error de usuarios						
Error de administrador						
Error de configuración						
Deficiencia de organización						
Difusión sw maligno						
Divulgación de información						
Escape de información						
Introducción de información						
Indisponibilidad del personal						

Suplantación de identidad						
Uso no previsto						
Acceso no autorizado						
Repudio						
Modificación de la información						
Destrucción de información						
Divulgación de información						
Robo						

Según la tabla Estimación del Riesgo los activos relacionados directamente con el sistema de información Sivigila están sujetos a riesgos muy altos, a partir de la información anterior la administración deberá tomar decisiones que vallan en pro de solucionar o bajar la intensidad de estos. Evitar los riesgos siempre es lo primero que se considera, pero esto se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

Si el riesgo ya es tan real como las consecuencias que este desata lo mejor es pensar en reducirlo al nivel más bajo posible, siendo esta la decisión más económica para la entidad, antes de que los daños sean irreversibles.

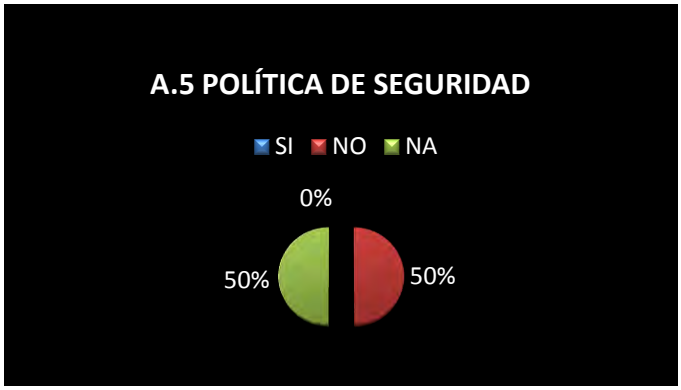
Pero sin duda lo que debe de hacer la entidad frente a una situación como esta es asumir los riesgos, ya que el Sivigila es uno de los sistemas que maneja información sensible del municipio y de le integridad y confiabilidad de esta depende la tranquilidad en aspecto de salud de toda una comunidad.

7 ANÁLISIS GRAFICO DE LOS HALLAZGOS DEL PROCESO DE AUDITORIA

El siguiente análisis gráfico es el resultado de la información obtenida de las herramientas de recolección de datos hechas al sistema Sivigila el cual procesa todos los datos epidemiológicos de la secretaria de salud de la alcaldía de Tumaco. Las herramientas utilizadas para el desarrollo de este proceso de auditoria fueron lista de chequeo, observación directa y entrevista.

A las listas de chequeo se le dio una valoración numérica de 1 si hay cumplimento y de 0 si no lo hay con la intensión de poder generar la tabulación y obtener información gráfica sobre el estado de la situación de seguridad de la información del sistema auditado, además para lograr separar situaciones que solo gráficamente pueden dar una conclusión clara y sin muchos rodeos.

Figura 9. A.5 Política de seguridad

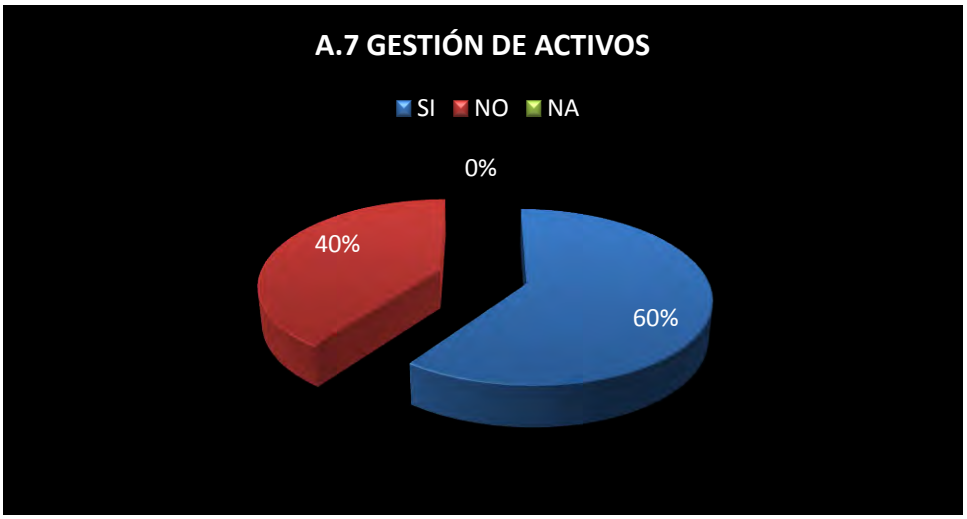


La gráfica 9, muestra un porcentaje de 50% para No cumple y 50% para No aplica esto quiere decir que no existen políticas de seguridad de la información en la entidad y por lo tanto como no están ni siquiera propuestas no hay que hacerle revisión ni seguimiento.

Figura 10. A.6 Organización de la seguridad de la información

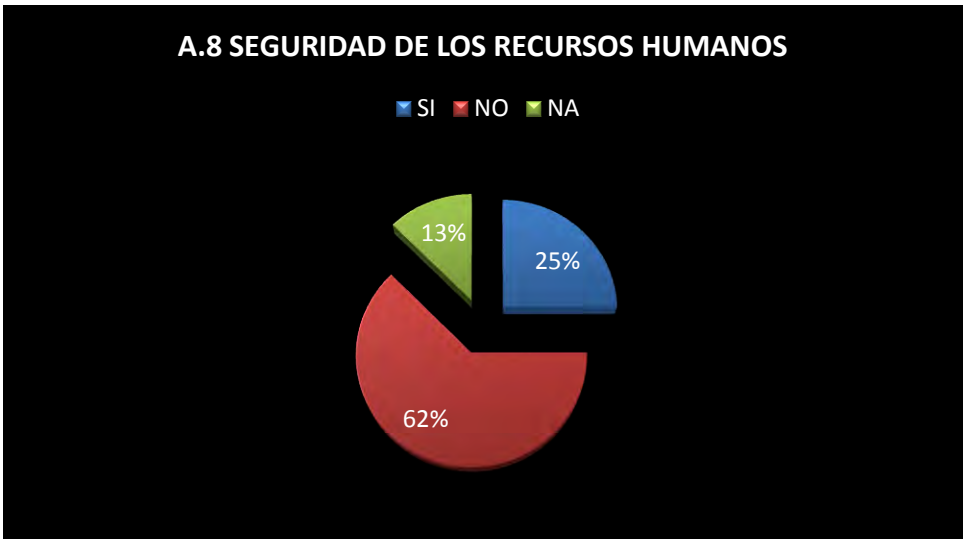
La grafica 10, ilustra un 80% de no cumplimento, 10% Si cumple y 10% No aplica, es decir refleja el no compromiso, no coordinación de la administración con la seguridad de la información, el Si cumple hace referencia a que si es la administración la única para permitir autorizaciones de nuevos servicios donde se involucre al sistema de información Sivigila y el 10% de No aplica deduce que como no hay un acuerdo de confidencialidad de la información que se maneja en el Sivigila y por lo tanto no aplica el hecho que sea conocido por los funcionarios que manejan el sistema.

Figura 11. A.7 Gestión de activos



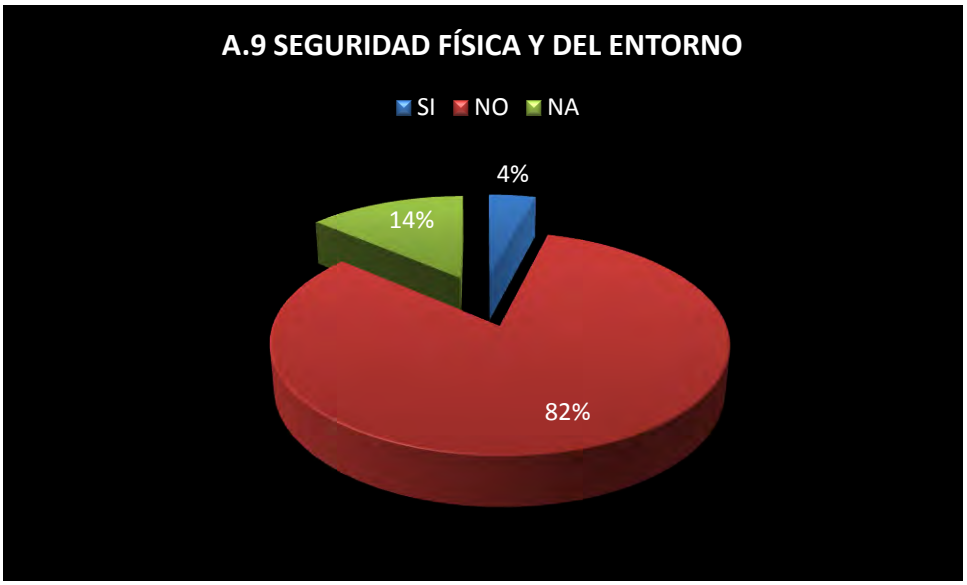
El 60% resume que en la entidad el Sivigila si está incluido como propiedad de la secretaria de salud, que la información que se maneja está clasificada y a su vez etiquetada, el 40% a que el sistema auditado no está en la lista de inventario de activos generales de la entidad y a que no se lleva registro del uso aceptable de la información dada por él.

Figura 12. A.8 Seguridad de los recursos humanos.



El 62% implica que la entidad no revisa antecedentes laborales cuando se contrata personal nuevo para interactuar con el Sivigila, que los funcionarios que manejan el sistema no reciben ni han recibido formación sobre políticas y procedimiento de la organización y que no existe ningún proceso disciplinario en caso de violación a la información emitida por el, el 13% manifiesta que para el manejo del sistema auditado si se ha definido roles y responsabilidades y que lo empleados que lo manejan si firmaron un documento de términos y condiciones, el 25% no aplica porque no existe documento de políticas de seguridad de la información por lo tanto no se le puede exigir a los usuarios revisarlo y practicarlo.

Figura 13. A.9 Seguridad física y del entorno

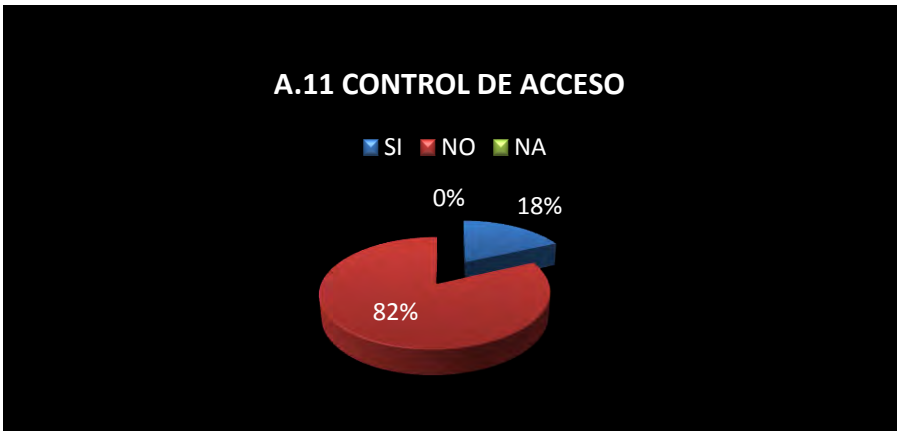


Hay un 82% porque según lo investigado en la entidad para un empleado que haya trabajado con el Sivigila no se contempla en caso de concluir su trabajo algún acuerdo de no divulgación de la información, no se retira de su alcance datos del sistema, no existe un perímetro seguro, no se controla el acceso no autorizado, no se tiene diseñada protecciones contra amenazas externa y ambientales y no se reconoce como área segura; 14% porque se le retira el derecho de acceso al sistema pero solo es eso toda aplicación relacionada con este no se verifica si esta es desinstalada o no del equipo del usuario y el 4% es porque no se permite que los equipos salgan de la secretaria de salud por lo tanto no hay necesidad de brindar seguridad a estos.

Figura 14. A.10 Gestión de comunicaciones y operaciones

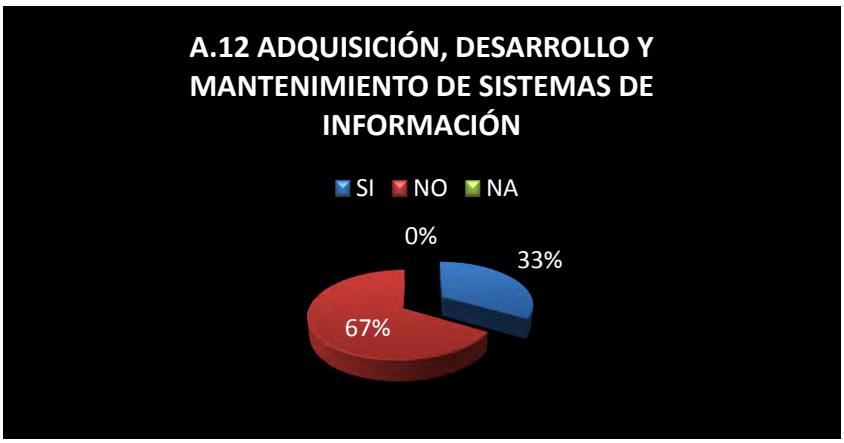
La gráfica 14, muestra un 86% porque en la entidad no se hace seguimiento al desempeño funcional del Sivigila, no hay criterios de aceptación para los cambios en el, no hay controles contra códigos maliciosos, no hay políticas de seguridad para uso de códigos maliciosos, no se hacen copias de la aplicación, no se controlan las redes de tráfico de información del sistema, no hay acuerdos sobre servicios de las redes del sistema y no existe procedimiento contra la no divulgación de los datos dados por él, además de no existir registros de auditorías, monitoreo del uso del sistema, protección de la información y registro de fallas; 5% porque si se hacen cambios de la información que se genera en el sistema esto sucede al momento de recolectar los reportes por la UNM a las UPGD, y también porque si se hacen copias de estos informes; 9% porque como no existen equipos desatendidos en el entorno del Sivigila no se hace necesario exigir protección para estos, no existe políticas de control de acceso entonces no aplica controlar su cumplimiento y como no existen programas criptográficos no hace falta tener controles para estos.

Figura 15. A.11 Control de acceso



El 18% porque si se lleva a cabo registro de usuario en el Sivigila, existen redes agrupadas y compartidas en su entorno; 82% porque no hay restricción en el uso de privilegios, no se revisa los derechos de acceso, no se le exige a los usuarios el uso de contraseña en los equipos donde está instalado el Sivigila, no se controla por la entidad de forma personal si el puerto por donde escucha este está seguro o no, las redes compartidas no se controlan, no existen redes enrutadas en el entorno del sistema, no hay un sistema de gestión de contraseña, no hay políticas de control de acceso y no se tiene al sistema como sensible.

Figura 16. A.12 Adquisición, desarrollo y mantenimiento de sistemas de información



Hay 33% positivo porque si se hacen validaciones de datos de entrada y salida en el Sivigila y porque este se somete a pruebas a nivel de aplicación una vez haya cambios de sistema operativo; 67% porque no existen requisitos para proteger la integridad de los datos, no hay control en caso de mensaje errado, no hay controles criptográficos, no se controla la instalación de software en los equipos donde esté instalado el sistema auditado, no hay un procedimiento formal para elegir datos de prueba para este, la entidad no tiene acceso al código fuente, y no se tiene información sobre vulnerabilidades técnicas que tenga el Sivigila.

Figura 17. A.13 Gestión de los incidentes de la seguridad de la información

Se muestra un 100% de no cumplimiento en esta parte porque no hay reportes de debilidades de la seguridad del Sivigila y no se ha hecho nunca seguimiento a usuarios del sistema y tampoco se ha recolectado evidencia de esto.

Figura 18. A.15 Cumplimiento

El 75% muestra que no se han hecho auditorías al Sivigila, no hay garantías de cumplir procedimientos en el sistema y no se ha planificado requisitos para auditorias, el 25% no aplica cuidar herramientas que deja una auditoria si no se han hecho.

8 INFORME FINAL DE AUDITORIA

8.1 INFORME DE AUDITORIA

OBJETIVOS

OBJETIVO GENERAL

Elaborar planes de mejoramiento que redunden en la gestión de la información mediante la aplicación de procesos de auditoría a la seguridad basada en el estándar ISO 27001 en el sistema de información SIVIGILA de la secretaria de salud de la Alcaldía de Tumaco.

OBJETIVOS ESPECÍFICOS

- Identificar el lugar a auditar que permita desarrollar una investigación completa y verídica que dé lugar a un plan de auditoria completo y que valla acorde con las necesidades de la entidad que se está evaluando.
- Desarrollar un plan de auditoria acorde con la investigación hecha en el lugar a auditar.
- Desarrollar herramientas, técnicas y procedimientos para la recolección de información y obtención de evidencias en el proceso de auditoría.
- Obtener evidencias mediante la ejecución del plan de auditoria.
- Sintetizar y sistematizar los hallazgos del resultado del proceso de auditoría
- Socializar el informe final de auditoria a la alcaldía de Tumaco

HALLAZGOS Y EVIDENCIAS

Todo proceso de auditoria conduce a encontrar procesos cumplidos y no cumplidos en una entidad determinada según la norma que se esté aplicando en el presente trabajo se tuvo de referente la norma ISO/IEC 27001 a continuación se describe lo hallado mediante el método observación directa y el análisis obtenido de la entrevista y la lista de chequeo.

Según lo antes dicho teniendo en cuenta las listas de chequeo, la entrevista, además del recorrido hecho en la entidad se encontró lo siguiente:

❖ En el entorno del Sivigila:

- Una oficina sin perímetro seguro.
- El equipo de la UNM del Sivigila ubicado en la primera esquina de la entrada de la oficina.
- El equipo donde reposa la información de todos los reportes del sistema puede ser usados por cualquier otro usuario
- Existen copias de los reportes del Sivigila pero que estos están en el mismo equipo de la UNM.
- Se tiene copias de la información del Sivigila en la web pero en el correo personal de la UNM.
- Son en total 12 UPGD que reportan información a la UNM.
- La UNM del Sivigila maneja la parte funcional de este con total destreza y rapidez.
- El Sivigila funcionalmente está en óptimas condiciones, el problema radica en el forma como los usuarios tratan y no cuidan la información que este genera.

❖ En la dependencia de sistemas:

- En la entidad se utiliza esta área para trabajos técnicos.
- Que la seguridad de la información no es tema de trabajo en esta área de la entidad.
- Los funcionarios de esta parte de la entidad no están obligados a dar formación acerca de seguridad de la información a otras dependencias.

❖ En la entidad en general:

- No hay políticas de seguridad de la información.
- Se tiene como poco importante la seguridad de la información
- La información no se contempla como activo de la entidad.
- No hay mucho compromiso con la seguridad de la información
- La palabra “auditoria” genera malestar laboral.
- Siempre hay temas más importantes que ser pioneros en la protección de los datos manejados en la organización.
- Poco orden en el desarrollo de los procesos.

RECOMENDACIONES DEL INFORME DE AUDITORIA

- Trazar un perímetro seguro en la oficina donde se hace la recepción de la información del Sivigila, con la finalidad de generar un ambiente seguro para la información que se maneja no solo en el sistema Sivigila sino al mismo tiempo los otros sistemas que estén al servicio de la alcaldía que permiten la recepción de datos y consolidado de información.

- Ubicar el equipo de la UNM de forma estratégica de tal forma que sea de difícil acceso al personal no autorizado, en este equipo se guarda toda la información epidemiológica del municipio, es decir, está el consolidado de todos los pacientes con sus respectivas dolencias y enfermedades, en un caso de violación de datos y en las manos equivocadas podrían ocasionar grandes daños en la comunidad tumaqueña.

- Realizar copias de seguridad en la web, dichas copias que no estén en el correo personal de la UNM sino en una cuenta electrónica institucional de la alcaldía donde se tenga la seguridad que únicamente el personal autorizado tenga acceso a ella.

- Solo el personal autorizado puede hacer la notificación a la UNM, de esta forma queda claro para los funcionarios que solo el personal que está avalado es el que maneja información tan delicada como la que se procesa en el Sivigila.

9 ESTRUCTURA DE POLITICA DE SEGURIDAD DE LA INFORMACION PARA LA ALCALDIA DE SAN ANDRES DE TUMACO

Desarrollado el trabajo y teniendo en cuenta las necesidades de la Alcaldía de Tumaco a partir del proceso de auditoria realizado al sistema de información Sivigila, se miró con buenos ojos la creación de la primera política de seguridad de la información para la entidad, que busca despertar el interés de la administración y los funcionarios de la organización para poder asegurar que se está trabajando por obtener la confiabilidad, disponibilidad, e integridad de la información, a continuación se describe la estructura la política de seguridad que se propone.

Alcance

1. TÉRMINOS Y DEFINICIONES
    - Seguridad de la información
    - Evaluación de riesgos
    - Administración de riesgos
    - Comité de seguridad de la información
    - Responsable de seguridad informática
    - Incidente de seguridad
2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
    - Aspectos generales
    - Sanciones previstas por incumplimiento
3. ORGANIZACIÓN DE LA SEGURIDAD
    - Infraestructura de la seguridad de la información
    - Cooperación entre organismos
    - Seguridad frente al acceso por parte de terceros
    - Tercerización
4. CLASIFICACIÓN Y CONTROL DE ACTIVOS
    - Inventario de activos
    - Clasificación de la información
    - Rotulado de la información
5. SEGURIDAD DEL PERSONAL
    - Seguridad en la definición de puestos de trabajo y la asignación de recursos
    - Capacitación del usuario
    - Respuesta a incidentes y anomalías en materia de seguridad
6. SEGURIDAD FÍSICA Y AMBIENTAL
    - Perímetro de seguridad física
    - Controles de Acceso Físico
    - Protección de oficinas, recintos e instalaciones
    - Desarrollo de tareas en áreas protegidas
    - Aislamiento de las áreas de recepción y distribución

- Ubicación y protección del equipamiento y copias de seguridad
- Suministros de energía
- Seguridad del cableado
- Mantenimiento de equipos
- Seguridad de los equipos fuera de las instalaciones.
- Desafectación o reutilización segura de los equipos.
- Políticas de escritorios y pantallas limpias.
- Retiro de los bienes

7. GESTIÓN DE COMUNICACIONES Y OPERACIONES
   - Procedimientos y responsabilidades operativas
   - Planificación y aprobación de sistemas
   - Protección contra software malicioso
   - Mantenimiento
   - Administración de la red
   - Administración y seguridad de los medios de almacenamiento
   - Intercambios de información y software
8. CONTROL DE ACCESOS
   - Requerimientos para el control de acceso
   - Administración de accesos de usuarios
   - Responsabilidades del usuario
   - Control de acceso a la red
   - Control de acceso al sistema operativo
   - Control de acceso a las aplicaciones
   - Monitoreo del acceso y uso de los sistemas
   - Computación móvil y trabajo remoto
9. DESARROLLO Y MANTENIMIENTO DE SISTEMAS
   - Requerimientos de seguridad de los sistemas
   - Controles criptográficos
   - Seguridad de los archivos del sistema
   - Seguridad de los procesos de desarrollo y soporte
10. ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL LA ALCALDIA
    - Proceso de la administración de la continuidad de la alcaldía
    - Continuidad de las actividades y análisis de los impactos
    - Elaboración e implementación de los planes de continuidad de las actividades de la alcaldía
    - Marco para la planificación de la continuidad de las actividades de la alcaldía
    - Ensayo, mantenimiento y reevaluación de los planes de continuidad de la alcaldía.
11. CUMPLIMIENTO

- Cumplimiento de requisitos legales
- Revisiones de la política de seguridad y la compatibilidad técnica
- Consideraciones de auditorías de sistemas
- Sanciones previstas por incumplimiento

Una vez desarrollada la política de seguridad de la información para la alcaldía es necesario tener técnicas de divulgación para hacer que lo funcionarios de la entidad la conozcan y la pongan en práctica, dichas técnicas se describen a continuación.

9.1 ESTRATEGIA DE DIVULGACION DE POLITICA DE SEGURIDAD DE LA INFORMACION A LA ALCALDIA DE TUMACO.

La estrategia para dar a conocer la política de seguridad fue la siguiente:

- ❖ Socializar política con los administradores de la alcaldía: con la finalidad de despertar el interés y obtener ayuda y respaldo para tener vía libre con los funcionarios de la entidad.

- ❖ Reunión general con los funcionarios jefes de la alcaldía: son ellos los que después de administración deben conocer y aprender a tener interés por la política para que puedan dar permisos a sus súbditos para los talleres.

- ❖ Talleres: una vez dada a conocer la política a los funcionarios jefes programar reuniones con los demás empleados de la entidad, en forma taller donde ellos pregunten, se les enseñe algo sobre seguridad de la información y su importancia, sobre consecuencias de perdida de información y además sobre la responsabilidad que tienen ellos con el cuidado de la misma, que ellos tengan la oportunidad de aprender y participar para poder asegurar el cumplimiento de la política.

Toda esta estrategia es posible si la primera reunión propuesta en la misma tiene resultados positivos, porque de esta forma serán más fáciles los otros puntos mencionados.

10 CONCLUSIONES.

- Con la investigación hecha al sistema de información Sivigila este tendrá políticas de seguridad para la protección de la información que reporta a la alcaldía de Tumaco, las cuales estarán basadas en herramientas y normas ya establecidas y aprobadas para asegurar y disminuir la perdida y mal uso de los datos que se tengan de él.

- Se desarrolló un plan de auditoria que permitieron desarrollar herramientas para la recolección de datos donde se concluyó que el Sivigila es un sistema que maneja información delicada del municipio de Tumaco y que por lo tanto el cuidado de esta es tarea de la administración y que debe haber compromiso de la misma para que se asegure que no haya violación y alteraciones de los datos.

- Evidencia que permitieron sintetizar los hallazgos encontrados y posteriormente la socialización del trabajo el cual demostró los resultados obtenidos a partir de la auditoria desarrollada en la Alcaldía.

- La alcaldía de Tumaco como mayor entidad en el municipio debe tener funcionarios comprometidos, conscientes de la importancia de cuidar la información y de los daños que causa la pérdida o falta de integridad de esta en una organización que vela por el bienestar de toda una comunidad.

- La ISO 27001 es una norma que orienta, guía y ayuda para saber qué hacer en una entidad cuando se dice que se va a auditar un área o sistema específico, da bases para hacer un trabajo con un fin y llegar a una conclusión y poder establecer una hipótesis y en base a esto dar una posible solución.

11 RECOMENDACIONES

- Comprometer la seguridad de la información, de lo contrario no es posible adelantar ningún proceso en una entidad si no existe un interés por partes de los directivos por mejorar y marcar un tendencia sobre otros referentes.

- Definir al Sivigila como un sistema sensible, donde se maneja información delicada y de mucho cuidado por parte de los funcionarios que la manejan.

- Plantear un SGSI para la secretaria de salud que sirva como base para una propuesta futura para toda la organización, sirviendo este para empezar a manejar la información procesad en el Sivigila de una forma adecuada y así asegurar con bases que los datos son íntegros y no sufren alteración.

- Definir políticas de seguridad de la información que tenga como finalidad proteger no solo la información dada por el Sivigila sino de toda la entidad, siendo estas acatadas y cumplidas por todos los funcionarios de le entidad.

- Capacitar a los funcionarios de la entidad sobre seguridad de la información y hacerles ver que los datos que maneja toda la organización son importantes porque de cierta forma son el consolidado de toda una población que confía en los procesos que se desarrollan dentro de esta.

- Involucrar a la Universidad de Nariño como institución de educación superior para el apoyo y acompañamiento en la planificación e implantación del SGSI, políticas de seguridad de la información y capacitación del personal de la alcaldía.

- Orientar a los funcionarios de la alcaldía para que guarden escrupulosamente los secretos técnicos, comerciales en los que se encuentren involucrados directa o indirectamente, o de los cuales ellos tengan conocimiento por la razón del trabajo que ellos desempeñen, de la misma manera los asuntos de carácter administrativo reservados cuya divulgación pueda ocasionar malestares a la entidad.

- Establecer políticas para los funcionarios ya sea en el entorno del Sivigila o la entidad en general donde estos se encuentren involucrados en tratar datos personales como por ejemplo en nómina y contrataciones a guardar la confidencialidad respecto a estos, y aclarar que esta obligación se mantendrá aun después de finalizar relaciones con la alcaldía.

- Informar de forma inmediata a los responsables de los datos con la finalidad de que ellos puedan tomar medidas necesarias de control a la defensa de la información.

- Realizar Campañas de concientización entre los funcionarios de la Alcaldía desde los guardias de seguridad hasta los administrativos, con la finalidad de que ellos comprendan:
  a. Que es información confidencial, secreta, sensible o clasificada, y por qué dicha información esta etiquetada de esta forma.
  b. Conozcan las implicaciones legales que pueden surgir si comparten, copian o divulgan dicha información, donde las consecuencias pueden ir desde una amonestación administrativa hasta el despido o la cárcel.
  c. Hacer revisiones en determinado tiempo de las contrataciones individuales para asegurase de que los documentos firmados por los funcionarios de la alcaldía tenga cláusulas de confidencialidad de la información y la protección de los datos.

- Elaborar políticas donde se relacionen temas que regulen el uso de redes sociales, recursos informáticos, información confidencial y privada, dichas políticas debe estar ligado a reglamentos internos o los contratos de los funcionarios de la alcaldía y ser de total conocimiento para ellos.

- Tener en la Alcaldía medida de seguridad técnicas, físicas, y administrativas para proteger la información contra robos, destrucción, alteración, uso o acceso no autorizado.

- Tener un plan de reacción, sí llega a darse el caso de vulneración de la información o bases de datos del Sivigila o demás sistemas de la Alcaldía.

- Enterar de forma inmediata a los funcionarios que pudieran haber sido comprometidos
- Aplicar sanciones laborales en caso de existir responsabilidad por parte de los funcionarios.

12 BIBLIOGRAFÍA

- Echenique García, José Antonio. Auditoria En Informática: McGraw-Hill/Interamericana editores, S.A de C.V., 2001. Pág.11.

- Razo Muñoz Carlos . Auditoria en Sistemas Computacionales: Pearson Educacion Mexico 2002. Pág. 11.

- Sanchez Curiel Gabriel. Auditoria de Sistemas Financieros: Pearson Educacion Mexico 2006. Pág. 2.

- MAGERIT Metodología de Análisis y Gestión de Riesgos. pág. 7

- Norma Técnica Colombiana NTC-ISO/IEC 27001, 2006

- Castello Ricardo. Auditoria de Entornos Informáticos: Segunda edición - Diciembre de 2006 I.S.B.N. 950-33-0199-8 2006. Pág. 225

- Rodea Jesús. Seguridad Informática. Pág. 26.

- http://www.mailxmail.com/curso-implantacion-sistema-gestion-seguridad/definicion-politica-seguridad

- http://www.iso27000.es/glosario.html

- http://www.portalcalidad.com/etiquetas/240-Checklist._Lista_de_verificacion

- http://www.tumaco-narino.gov.co/index.shtml#5

- http://www.tumaco-narino.gov.co/informacion_general.shtml#geografia

- http://www.tumaco-narino.gov.co/quienes_somos.shtml

13 ANEXOS

Anexo 1. Carta de presentación del informe

Señores Alcaldía de Tumaco.

De la forma más atenta y agradecida les manifiesto mi gratitud por la oportunidad que se me fue dada al permitir desarrollar la auditoria de sistemas en las instalaciones de la alcaldía. Fue una experiencia agradable y gratificante para la vivencia profesional que comenzó desde el primer instante que fui aceptada en la entidad.

El presenta documento contienen los resultados del proceso de auditoria donde se describe los hallazgos encontrados basados en la ISO/IEC, además la gestión de riesgo mediante basado en el marco del estándar MAGERIT utilizado como referencia para el desarrollo de este capítulo del presente trabajo; se describe también todos los estándares que se citan, los autores, conclusiones y recomendaciones hechas según los resultados de la auditoria.

Mis más sinceros respetos para el señor alcalde Víctor Arnulfo Gallo Ortiz quien no tuvo reservas en darme una respuesta positiva a la propuesta que se planteó desde el inicio, a la señora Yamileth Ramos quien es la Notificadora Municipal y principal usuario del sistema de información Sivigila en el municipio de San Andrés de Tumaco, por permitir y enseñarme el manejo del sistema y como podría abordar el acceso a la información que se necesitó para continuar con el trabajo propuesto; al señor Jhon Javer Mininderos Satizabal Coordinador de la Oficina de Sistemas de la alcaldía quien en todo momento tuvo disposición, paciencia y toda la amabilidad para atenderme y despejar dudas de procesos que se manejan en la entidad, además de ser el profesional afine al trabajo realizado quien dio el visto bueno y el aporte final para la culminación de la auditoria, a todos los compañeros que hicieron posible pasar tardes agradables permitiendo que el trabajo fuera más ameno y menos pesado, gracias por toda la atención y disponibilidad prestada.

Yurani Alejandra Landázuri Guevara
Estudiante de Ingeniería de Sistemas
Universidad de Nariño.

Anexo 1. Lista de chequeo

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control		**A.5 POLÍTICA DE SEGURIDAD**	
	Objetivo de lista de chequeo:			
Lista de chequeo	Numero	1	Duración	1 día
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.5 POLÍTICA DE SEGURIDAD

A.5.1 Política de seguridad de la información

Objetivo: Brindar apoyo y orientación a la administración de la alcaldía respecto a la seguridad de la información, de acuerdo con los requisitos de la alcaldía de San Andrés de Tumaco y los reglamentos y las leyes pertinentes.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.5.1.1	Documento de la política de seguridad de la información.	1. ¿Existe una política de seguridad de la información aprobada por la administracion de la alcaldía?		X		
		2. ¿Es conocida esta política por los funcionarios y parte externa a la alcaldía?			X	
A.5.1.2	Revisión de la política de seguridad de la información.	3. ¿Se planifican intervalos de revisión de la política de seguridad?			X	

<table>
<tr><td colspan="4">UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
FACULTAD DE INGENIERIA
PROGRAMA DE SISTEMAS
ALCALDIA DE SAN ADRES DE TUMACO
LISTA DE CHEQUEO</td><td>UNIVERSIDAD DE NARIÑO.</td></tr>
<tr><td rowspan="2">Programa de formación: Ingeniería de Sistemas</td><td colspan="2">Control :</td><td colspan="2">A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td colspan="2">Objetivo de lista de chequeo.</td><td colspan="2"></td></tr>
<tr><td>Lista de chequeo</td><td>Numero</td><td>2</td><td>Duración</td><td>1 día</td></tr>
<tr><td>Nombre auditor</td><td colspan="4">Yurani Alejandra Landázuri Guevara</td></tr>
<tr><td>Nombre asesor</td><td colspan="4">José Javier Villalba Romero</td></tr>
</table>

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
A.6.1 Organización interna

Objetivo: gestionar la seguridad de la información dentro de la alcaldía de San Andrés Tumaco.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.6.1.1	Compromiso de la dirección con la seguridad de la información	4. ¿La administracion apoya de forma activa la seguridad de la información dentro de la alcaldía?		X		La parte directiva de la entidad de cierta manera ignora la importancia de la seguridad de la información
A.6.1.2	Coordinación de la seguridad de la información	5. ¿Existen en la entidad actividades de la seguridad de la información?		X		
		6. ¿Coordina la secretaria de salud de la alcaldía alguna actividad de la seguridad de la		X		
A.6.1.3	Asignación de responsabilidades para la seguridad de la información	7. ¿En la secretaria de salud se ha asignado responsabilidades para la seguridad de la información?		X		
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información	8. ¿Es la dirección de la secretaria de salud la encargada de emitir autorizaciones para nuevos servicios que involucren al Sivigila?	X			Es así de cierta forma porque es la jefe de epidemiologia quien autoriza la utilización del Sivigila en
A.6.1.5	Acuerdos sobre confidencialidad	9. ¿Existe algún acuerdo de confidencialidad formal para proteger la información que maneja el Sivigila?		X		
		10. ¿Si existe un acuerdo de confidencialidad, este es conocido por los funcionarios de la secretaría de la salud?			X	Ignoran en esta área que es un acuerdo de confidencialidad
A.6.1.6	Contactos con las autoridades	11. ¿Se mantiene contactos con las autoridades en caso de robo de información?		X		
A.6.1.7	Contactos con grupos de interés especiales	12. ¿La secretaria de salud tiene contacto con grupos especializados en seguridad de información?		X		
A.6.1.8	Revisión independiente de la seguridad de la información	13. ¿Hace la secretaria revisiones de la documentos que traten sobre la seguridad de la información (es decir, objetivos de control, controles y proceso para la seguridad de			X	No tienen política de seguridad de la información

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	3	Duración	2 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.6.2 Partes externas

Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la alcaldía de San Andrés de Tumaco a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.6.2.1	Identificación de los riesgos relacionados con la partes externa	14. ¿La secretaria de salud tiene identificado los riesgos a los que está expuesta la información y activos relacionados con el Sivigila cuando se involucran partes externas?		X		Son conscientes de cuidarse respecto a partes externas pero es solo eso
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	15. ¿Se ha considerados requisitos de seguridad que implique procesamiento de información en el Sivigila en acuerdos		X		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.7 GESTIÓN DE ACTIVOS**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	4	Duración	2 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.7.1 Responsabilidad por los activos

Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.7.1.1	Inventario de activos	16. ¿Está incluido el Sivigila en el inventario de activos de la alcaldía?		X		
A.7.1.2	Propiedad de los activos	17. ¿Está registrado el Sivigila como propiedad de la secretaria de salud?	X			
A.7.1.3	Uso aceptable de los activos	18. ¿Se maneja documentos del uso aceptable de la información procesada por el		X		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.7 GESTIÓN DE ACTIVOS**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	5	Duración	2 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.7.2 Clasificación de la información

Objetivo: asegurar que la información recibe el nivel de protección adecuado.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.7.2.1	Directrices de clasificación	19. ¿La información procesada por el Sivigila está clasificada?	X			
		20. ¿Para clasificar la información manejada en el Sivigila se tiene en cuenta la sensibilidad y la importancia que esta tiene para la entidad?		X		Se clasifica la información pero por orden de fecha
A.7.2.2	Etiquetado y manejo de información	21. ¿Esta etiquetada la información que se maneja en el Sivigila?	X			Esta etiquetada por UPGD

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.8 SEGURIDAD DE LOS RECURSOS HUMANOS**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	6	Duración	2 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.8.1 Antes de la contratación laboral

Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.8.1.1	Roles y responsabilidades	22. ¿Se tiene definido y documentado roles y responsabilidades de los empleados que manejan el Sivigila?	X			
A.8.1.2	Selección	23. ¿Para adquirir personal nuevo en el manejo de información procesada por el Sivigila se verifica antecedentes antes de la contratación?		X		
A.8.1.3	Términos y condiciones laborales	24. ¿Los empleados que manejan el Sivigila conocen y han firmado acuerdos de término y condiciones?	X			

<table>
<tr><td colspan="4">UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
FACULTAD DE INGENIERIA
PROGRAMA DE SISTEMAS
ALCALDIA DE SAN ADRES DE TUMACO
LISTA DE CHEQUEO</td><td>UNIVERSIDAD DE NARIÑO.</td></tr>
<tr><td rowspan="2">Programa de formación: Ingeniería de Sistemas</td><td colspan="2">Control :</td><td colspan="2">A.8 SEGURIDAD DE LOS RECURSOS HUMANOS</td></tr>
<tr><td colspan="2">Objetivo de lista de chequeo.</td><td colspan="2"></td></tr>
<tr><td>Lista de chequeo</td><td>Numero</td><td>7</td><td>Duración</td><td>2 horas</td></tr>
<tr><td>Nombre auditor</td><td colspan="4">Yurani Alejandra Landázuri Guevara</td></tr>
<tr><td>Nombre asesor</td><td colspan="4">José Javier Villalba Romero</td></tr>
</table>

A.8.2 Durante la vigencia de la contratación laboral

Objetivo*:* asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.8.2.1	Responsabilidades de la dirección	25. ¿Exige la administracion a los empleados que manejan el Sivigila aplicar políticas de seguridad?			**X**	No existen políticas de seguridad
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	26. ¿El personal involucrado con la información procesada por el Sivigila recibe formación sobre políticas y procedimientos de la alcaldía?		**X**		
A.8.2.3	Proceso disciplinario	27. ¿Existe algún proceso disciplinario para los empleados que hayan cometido violación a la seguridad de la información manejada en el Sivigila?		**X**		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.8 SEGURIDAD DE LOS RECURSOS HUMANOS**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	7	Duración	3 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo: asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la alcaldía de San Andrés de Tumaco o cambian su contrato laboral de forma ordenada.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.8.3.1	Responsabilidades en la terminación	28. ¿Un empleado termina su contratación, si ha manejado información en el Sivigila se tiene en cuenta las responsabilidades		**X**		
A.8.3.2	Devolución de activos	29. ¿Al finalizar contrataciones la App del Sivigila es retirada del alcance de los empleados?		**X**		
A.8.3.3	Retiro de los derechos de acceso	30. ¿Cuándo se termina una contratación, se retira el derecho de acceso al Sivigila?	**X**			Aunque quede la App instalada en la Pc del empleado retirado este ya no tiene acceso porque el código único es dado de baja en el sistema

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.9 SEGURIDAD FÍSICA Y DEL ENTORNO**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	8	Duración	4 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.9.1 Áreas seguras

Objetivo*:* evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la alcaldía de San Andrés de Tumaco.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.9.1.1	Perímetro de seguridad física	31. ¿En el área donde se procesa la información consolidada del Sivigila se utiliza perímetro de seguridad?		X		Es una oficina común y corriente a donde toda persona tiene acceso
A.9.1.2	Controles de acceso físico	32. ¿En el área principal de procesamiento de información del Sivigila se controla el acceso de personal no autorizado?		X		
A.9.1.4	Protecciones contra amenazas externas y ambientales	33. ¿Se tiene diseñada protecciones contra amenazas externas y ambientales en la secretaria de salud?		X		
A.9.1.5	Trabajo en áreas seguras	34. ¿Se tiene el área de procesamiento de información del Sivigila como área segura?		X		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.9 SEGURIDAD FÍSICA Y DEL ENTORNO**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	9	Duración	1 día
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.9.2 Seguridad de los equipos

Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la alcaldía de San Andrés de Tumaco.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.9.2.1	Ubicación y protección de los equipos	35. ¿Los equipos utilizados para procesar información del Sivigila están bien ubicados?		X		
A.9.2.2	Servicios de suministro	36. ¿Los equipos utilizados para procesar información del Sivigila están protegidos contra fallas eléctricas?	X			
A.9.2.3	Seguridad del cableado	37. ¿El cableado de energía eléctrica que transporta los datos emitidos por el Sivigila está protegido contra daños?	X			
A.9.2.4	Mantenimiento de los equipos	38. ¿Los equipos utilizados para procesar información del Sivigila reciben mantenimiento?	X			
A.9.2.5	Seguridad de los equipos fuera de las instalaciones	39. ¿En caso de salir de las instalaciones los equipos donde se encuentre información del Sivigila se les suministran seguridad?			X	No se permite sacar equipos de la secretaria de salud
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos	40. ¿Se verifican los elementos o medios de almacenamiento de los equipos donde se tiene información del Sivigila una vez estos ya no se utilizan?	X			

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	10	Duración	3 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.10.3 Planificación y aceptación del sistema

Objetivo*:* minimizar el riesgo de fallas de los sistemas.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.10.3.1	Gestión de la capacidad	41. ¿Se hace seguimiento al desempeño funcional del Sivigila?		**X**		Por parte de le entidad no se hace
A.10.3.2	Aceptación del sistema	42. ¿Se tiene establecido criterios de aceptación para actualizaciones o cambios en el Sivigila?		**X**		Solo se instalan la actualización y listo

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	11	Duración	2 días
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.10.4 Protección contra códigos maliciosos y móviles

Objetivo: proteger la integridad del software y de la información.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.10.4.1	Controles contra códigos maliciosos.	43. ¿Se tiene controles de detección, protección y recuperación contra códigos maliciosos para el Sivigila?		X		
A.10.4.2	Controles contra códigos móviles	44. ¿Se autoriza utilización de códigos móviles en equipos donde trabaja con el Sivigila?			X	No tiene noción de que son códigos móviles no se sabe con exactitud si lo permiten o no
		45. ¿Hay políticas de seguridad establecida para uso de códigos móviles en el Sivigila?		X		

A.10.5 Respaldo

Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.10.5.1	Respaldo de la información.	46. ¿Se hacen copias de seguridad de la App del Sivigila?	X			
		47. ¿Se hacen copias de la información procesada en el Sivigila?	X			Las copias de la información consolidada del Sivigila reposan en el equipo de la UNM

		48. ¿Se prueban de forma regular las copias hechas del Sivigila?		**X**		
A.10.6 Gestión de la seguridad de las redes Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.10.6.1	Controles de la redes.	49. ¿Las redes por donde viaja la información dada por el Sivigila se controlan y se mantiene protegidas?		**X**		
A.10.6.2	Seguridad de los servicios de la red.	50. ¿Se tiene acuerdo sobre servicios de las redes usadas por el Sivigila?		**X**		
A.10.7 Manejo de los medios Objetivo*:* evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades de la alcaldía de San Andrés de Tumaco.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.10.7.1	Gestión de los medios removibles	51. ¿Existe algún procedimiento para la gestión de medios removibles en los equipos donde se trabaja con el Sivigila?		**X**		Si es necesario para la persona que está en el equipo en un llegado momento trabajar con medios removibles solo lo hace y ya.
A.10.7.2	Eliminación de los medios	52. ¿Cuándo los medios ya no se requieren en los equipos donde se trabaja con el Sivigila se utilizan procedimientos formales para retirarlos?		**X**		

A.10.7.3	Procedimientos para el manejo de la información	53. ¿Para el manejo de la información dada por el Sivigila existe algún procedimiento contra la divulgación no autorizada?		**X**		Es el usuario que define que tanto divulga o que tanto guarda de la información dada por el Sivigila
A.10.7.4	Seguridad de la documentación del sistema	54. ¿Tiene la secretaria de salud documentación del Sivigila (Manuales, documentos de fallas, reportes, etc.)?	**X**			Se puede decir en este control que sí y no. Si porque se tiene el manual dado por el fabricante y no porque demás manuales de fallas y reportes no se tienen
		55. ¿Está protegida la documentación del Sivigila contra el acceso no autorizado?		**X**		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	12	Duración	1 día
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.10.8 Intercambio de la información

Objetivo*:* mantener la seguridad de la información y del software que se intercambian dentro de la alcaldía de San Andrés de Tumaco y con cualquier entidad externa.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.10.8.1	Políticas y procedimientos para el intercambio de información	56. ¿Se hacen intercambios de información emitidas por el Sivigila?	**X**			
		57. ¿Para el intercambio de información del Sivigila se tienen controles formales?		**X**		
A.10.8.2	Acuerdos para el intercambio	58. ¿Existen acuerdos para el intercambio de información dada por el Sivigila?		**X**		
A.10.8.3	Medios físicos en tránsito.	59. ¿Todos los medios que contienen información del Sivigila están protegidos contra el acceso no autorizado y uso inadecuado?		**X**		

A.10.8.4	Mensajería electrónica.	60. ¿La información del Sivigila que está en mensajería electrónica está debidamente cuidada?		**X**		Únicamente con la contraseña de correo personal del usuario del sistema
A.10.8.5	Sistemas de información del negocio.	61. ¿Hay políticas que protejan la información del Sivigila en el caso de interconectarse con otros sistemas de información de la alcaldía?		**X**		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	13	Duración	2 días
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.10.10 Monitoreo

Objetivo: detectar actividades de procesamiento de la información no autorizadas.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.10.10.1	Registro de auditorias	62. ¿Se han desarrollado auditorias en la secretaria de salud o de forma general en la alcaldía?		X		
		63. ¿Se tiene registro de auditorías pasadas hechas al Sivigila o algún otro sistema de información de la entidad?		X		Porque no se han hecho auditorias de ningún tipo
A.10.10.2	Monitoreo del uso del sistema	64. ¿Se hacen monitoreo al uso del Sivigila?		X		
		65. ¿Hay algún procedimiento definido para realizar monitoreo al Sivigila?		X		
		66. ¿Se revisa con regularidad los resultados del monitoreo al Sivigila?		X		
A.10.10.3	Protección de la información del registro	67. ¿Se lleva registro de la actividad del Sivigila?		X		
		68. ¿Están protegidos estos registros contra manipulación no autorizada?		X		

A.10.10.4	Registros del administrador y del operador	69. ¿Se registran actividades de las UPGD y la UNM del Sivigila?		**X**		
A.10.10.5	Registro de fallas	70. ¿Se lleva registro de fallas del Sivigila?		**X**		
		71. ¿Se hacen análisis de fallas del Sivigila?		**X**		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.11 CONTROL DE ACCESO**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	14	Duración	3 días
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.11.2 Gestión del acceso de usuarios

Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.11.2.1	Registro de usuarios	72. ¿Se lleva a cabo en el Sivigila registro de usuarios?	**X**			
		73. ¿Existe procedimientos formales para el registro de usuarios en el Sivigila?		**X**		
A.11.2.2	Gestión de privilegios	74. ¿Para procesar información en el Sivigila se restringe la asignación de privilegios?		**X**		
A.11.2.3	Gestion de contraseñas para usuarios	75. ¿la asignación de contraseñas en el Sivigila se hace bajo un procedimiento formal?		**X**		

A.11.2.4	Revisión de los derechos de acceso de los usuarios	76. ¿Se revisa periódicamente los derechos de acceso de usuarios?		**X**		
A.11.3 Responsabilidades de los usuarios Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.11.3.1	Uso de contraseñas	77. ¿Se le exige a los usuarios el uso de contraseñas, en los equipos donde se trabaja con el Sivigila?		**X**		
A.11.3.2	Equipo de usuario desatendido	78. ¿Existe equipo desatendidos en la secretaria de salud?		**X**		
		79. ¿Se les brinda seguridad a estos equipos desatendidos?			**X**	No hay equipos desatendidos en el entorno del Sivigila
A.11.3.3	Política de escritorio despejado y de pantalla despejada	80. ¿Existe política de escritorio despejado en los equipos donde se trabaja con el Sivigila?		**X**		
		81. ¿Existe política de pantalla despejada en los equipos donde se trabaja con el Sivigila?		**X**		
A.11.4 Control de acceso a las redes Objetivo: evitar el acceso no autorizado a servicios en red.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.11.4.1	Política de uso de los servicios de red.	82. ¿Los usuarios del Sivigila usan solo los servicios que se les autoriza?		**X**		Tienen la autonomía de usar lo que gusten no hay controles para cuidar el uso de los
A.11.4.2	Autenticación de usuarios para conexiones externas.	83. ¿Hay control en la autenticación de usuario en el Sivigila de forma remota?		**X**		

A.11.4.3	Identificación de los equipos en las redes.	84. ¿Se tiene en cuenta la identificación automática de los equipos que trabajan con el Sivigila?		**X**		No saben lo que significa este procedimiento por lo tanto no lo practican
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	85. ¿El puerto por donde escucha el Sivigila está controlado?		**X**		En este caso fue necesario preguntar al Ing. de sistemas de la entidad y lastimosamente no hubo respuesta
A.11.4.5	Separación en la redes.	86. ¿Las redes usadas por el Sivigila están agrupadas?	**X**			
A.11.4.6	Control de conexión a las redes.	87. ¿Existen redes compartidas en el entorno del Sivigila?	**X**			
		88. ¿Si hay redes compartidas, estas son controladas?		**X**		
A.11.4.7	Control de enrutamiento en la red.	89. ¿En el entorno lógico del Sivigila están las redes enrutadas?		**X**		En el entorno del Sivigila la parte lógica de las redes no se cuida mucho de hecho no se le tiene considerado controles de seguridad

A.11.5 Control de acceso al sistema operativo
Objetivo: evitar el acceso no autorizado a los sistemas operativos.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			
			SI	NO	NA	
.11.5.1	Procedimientos de ingreso seguros	90. ¿El acceso a los equipos donde se trabaja con el Sivigila, se hace bajo el procedimiento de inicio seguro?		**X**		Ignoran este procedimiento
A.11.5.2	Identificación y autenticación de usuarios.	91. ¿Tienen los usuarios del Sivigila ID de usuario?	**X**			
		92. ¿Se tienen técnicas para comprobar la identidad de cada usuario?		**X**		

A.11.5.3	Sistema de gestión de contraseñas.	93. ¿Existen sistemas de gestión de contraseñas en la organización?		**X**		
		94. ¿Si existen tales sistemas aseguran la calidad de las contraseñas?			**X**	No se tiene este tipo de sistema en la entidad
A.11.5.4	Uso de las utilidades del sistema	95. ¿Se tienen programas utilitarios en los equipos que trabajan con el Sivigila?		**X**		Se ignora este tipo de sistema en la entidad
		96. ¿Se restringe el uso de estos programas?			**X**	
A.11.5.5	Tiempo de inactividad de la sesión	97. ¿Se suspenden en el Sivigila las secciones inactivas?		**X**		
A.11.5.6	Limitación del tiempo de conexión.	98. ¿Una vez en el sistema, se utilizan restricciones en los tiempos de conexión?		**X**		El tiempo de conexión de cada usuario en el Sivigila depende de ellos

A.11 CONTROL DE ACCESO				
A.11.6 Control de acceso a las aplicaciones y a la información Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.				
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**	

			SI	NO	NA	
A.11.6.1	Restricción de acceso a la información.	99. ¿Existen políticas de control de acceso?		**X**		
		100. ¿Se cumple esta política si la hay?			**X**	
A.11.6.2	Aislamiento de sistemas sensibles.	101. ¿Se tiene al Sivigila como un sistemas sensible?		**X**		
		102. ¿Está el Sivigila en un entorno aislado?		**X**		

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	15	Duración	3 días
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.12.2 Procesamiento correcto en las aplicaciones

Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.12.2.1	Validación de los datos de entrada.	103. ¿Se hacen validaciones de datos de entrada en el Sivigila?	X			
A.12.2.2	Control de procesamiento interno.	104. ¿Están incorporadas verificaciones de validación contra errores de procesamiento en el Sivigila?	X			
A.12.2.3	Integridad del mensaje.	105 ¿Existen requisitos para proteger la integridad de los mensajes emitidos por el Sivigila?		X		
		106. ¿Existen controles adecuados para tratar un caso de mensaje errado?		X		
A.12.2.4	Validación de los datos de salida.	107. ¿Se validan los datos de salida en el Sivigila?	X			

A.12.3 Controles criptográficos Objetivo*:* proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.12.3.1	Política sobre el uso de controles criptográficos.	108. ¿Hay controles criptográficos en la entidad?		**X**		Este tipo de controles se ignoran en la entidad
		109. ¿Existe alguna política para estos controles?			**X**	
A.12.3.2	Gestion de llaves.	110. ¿Existe un sistema de gestión de llaves en la alcaldía?		**X**		Son términos desconocidos para los funcionarios de la entidad
A.12.4 Seguridad de los archivos del sistema Objetivo: garantizar la seguridad de los archivos del sistema.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.12.4.1	Control del software operativo.	111. ¿En los equipos donde se trabaja con el Sivigila, se controla la instalación de software?		**X**		
A.12.4.2	Protección de los datos de prueba del sistema.	112. ¿Existe algún procedimiento para la selección de datos de pruebas para el Sivigila?		**X**		
		113. ¿Se protegen estos datos ya una vez seleccionados?		**X**		
A.12.4.3	Control de acceso al código fuente de los programas	114. ¿En la entidad tiene acceso al código fuente del Sivigila?		**X**		

		115. ¿Si la entidad tiene acceso al código fuente del Sivigila se restringe la posibilidad de tenerlo?			**X**	
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	116. ¿Si hay cambio de sistema operativo en los equipos que trabajan con el Sivigila este se somete a prueba una vez terminado el cambio?	**X**			Siempre que se dan cambios en los equipos donde se trabaja con el Sivigila este se prueba
A.12.5.4	Fuga de información	117. ¿Hay procedimientos para controlar la fuga de información en el Sivigila?		**X**		
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.12.6.1	Control de vulnerabilidades técnicas	118. ¿Se tiene información sobre vulnerabilidades técnicas que pueda tener el Sivigila?		**X**		La seguridad de la información en la entidad es una tema que lastimosamente no se trata
A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN						

A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.13.1.2	Reporte sobre las debilidades de la seguridad	119. ¿Se les exige a los usuarios del Sivigila que reporten debilidades observadas?		X		Los funcionarios que utilizan el Sivigila ni siquiera se dan cuenta cuando el sistema falla

A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.13.2.3	Recolección de evidencia	120. ¿Alguna vez se le ha hecho seguimiento a un usuario del Sivigila?		X		
		121. ¿Se ha recolectado evidencia en una situación de seguimiento?			X	En la entidad no se sigue ni se cuida el manejo de la información

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO LISTA DE CHEQUEO				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :		**A.15 CUMPLIMIENTO**	
	Objetivo de lista de chequeo.			
Lista de chequeo	Numero	16	Duración	1 día
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico

Objetivo*:* asegurar que los sistemas cumplen con las normas y políticas de seguridad de la alcaldía de San Andrés de Tumaco.

ID CONTROL	NOMBRE CONTROL	PREGUNTA	CUMPLIMIENTO			OBSERVACION
			SI	NO	NA	
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	122. ¿La directora de epidemiologia área donde funciona el Sivigila en la secretaria de salud de la entidad garantiza que los procedimientos de seguridad se cumplan?		X		Para la funcionaria es tarea principal en el Sivigila reportar eventos referidos a la salud del
A.15.2.2	Verificación del cumplimiento técnico.	123. ¿Se verifica si las políticas de seguridad si las hay se cumplen en el entorno del Sivigila?		X		Porque no se tiene ninguna política de seguridad
A.15 CUMPLIMIENTO						
A.15.3 Consideraciones de la auditoría de los sistemas de información Objetivo*:* maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.						
ID CONTROL	**NOMBRE CONTROL**	**PREGUNTA**	**CUMPLIMIENTO**			**OBSERVACION**
			SI	**NO**	**NA**	
A.15.3.1	Controles de auditoría de los sistemas de información.	124. ¿Al Sivigila se le han hecho auditorias?		X		Este es el primer procedimiento de evaluación al funcionamiento, entorno tratamiento de la información
		125. ¿Se han planificado requisitos de auditoria al Sivigila?		X		No se han hecho de ningún tipo en la
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	126. ¿Se protege el acceso a herramientas de auditorías hechas al Sivigila si las hay?			X	

Anexo 2. Entrevista

<table>
<tr><td colspan="5">UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
FACULTAD DE INGENIERIA
PROGRAMA DE SISTEMAS
ALCALDIA DE SAN ADRES DE TUMACO
ENTREVISTA A JEFE DE EPIDEMIOLOGIA</td><td>UNIVERSIDAD DE NARIÑO.</td></tr>
<tr><td rowspan="2">Programa de formación:
Ingeniería de Sistemas</td><td colspan="2">Control :</td><td colspan="2"></td></tr>
<tr><td colspan="2">Objetivo de entrevista.</td><td colspan="2">Establecer contacto directo con la Jefe de Epidemiologia de la secretaria de salud</td></tr>
<tr><td>Entrevista</td><td>Numero</td><td>1</td><td>Duración</td><td>2 horas</td></tr>
<tr><td>Nombre auditor</td><td colspan="4">Yurani Alejandra Landázuri Guevara</td></tr>
<tr><td>Nombre asesor</td><td colspan="4">José Javier Villalba Romero</td></tr>
</table>

¿Es usted funcionaria activa de la alcaldía de Tumaco?

_____

¿Qué cargo desempeña actualmente?

_____

_____

¿En el entorno de su trabajo y desarrollo de sus funciones conoce usted o ha llegado a escuchar el término Políticas de seguridad de la información? Si lo conoce describa por favor según su experiencia a que se refiere.

_____

¿Tiene usted conocimiento de algún proceso de auditoría informática que se haya desarrollado en la entidad, dependencia o en el sistema de información Sivigila?

_____

¿Podría describir que funciones desarrolla usted en el sistema de información Sivigila?

_____

_____

¿Según su experiencia en el manejo del sistema de información Sivigila como califica usted la complejidad de este?

Fácil___ Media__ Compleja__

Explique por favor el porqué de su respuesta

_____

_____

¿Es usted consiente del grado de importancia de la información que se maneja en el Sivigila?

_____

¿Considera usted que la información manejada en el Sivigila tiene un grado de importancia como para ser aislada? Justifique su respuesta.

_____
_____

¿Además del manual general para usuarios que proporciona el desarrollador del Sivigila manejan en la secretaria de salud otro tipo de manuales del sistema de información? ¿Si los hay puede usted mencionarlos?

_____
_____

¿Manejan en la secretaria de salud o usted en forma personal documentos de novedades del Sivigila? Si los maneja menciónelos por favor

_____
_____

¿Desde el momento que usted inicio funciones en el Sivigila este ha tenido fallas?

_____

¿Maneja usted documento de fallas o avances del Sivigila?

_____

¿Si maneja documentos de fallas es por iniciativa propia o por mandato de la entidad?

_____

¿Puede usted describir el proceso de recolección de la información que es procesada en el Sivigila?

_____
_____
_____

¿Cuáles son las unidades que le reportan información del Sivigila a usted y que días lo hacen?

_____
_____

¿Qué días reporta usted información del Sivigila y a que unidades reporta?

_____
_____

¿Maneja usted copias de seguridad de la información del Sivigila?

_____

¿Puede usted mencionar donde guarda las copias de seguridad de la información del Sivigila?

_____

¿Guarda copias de la información del Sivigila en su correo electrónico? ¿Si lo hace es por decisión personal o a petición de la entidad?

_____
_____

¿Considera usted necesario auditar un sistema de información como el Sivigila? Justifique su respuesta

_____
_____

¿Está de acuerdo con la práctica de cuidar la información emitida por el Sivigila o cualquier sistema de información de la entidad? Justifique su respuesta

_____
_____

Muchas gracias por su ayuda

_____	_____
Yurani Landázuri Guevara	Yamileth Ramos
Auditora	Jefe Epidemiologia

UNIVERSIDAD DE NARIÑO SAN JUAN DE PASTO FACULTAD DE INGENIERIA PROGRAMA DE SISTEMAS ALCALDIA DE SAN ADRES DE TUMACO ENTREVISTA A COORDINADOR DE SISTEMAS				UNIVERSIDAD DE NARIÑO.
Programa de formación: Ingeniería de Sistemas	Control :			
	Objetivo de lista de entrevista			
entrevista	Numero	2	Duración	2 horas
Nombre auditor	Yurani Alejandra Landázuri Guevara			
Nombre asesor	José Javier Villalba Romero			

¿Es usted funcionario activo de la alcaldía de Tumaco?

_____

¿Qué cargo desempeña actualmente?

_____

¿Cómo coordinador del área de sistemas tiene usted conocimiento de la existencia del área de control interno en la entidad?

_____

¿Si existe el área de control interno en la entidad conoce usted si en el grupo de trabajo está incluido un ingeniero de sistemas?

_____

¿Conoce usted las funciones que esta área desarrolla en la entidad?

_____

_____

_____

¿Tiene usted conocimiento de algún proceso de auditoria informática desarrollada en la entidad?

_____

¿Tiene conocimiento de los sistemas de información que se manejan en la entidad? Menciónelos por favor

_____

_____

_____
_____

¿Es usted el responsable de la configuración de los sistemas de información que se manejan en la entidad o es contratado a terceros?

_____
_____

¿Ha configurado usted algún sistema de información en la entidad? Mencione cuales.

_____
_____

¿Conoce el sistema de información Sivigila, sabe qué tipo de información procesa para la entidad?

_____
_____

¿Conoce usted si existe alguna política de seguridad de la información dada por la administración para la entidad? Si la hay menciónela por favor

_____
_____

¿Sabe usted si en la entidad existe un SGSI? ¿Si existe se cumple?

_____
_____

¿Cómo ingeniero de sistemas cree usted que la entidad contempla la seguridad de la información?

_____

¿Qué piensa usted de cuidar la información en una entidad como la Alcaldía de Tumaco?

_____
_____

¿Considera necesario auditar un lugar como la entidad? ¿Por qué?

_____
_____

Muchas gracias por su ayuda

_____ _____

Yurani Landázuri Guevara Auditora	Javier Mindineros Jefe Epidemiologia

Anexo 3. Hoja de no conformidades.

HOJA DE NO CONFORMIDADES (1/139) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:1	PREGUNTA: 1	CCP _____ CCA _____	N*. 1
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA Actualmente en la alcaldía de Tumaco no se tiene una política de seguridad de la información, que tenga como objetivo el cuidado de los sistemas de información entre ellos el Sivigila.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Es necesario que en la alcaldía de Tumaco se cree y se comunique para su aplicación una política de seguridad de la información y que la administración muestre su interés por la mejora en el cuidado de la información.			

HOJA DE NO CONFORMIDADES (1/139) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 4	CCP _____ CCA _____	N*. 2
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay existe un apoyo de la administracion por la seguridad de la información que se maneja en la alcaldía			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Es necesario que en la administracion de la alcaldía de Tumaco se interese por cuidar la información que se obtiene de los sistemas de información entre ellos el Sivigila y demás entes que funcionen dentro de la entidad.			

HOJA DE NO CONFORMIDADES (1/139) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 5	CCP _____ CCA _____	N*.3
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se desarrollan dentro de la alcaldía de Tumaco actividades para la seguridad de la información.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
En las instalaciones de la alcaldía o en el caso mínimo desde las dependencias es necesario que se desarrollen actividades que sean orientadas a buscar cuidar la información que se maneja en el día a día de la entidad.			

HOJA DE NO CONFORMIDADES (1/140) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 6	CCP _____ CCA _____	N*. 4
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA En las dependencias de la alcaldía de Tumaco en este caso especial la secretaria de salud no existe coordinación para alguna actividad para la seguridad de información			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Coordinar actividades para la seguridad de la información desde la secretaria de salud de Tumaco siendo esta un brazo importante para la alcaldía, haciendo estas actividades como iniciativa propia.			

HOJA DE NO CONFORMIDADES (1/140) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 7	CCP _____ CCA _____	N*. 5
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA Como no se tienen identificadas actividades para la seguridad de la información en la secretaria de salud no hay asignación de responsabilidades para la misma			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Una vez identificadas las actividades para la seguridad de la información en la secretaria de salud, asignar responsabilidades para el cumplimiento de las mismas.			

HOJA DE NO CONFORMIDADES (1/140) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 9	CCP _____ CCA _____	N*. 6
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No existe un acuerdo formal de confidencialidad para la información que maneja el Sivigila.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Desarrollar y publicar un acuerdo formal de confidencialidad para proteger la información que se obtiene del Sivigila .			

HOJA DE NO CONFORMIDADES (1/141) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 11	CCP _____ CCA _____	N*. 7
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA En caso de robo de la información dada por el Sivigila no se tiene contacto con las autoridades pertinentes.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Establecer y mantener contactos con autoridades pertinentes en caso de robo de información.			

HOJA DE NO CONFORMIDADES (1/141) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:2	PREGUNTA: 12	CCP _____ CCA _____	N*. 8
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay contacto con grupos especializados en seguridad de la información.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
La secretaria de salud de la alcaldía de Tumaco debe establecer contacto con grupos especializados para la seguridad de la información que se obtiene del Sivigila, incluso de los desarrolladores del mismo sistema debe haber alguien que este destinado para esta actividad.			

HOJA DE NO CONFORMIDADES (1/141) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:3	PREGUNTA: 14	CCP _____ CCA _____	N*. 9
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se ha identificado riesgos a los que están expuestos la información y activos relacionados con el Sivigila.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Identificar riesgos a los que pueden estar expuestos la información y activos relacionados con el Sivigila.			

HOJA DE NO CONFORMIDADES (1/142) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:4	PREGUNTA: 16	CCP _____ CCA _____	N*. 10
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se encontró al Sivigila en el inventario de la alcaldía ni como sistema de información y tampoco como aplicación.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Incluir al Sivigila en el inventario de la alcaldía.			

HOJA DE NO CONFORMIDADES (1/142) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:5	PREGUNTA: 20	CCP _____ CCA _____	N*. 11
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA Aunque de cierta forma la información obtenida del Sivigila se clasifica, dicha clasificación no es según lo sensible que sea esta para la alcaldía.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Clasificar la información obtenida del Sivigila según su sensibilidad.			

HOJA DE NO CONFORMIDADES (1/142) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:6	PREGUNTA: 23	CCP _____ CCA _____	N*. 12
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se verifica antecedentes para la contratación de personal en la alcaldía			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Verificar antecedentes antes de hacer efectiva una nueva contratación en la entidad.			

HOJA DE NO CONFORMIDADES (1/143) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:7	PREGUNTA: 26	CCP _____ CCA _____	N*. 13
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA El personal que trabaja con el Sivigila no recibe información sobre los procedimientos de la alcaldía.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Educar al personal sobre los procedimientos de la entidad y sobre todo con aquellos que tenga que ver con el Sivigila.			

HOJA DE NO CONFORMIDADES (1/143) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:7	PREGUNTA: 27	CCP _____ CCA _____	N*. 14
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay un proceso disciplinario en caso de robo de información dada por el Sivigila.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Crear y comunicar un proceso disciplinaron en caso de robo de información dada por el Sivigila o cualquier sistema de la entidad			

HOJA DE NO CONFORMIDADES (1/143) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:7	PREGUNTA: 28	CCP _____ CCA _____	N*. 15
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No están enterados los empleados que manejan información del Sivigila de responsabilidades de no divulgación en caso de liquidar laborares en la entidad			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	

Informar a los empleados relacionados con el Sivigila de responsabilidades de no divulgación de información del sistema en caso de terminar relaciones con la entidad.

HOJA DE NO CONFORMIDADES (1/144) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:8	PREGUNTA: 31	CCP _____ CCA _____	N*. 16
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay perímetro de seguridad en el área donde se consolidad la información del Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Trazar un perímetro de seguridad en el área de trabajo del Sivigila.			

HOJA DE NO CONFORMIDADES (1/144) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:8	PREGUNTA: 32	CCP _____ CCA _____	N*. 17
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay control de acceso no autorizado			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Controlar el acceso no autorizado de personal a el área donde se procesa la información del Sivigila			

HOJA DE NO CONFORMIDADES (1/144) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:8	PREGUNTA: 33	CCP _____ CCA _____	N*. 18
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay protección contra amenazas ambientales en la secretaria de salud			

DESCRIPCION DE ACCION CORRECTIVA	**FECHA** 15/09/ 2015 **HORA** 9:00 AM
Diseñar protecciones contra amenazas externas o ambientales	

HOJA DE NO CONFORMIDADES (1/145) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:8	PREGUNTA: 34	CCP _____ CCA _____	N*. 19
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se identifica el área donde se maneja la información del Sivigila como área segura.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Identificar el área donde se hace el consolidado de la información del Sivigila como área segura.			

HOJA DE NO CONFORMIDADES (1/145) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:9	PREGUNTA: 35	CCP _____ CCA _____	N*. 20
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA Mala ubicación de los equipos donde se maneja información del Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Ubicar los equipos donde se maneja información del Sivigila del modo adecuado.			

HOJA DE NO CONFORMIDADES (1/145) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:10	PREGUNTA: 41	CCP _____ CCA _____	N*. 21
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	

DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay seguimiento al funcionamiento del Sivigila	
DESCRIPCION DE ACCION CORRECTIVA	**FECHA** 15/09/ 2015 **HORA** 9:00 AM
Hacer seguimiento al funcionamiento del Sivigila sin importar su resultado.	

HOJA DE NO CONFORMIDADES (1/146) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:10	PREGUNTA: 42	CCP _____ CCA _____	N*. 22
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA Se actualiza la información y la App del Sivigila pero no hay criterios formales de aceptación de este proceso			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Además de actualizar la App y la información del Sivigila establecer criterios de aceptación para los usuarios.			

HOJA DE NO CONFORMIDADES (1/146) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:11	PREGUNTA: 43	CCP _____ CCA _____	N*. 23
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay controles de detección, protección y recuperación contra códigos maliciosos en el entorno del Sivigila.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Diseñar e implementar controles de detección, protección y recuperación contra códigos maliciosos.			

HOJA DE NO CONFORMIDADES (1/146) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:11	PREGUNTA: 45	CCP _____ CCA _____	N*. 24

REPORTE DE NO CONFORMIDAD	**FECHA** 15/09/ 2015 **HORA** 9:00 AM
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay políticas de seguridad para el uso de códigos móviles.	
DESCRIPCION DE ACCION CORRECTIVA	**FECHA** 15/09/ 2015 **HORA** 9:00 AM
Crear y comunicar políticas de seguridad para el uso de códigos móviles en los equipos donde se trabaja con el Sivigila y otros sistemas de información si es posible.	

HOJA DE NO CONFORMIDADES (1/147) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:11	PREGUNTA: 48	CCP _____ CCA _____	N*. 25
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se prueban las copias de seguridad hechas del Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Establecer tiempos y espacios para probar las copias que se hagan del Sivigila			

HOJA DE NO CONFORMIDADES (1/147) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:11	PREGUNTA: 49	CCP _____ CCA _____	N*. 26
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA Redes de flujo de información no seguras.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Establecer criterios de control y protección para las redes de flujo de información.			

HOJA DE NO CONFORMIDADES (1/147) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD

GUIA:11	PREGUNTA: 50	CCP _____ CCA _____	N*. 27
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No hay acuerdos de servicios de las redes usadas por el Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Establecer acuerdos sobre uso de redes usadas por el Sivigila, y en el mejor de los casos de todos los sistemas de información que se manejan en la entidad.			

HOJA DE NO CONFORMIDADES (1/148) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:12	PREGUNTA: 57	CCP _____ CCA _____	N*. 28
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No existen controles formales para el intercambio de información relacionadas con el Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Diseñar controles que permitan el intercambio formal de la información relacionada con el Sivigila			

HOJA DE NO CONFORMIDADES (1/148) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:12	PREGUNTA: 59	CCP _____ CCA _____	N*. 29
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No existe protección para los medios que contiene información del Sivigila contra acceso no autorizado.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Diseñar estrategias de protección para el cuidado de los medios que contiene información del Sivigila			

HOJA DE NO CONFORMIDADES (1/148) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:12	PREGUNTA: 60	CCP _____ CCA _____	N*. 30
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No existe cuidado especial para la información del Sivigila que se encuentra en mensajería electrónica.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Crear una en cuenta electrónica que no se la de la UNM del Sivigila para guardar la información que ese obtiene de este y mantener el debido cuidado.			

HOJA DE NO CONFORMIDADES (1/149) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:13	PREGUNTA: 62	CCP _____ CCA _____	N*. 31
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se han hecho auditorias de ningún tipo en la alcaldía			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Plantear tiempos y responsables para llevar a cabo el proceso de auditoria en la alcaldía y llevar su registro.			

HOJA DE NO CONFORMIDADES (1/149) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:13	PREGUNTA: 64	CCP _____ CCA _____	N*. 32
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se hacen monitoreo al uso del Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Realizar monitoreo al uso del Sivigila y documentarlo.			

HOJA DE NO CONFORMIDADES (1/149) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 15/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:13	PREGUNTA: 70	CCP _____ CCA _____	N*. 33
REPORTE DE NO CONFORMIDAD		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se lleva registro de fallas del Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 15/09/ 2015 **HORA** 9:00 AM	
Llevar registro de fallas posibles del Sivigila y hacer su posterior análisis.			

HOJA DE NO CONFORMIDADES (1/150) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:14	PREGUNTA: 76	CCP _____ CCA _____	N*. 33
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se revisa los derechos de usuarios del Sivigila porque no se tiene ninguno identificado			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
Identificar los derechos de usuarios del Sivigila, comunicarlos y hacerle la revisión pertinente			

HOJA DE NO CONFORMIDADES (1/150) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:14	PREGUNTA: 80	CCP _____ CCA _____	N*. 34
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No existe política de escritorio despejado en los equipos relacionados con el Sivigila.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
Crear políticas de escritorio despejado en los equipos relacionados con el Sivigila.			

HOJA DE NO CONFORMIDADES (1/150) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:14	PREGUNTA: 85	CCP _____ CCA _____	N*. 35
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se controla el puerto por donde el Sivigila escucha.			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
Establecer controles para el puerto por donde el Sivigila escucha.			

HOJA DE NO CONFORMIDADES (1/151) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:14	PREGUNTA: 99	CCP _____ CCA _____	N*. 37
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se tiene políticas de control de acceso			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
Crear y comunicar a los funcionarios de la entidad una política de control de acceso			

HOJA DE NO CONFORMIDADES (1/151) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:14	PREGUNTA: 101	CCP _____ CCA _____	N*. 38
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se clasifica al Sivigila como sistema de información sensible.			

DESCRIPCION DE ACCION CORRECTIVA	**FECHA** 16/09/ 2015 **HORA** 9:00 AM
Clasificar al Sivigila como sistema sensible.	

HOJA DE NO CONFORMIDADES (1/151) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:14	PREGUNTA: 102	CCP _____ CCA _____	N*. 39
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se tiene a los equipos relacionados con el Sivigila en un entorno aislado			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
Tener a los equipos relacionados con el Sivigila en entorno aislado			

HOJA DE NO CONFORMIDADES (1/152) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:15	PREGUNTA: 118	CCP _____ CCA _____	N*. 40
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se tiene documentos de fallas técnicas del Sivigila			
DESCRIPCION DE ACCION CORRECTIVA		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	
Registrar y comunicar cualquier falla de tipo técnico del Sivigila			

HOJA DE NO CONFORMIDADES (1/152) REPORTE NC CIUDAD: San Andrés de Tumaco
FECHA 16/09/2015 AUDITOR: Yurani Landázuri Guevara CODIGO: 1087189396

FORMATO DE REPORTE DE NO CONFORMIDAD			
GUIA:16	PREGUNTA: 125	CCP _____ CCA _____	N*. 41
REPORTE DE NO CONFORMIDAD		**FECHA** 16/09/ 2015 **HORA** 9:00 AM	

DESCRIPCION DE LA NO CONFORMIDAD CRITICA No se ha identificado requisitos de auditoria a los sistemas de información entre ellos el Sivigila	
DESCRIPCION DE ACCION CORRECTIVA	**FECHA** 16/09/ 2015 **HORA** 9:00 AM
Identificar requisitos de auditoria para los sistemas de información entre ellos el Sivigila	

Anexo 4. Identificación de controles y objetivos de control según iso-iec/27001

A.5 POLÍTICA DE SEGURIDAD			
A.5.1 Política de seguridad de la información Objetivo: Brindar apoyo y orientación a la alcaldía con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.			
A.5.1.1	Documento de la política de seguridad de la información.	Control La alcaldía debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes	
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 Organización interna Objetivo: Gestionar la seguridad de la información dentro de la alcaldía			
A.6.1.1	Compromiso de la administration con la seguridad de la Información.	La administración debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la Información	
A.6.1.2	Coordinación de la seguridad de la información.	Control Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales Pertinentes	
A.6.1.3	Asignación de Responsabilidades para la Seguridad de la información.	Control Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la Información.	

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Control Se debe definir e implementar un proceso de autorización de la dirección para nuevos serviciosde procesamiento de información.	
A.6.1.5	Acuerdos sobre Confidencialidad	Control Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	
A.6.1.6	Contacto con las autoridades	Control Se deben mantener contactos apropiados con las autoridades pertinentes.	
A.6.1.7	Contacto con grupos de interés especiales	Control Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.	
A.6.1.8	Revisión independiente de la seguridad de la información.	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.	
A.6.2 Partes externas Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la alcaldía a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.			
A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	Control Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar elacceso.	
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Control Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización	

A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Control Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la alcaldia, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad	

A.7 GESTIÓN DE ACTIVOS			
A.7.1 Responsabilidad por los activos Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.			
A.7.1.1	Inventario de activos	Control Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.	
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad"[3)] de una parte designada de la alcaldia	
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	
A.7.2 Clasificación de la información Objetivo: asegurar que la información recibe el nivel de protección adecuado.			
A.7.2.1	Directrices de clasificación	Control La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la alcaldía.	
A.7.2.2	Etiquetado y manejo de información	Control Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la alcaldía	

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS	
A.8.1 Antes de la contratación laboral Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.	

A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la alcaldía	
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.1.2	Selección	Control Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos	
A.8.1.3	Términos y condiciones laborales.	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la alcaldía con relación a la seguridad de la información.	
A.8.2 Durante la vigencia de la contratación laboral Objetivo*:* asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la alcaldía en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.			
A.8.2.1	Responsabilidades de la administracion	Control La administración debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la alcaldía.	
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Control Todos los empleados de la alcaldía y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la alcaldía, según sea pertinente para sus funciones laborales.	

A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.3 Terminación o cambio del contratación laboral Objetivo: asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la alcaldía o cambian su contrato laboral de forma ordenada..			
A.8.3.1	Responsabilidades en la terminación	Control Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.	
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la alcaldía que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	
A.8.3.3	Retiro de los derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.1 Áreas seguras Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la alcaldia.			
A.9.1.1	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información	
A.9.1.2	Controles de acceso físico.	Control Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	Control Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	

A.9.1.4	Protección contra amenazas externas y ambientales.	Control Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural oartificial.	
A.9.1.5	Trabajo en areas seguras.	Control Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	
A.9.1.6	Áreas de carga, despacho y acceso público	Control Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.	
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.2 Seguridad de los equipos Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la alcaldía.			
A.9.2.1	Ubicación y protección de los equipos.	Control Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado	
A.9.2.2	Servicios de suministro	Control Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	
A.9.2.3	Seguridad del cableado.	Control El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegido contra interceptaciones o daños	
A.9.2.4	Mantenimiento de los equipos.	Control Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	
A.9.2.5	Seguridad de los las equipos fuera de instalaciones.	Control Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la alcaldía.	
A.9.2.6	Seguridad en la reutilización de la eliminación d e equipos.	Control Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	

A.9.2.7	Retiro de activos	Control Ningún equipo, información ni software se deben retirar sin autorización previa.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.1 Procedimientos operacionales y responsabilidades Objetivo*:* asegurar la operación correcta y segura de los servicios de procesamiento de información.			
A.10.1.1	Documentación de los procedimientos de operación	Control Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	
A.10.1.2	Gestion del cambio.	Control Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.1.3	Distribución de Funciones.	Control Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la alcaldía.	
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Control Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	
A.10.2 Gestión de la prestación del servicio por terceras partes Objetivo: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por tercera spartes.			
A.10.2.1	Prestación del servicio	Control Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Control Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	Control Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	

A.10.3 Planificación y aceptación del sistema Objetivo: minimizar el riesgo de fallas de los sistemas.			
A.10.3.1	Gestion de l	Control Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	
A.10.3.2	Aceptación del sistema.	Control Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.4 Protección contra códigos maliciosos y móviles Objetivo: proteger la integridad del software y de la información.			
A.10.4.1	Controles contra códigos maliciosos.	Control Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	
A.10.5 Respaldo Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.			
A.10.5.1	Respaldo de l	Control Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	
A.10.6 Gestión de la seguridad de las redes Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.			
A.10.6.1	Controles de las redes.	Control Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	

A.10.6.2	Seguridad de los servicios de la red.	Control En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la alcaldía o se contratan externamente.	
A.10.7 Manejo de los medios Objetivo*:* evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades de la alcaldía.			
A.10.7.1	Gestión de los medios removibles	Control Se deben establecer procedimientos para la gestión de los medios removibles	
A.10.7.2	Eliminación de los medios.	Control Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.7.3	Procedimientos para el manejo de la información.	Control Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	
A.10.7.4	Seguridad de la documentación del sistema.	Control La documentación del sistema debe estar protegida contra el acceso no autorizado.	
A.10.8 Intercambio de la información Objetivo*:* mantener la seguridad de la información y del software que se intercambian dentro de la alcaldía y con cualquier entidad externa.			
A.10.8.1	Políticas y procedimientos para el intercambio de información	Control Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	
A.10.8.2	Acuerdos para el intercambio	Control Se deben establecer acuerdos para el intercambio de la información y del software entre la alcaldía y partes externas.	
A.10.8.3	Medios físicos en tránsito.	Control Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la alcaldía.	
A.10.8.4	Mensajería electronica.	Control La información contenida en la mensajería electrónica debe tener la protección adecuada	

A.10.8.5	Sistemas de información de la alcaldía.	Control Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información de la alcaldía.	
A.10.9 Servicios de comercio electrónico Objetivo: garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.			
A.10.9.1	Comercio electrónico	Control La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.	
A.10.9.2	Transacciones en línea	Control La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.9.3	Información disponible al público	Control La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	
A.10.10 Monitoreo Objetivo: detectar actividades de procesamiento de la información no autorizadas.			
A.10.10.1	Registro de auditorías	Control Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	
A.10.10.2	Monitoreo del uso del sistema	Control Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad	
A.10.10.3	Protección de la información del registro	Control Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	
A.10.10.4	Registros del administrador y del operador	Control Se deben registrar las actividades tanto del operador como del administrador del sistema.	
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	

A.10.10.6	Sincronización de relojes	Control Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la alcaldía o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	
A.11 CONTROL DE ACCESO			
A.11.1 Requisito del negocio para el control de acceso Objetivo: controlar el acceso a la información.			
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos de la alcaldía y de la seguridad para el acceso	
A.11.2 Gestión del acceso de usuarios Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.			

A.11 CONTROL DE ACCESO			
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	Control El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado	
A.11.4.5	Separación en las redes.	Control En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	
A.11.4.6	Control de conexión a las redes.	Control Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la alcaldía, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación de la alcaldía (véase el numeral 11.1).	
A.11.4.7	Control de enrutamiento en la red.	Control Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.	
A.11.5 Control de acceso al sistema operativo Objetivo: evitar el acceso no autorizado a los sistemas operativos.			
A.11.5.1	Procedimientos de ingreso seguros	Control El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	

A.11.5.2	Identificación y autenticación de usuarios.	Control Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	
A.11.5.3	Sistema de gestión	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	
A.11.5.4	Uso de las utilidades	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	
A.11.5.5	Tiempo de inactividad de la sesión	Control Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.	
A.11.5.6	Limitación del tiempo de conexión.	Control Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	
A.11 CONTROL DE ACCESO			
A.11.6 Control de acceso a las aplicaciones y a la información Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.			
A.11.6.1	Restricción de acceso a la información.	Control Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	
A.11.6.2	Aislamiento de sistemas sensibles.	Control Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	
A.11.7 Computación móvil y trabajo remoto Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móvil y de trabajo remoto.			
A.11.7.1	Computación y comunicaciones móviles.	Control Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	

A.11.7.2	Trabajo remoto.	Control Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.1 Requisitos de seguridad de los sistemas de información Objetivo*:* garantizar que la seguridad es parte integral de los sistemas de información.			
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Control Las declaraciones sobre los requisitos de la alcaldía para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.			
A.12.2.1	Validación de los datos de entrada.	Control Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados	
A.12.2.2	Control de procesamiento interno.	Control Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.2.3	Integridad del mensaje.	Control Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	
A.12.2.4	Validación de los datos de salida.	Control Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias	
A.12.3 Controles criptográficos Objetivo*:* proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.			

A.12.3.1	Política sobre el uso de controles criptográficos.	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	
A.12.3.2	Gestión de llaves.	Control Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la alcaldia.	
A.12.4 Seguridad de los archivos del sistema Objetivo: garantizar la seguridad de los archivos del sistema.			
A.12.4.1	Control del software operativo.	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	
A.12.4.2	Protección de los datos de prueba del sistema.	Control Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse	
A.12.4.3	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.	
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.			
A.12.5.1	Procedimientos de control de cambios.	Control Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Control Cuando se cambian los sistemas operativos, las aplicaciones críticas para la alcaldía se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la alcaldía.	
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Control Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	
A.12.5.4	Fuga de información	Control Se deben evitar las oportunidades para que se produzca fuga de información.	

A.12.5.5	Desarrollo de software contratado externamente	Control La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.			
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	
A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN			
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.			
A.13.1.1	Reporte sobre los eventos de seguridad de la información	Control Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	
A.13.1.2	Reporte sobre las debilidades de la seguridad	Control Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.			
A.13.2.1	Responsabilidades y Procedimientos	Control Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Control Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	
A.15 CUMPLIMIENTO			
A.15.1 Cumplimiento de los requisitos legales Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.			

A.15.1.1	Identificación de la legislación aplicable.	Control Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la alcaldía para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la alcaldía	
A.15.1.2	Derechos de propiedad intelectual (DPI).	Control Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	
A.1.5.1.3	Protección de los registros de la alcaldía.	Control Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	
A.15.1.4	Protección de los datos y privacidad de la información personal.	Control Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Control Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	
A.15.1.6	Reglamentación de los controles criptográficos.	Control Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	
A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico Objetivo*:* asegurar que los sistemas cumplen con las normas y políticas de seguridad de la alcaldía.			
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	Control Los jefes deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.	
A.15.2.2	Verificación del cumplimiento técnico.	Control Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.	
A.15 CUMPLIMIENTO			

A.15.3 Consideraciones de la auditoría de los sistemas de información Objetivo*:* maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.			
A.15.3.1	Controles de auditoría de los sistemas de información.	Control Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos de la alcaldía.	
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Control Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.	