AUDITORÍA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN “GESTIÓN INTEGRADA DE BIENESTAR SOCIAL” EN LA DIRECCIÓN TERRITORIAL DE SALUD DE CALDAS

JAIME ALBERTO PINEDA RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
LA DORADA CALDAS,
2017

AUDITORÍA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN “GESTIÓN INTEGRADA DE BIENESTAR SOCIAL” EN LA DIRECCIÓN TERRITORIAL DE SALUD DE CALDAS

JAIME ALBERTO PINEDA RAMIREZ

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Mariano Esteban Romero Torres
Director de proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
LA DORADA CALDAS,
2017

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

La Dorada, Caldas, octubre de 2017

AGRADECIMIENTOS

En primer lugar a Dios por guiarme en cada proyecto de superación emprendido en mi vida; en segundo lugar a mis padres Juan Francisco y Rosa Amelia, quienes me han enseñado que el estudio será siempre el instrumento necesario para la superación personal y laboral, a mi esposa Sandra quien siempre me ha apoyado en las metas propuestas y a mis hermanos Francisco y Diego a quiénes incentivo a seguir estudiando y nunca desfallecer en los objetivos.

Por ultimo a mis tutores y directores quienes han dado lo máximo en sus enseñanzas y aprendizajes brindando siempre un ambiente de apoyo y entusiasmo.

Jaime Alberto Pineda Ramírez

CONTENIDO

		pág.
GLOSARIO		12
INTRODUCCIÓN		15
1.	EL PROBLEMA	17
1.1	DESCRIPCIÓN DEL PROBLEMA	17
1.2	FORMULACIÓN DEL PROBLEMA	18
1.3	OBJETIVOS	18
1.3.1	General	18
1.3.2	Específicos	18
1.4	JUSTIFICACIÓN	19
1.5	ALCANCE Y DELIMITACIÓN	19
2.	MARCO DE REFERENCIA	21
2.1	ANTECEDENTES	21
2.2	MARCO TEÓRICO CONCEPTUAL	22
2.2.1	Seguridad informática	22
2.2.2	Auditoría	22
2.2.3	Auditoría informática	22
2.2.4	Auditoría de sistemas	23
2.2.5	Auditoría interna	23
2.2.6	Auditoría externa	23
2.2.7	Plan de auditoría	24
2.2.8	Sistema de gestión	24
2.2.9	Metodología cuantitativa	25
2.2.10	Metodología cualitativa	25
2.2.11	Políticas de seguridad informática	26

2.2.12 Valoración del riesgo 26
2.2.13 Observatorio social 26
2.3 MARCO CONTEXTUAL 27
2.3.1 Reseña Histórica 27
2.3.2 Misión. 28
2.3.3 Visión. 28
2.3.4 Políticas de calidad. 29
2.3.5 Objetivos de calidad. 29
2.3.6 Estructura organizacional. 30
2.3.7 Referente Nacional. 30
2.4 MARCO LEGAL 31
3. METODOLOGÍA 33
3.1 TIPO DE INVESTIGACIÓN 33
3.1.1 Investigación Cuantitativa. 33
3.2 DISEÑO DE INVESTIGACIÓN 34
3.2.1 Universo y muestra. 35
3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN INFORMACIÓN 35
3.3.1 Validez. 36
3.3.2 Confiabilidad. 36
4. PRODUCTO RESULTADO A ENTREGAR 37
4.1 PLAN DE AUDITORÍA 38
4.2 DESARROLLO DE LA AUDITORÍA 44
4.2.1 Reunión de inicio 45
4.2.2 Solicitud de información 46
4.2.3 Determinación de la muestra de auditoría 50

4.2.4 Papeles de trabajo 51

4.2.5 Diseño de las pruebas de auditoría 51

4.2.6 Desarrollo de observaciones 55

4.3 INFORME FINAL DE AUDITORÍA 80

5. CONCLUSIONES 103

6. RECOMENDACIONES 104

7. BIBLIOGRAFÍA 105

ANEXOS 108

LISTAS DE FIGURAS

pág.

Figura 1 Estructura Organizacional 30
Figura 2. Cifrado de usuario 53
Figura 3. Información de usuario 53
Figura 4. Parametrización Municipios 54
Figura 5. Parametrización de BD. 55
Figura 6. Árbol de Directorio 56
Figura 7. Archivos 56
Figura 8. Ruta 57
Figura 9. Información del ataque 57
Figura 10. Ataque Sistema 58
Figura 11. Roles usuarios 59
Figura 12. Privilegios de usuarios 59
Figura 13. Parametrización de usuarios 60
Figura 14. Envío al correo del usuario 61
Figura 15 Generación reporte bitácora 61
Figura 16 Reporte de bitácora 62
Figura 17. Usuario sin actividad 63
Figura. 18 Criterios de búsqueda 64
Figura 19. Reporte de búsqueda 65
Figura 20. Selección de campos a exportar 66
Figura 21. Reporte en Excel 67
Figura 22. Datos básicos persona 68
Figura 23. Usuario Jaime Pineda 75
Figura 24. Bloque página Facebook 76
Figura 25. Correo usuario Jaime Pineda 76
Figura 26. Antivirus ejecutándose. 77
Figura 27. Solicitud usuario y contraseña 77
Figura 28. Usuario Jaime Pineda 78
Figura 29. Usuario Carmenza Osorio 78
Figura 30. Unidades Extraíbles. 79
Figura 31. Página de YouTube. 79
Figura 32. Información del árbol de directorios 82
Figura 33. Archivos árbol de directorio 82
Figura 34. Ubicación árbol de directorios 83
Figura 35. Información sobre el administrador 83
Figura 36. Navegación en páginas que deben estar bloqueada 84
Figura 37. Información usuario aplicativo 85
Figura 38. Información enviada al correo del usuario 85
Figura 39. No se utiliza la opción de cambiar contraseña 86
Figura 40. Se utilizan correo personales y no institucionales 87
Figura 41. El aplicativo no bloquea a los usuarios inactivos 88
Figura 42. No se solicita contraseñas con niveles de seguridad 89

Figura 43. Permite exportar información sensible 90
Figura 44. Archivo que se exportan presentan información personal 91
Figura 45. Usuarios con perfil de consulta pueden exportar información personal 92
Figura 46. Usuario de consulta selecciona campos a exportar 93
Figura 47. Información personal en usuario de consulta 94
Figura 48. Aplicando método Post. 95
Figura 49. Página bloqueada desde el administrador. 96
Figura 50. Contraseña encriptada. 97
Figura 51. Opción cambiar password activada. 97
Figura 52. Requiere cambio de contraseña. 98
Figura 53. Cambiar correos personales de usuarios. 99
Figura 54. Usuario Inactivo. 99
Figura 55. Propuesta criterios para contraseñas. 100

LISTA DE CUADROS

pág.

Cuadro *1*. Marco normativo rector 31
Cuadro *2* Plan de auditoría 38
Cuadro *3* Seguridad informática DTSC 49
Cuadro *4* Seguridad informática sistema auditado 50
Cuadro *5*. Valoración política de seguridad física. 68
Cuadro 6. Valoración política de seguridad lógica. 72
Cuadro 7. Valoración uso de servicios de la Red. 73
Cuadro 8. Valoración directiva del servidor. 74
Cuadro 9 Valoración vulnerabilidad 80

LISTA DE ANEXOS

pág.

Anexo 1. Carta de aval del proyecto 108
Anexo 2. Acuerdo de Confidencialidad 109
Anexo 3. Informe vulnerabilidades 110
Anexo 4. Lista de chequeo políticas de seguridad – acceso físico 111
Anexo 5. Lista de chequeo políticas de seguridad - respaldo 112
Anexo 6. Lista de chequeo políticas derecho de autor 113
Anexo 7. Lista de chequeo políticas de seguridad – Red de datos 114
Anexo 8. Lista de chequeo políticas de seguridad – Sistema “Gestión Integrada de Bienestar Social” 115
Anexo 9. Lista de chequeo directivas de control 116
Anexo 10. Lista de chequeo directivas usuario final 117
Anexo 11. Cuestionario director sistemas TIC 118
Anexo 12. Cuestionario administrador sistemas 119
Anexo 13. Recomendación usuario 120

GLOSARIO

Amenaza Informática: Es la circunstancia que se presenta en un sistema de ser atacado o generar perdida de información bien sea por parte de delincuentes informáticos o por algún desastre de tipo natural.

Auditoría: Evaluación critica que se realiza a una actividad realizada, que pretende encontrar fallas que se están realizando y no han sido detectadas, con el fin de corregirlas y continuar con los procesos pero ya ajustados a los requerimientos.

Auditoría en TI: Auditoría informática trata de la serie de actividades con el propósito definido de evaluar las tecnologías de la información y la seguridad de la información y se basa en implementar normas nacionales e internacionales con el fin de determinar el correcto cumplimiento de las políticas de seguridad de tecnologías de información.

Auditoría Externa: Trata de una serie de actividades realizadas por un grupo de personas externas a la entidad, que por medio de diversos procesos determina si se está fallando en el proceso auditado.

Auditoría Interna: Trata de una serie de actividades que realizan un grupo de personas funcionarios de la entidad, pero que no hacen parte del proceso auditado. Con el fin de encontrar posibles fallas y riesgos que se estén presentado en los procedimientos.

Confidencialidad: El sistema “Gestión Integrada de Bienestar Social” posee información de carácter personal, de salud y condiciones socioeconómicas del núcleo familiar, lo que lo hace estrictamente confidencial y protegido por las leyes que dictan disposiciones generales para la protección de datos personales. Cada uno de los usuarios en las capacitaciones son informados que las datos que están manipulando está catalogada como información sensible y que el aplicativo genera una bitácora de cada una de las actividades que realiza el usuario. Este es uno de los aspectos de mayor importancia en la auditoría a realizar al SGSI, debido a que la información clínica y social de un ciudadano debe ser tratada como información de alta prioridad y las personas que la manipulan deben estar enteradas de los protocolos.

Disponibilidad: El sistema “Gestión Integrada de Bienestar Social” está disponible a sus usuarios en la modalidad 24/7/365 es decir 24 horas al día, 7 días a la semana por los 365 días del año. Con corte muy pequeños periódicamente de acuerdo al cronograma de mantenimiento. Por tal motivo el sistema de seguridad está diseñado para esta misma disponibilidad. De igual manera la plataforma del Web del aplicativo está disponible para todos los usuarios parametrizados de las 27 secretarias de salud de las Alcaldías del departamento de caldas y los 30 ESE

(Empresas Sociales del Estado) Hospitales de primer y segundo nivel de complejidad que tiene su red de servicios en el mismo departamento.

DTSC: Dirección Territorial de Salud de Caldas, entidad descentralizada de la Gobernación de Caldas, encargada de la inspección, vigilancia y control de los temas pertinentes con el área de la salud en el departamento.

Impacto: El sistema "Gestión Integrada de Bienestar Social" ha causado gran impacto a nivel nacional, ya que se ha convertido al departamento de Caldas como territorio piloto para la implementación de la estrategia de Atención Primaria Social (APS) de la cual este sistema es la plataforma tecnológica. Desde la Dirección Territorial de Salud de Caldas se han dictado charlas a otros departamentos interesados en aplicar el modelo APS y así cumplir con las disposiciones emanadas por el Ministerio de Salud Colombiano. En el marco del plan de desarrollo departamental se ha incluido la estrategia APS como un lineamiento más a seguir en el cuatrienio.

Integridad: los datos almacenados debes estar protegidos e íntegros, y es obligación de la seguridad informática velar por que esto se cumpla a cabalidad. De nada sirve tener una cantidad de información, si no se está seguro de integridad de sus datos, por de no ser así se convierte en información basura que no ha de servir.

ISO: Las normas ISO (International Organization for Standardization) son los documentos con la lista de actividades que se deben cumplir para garantizar que una entidad cumple con los parámetros requeridos de acuerdo a la norma implementada. Debe ser de carácter público para todos empleados, directivos y clientes de las instituciones.

Plan de mejoramiento: Son todas las acciones que se tomar direccionadas desde la alta gerencia de acuerdo al informe de recomendaciones generado desde una auditoría, con el propósito de corregir o mejorar las acciones y actividades que se están realizando.

Probabilidad: Las probabilidades de que esta estrategia sea aplicada a nivel nacional son altas, ya que en salud es más fácil y de menos costos prevenir la enfermedad que combatirla. Lo que hace muy atractiva esta iniciativa del departamento de caldas para toda la nación.

Riesgo Informático: Trata de la posibilidad de que una amenaza se convierta en realidad. Es en este momento donde se deben tomar todas las acciones de reacción previamente analizadas.

Vulnerabilidad Informática: Son los puntos de debilidad que presenta el sistema y por los cuales se le pueden causar daño al mismo sistema o a la integridad de la información.

RESUMEN

El Sistema informático “Gestión Integrada de Bienestar Social” ya implementado en la Dirección Territorial de Salud de Caldas, requiere que se le realice una Auditoría al sistema de seguridad, para determinar vulnerabilidades, amenazas y riesgos que se puedan estar presentando y que no han sido detectadas. Para este fin se ha propuesto realizar esta intervención que deje como resultado un documento final con los planes de mejoramiento a implementar en las políticas de seguridad al sistema.

Al identificar las vulnerabilidades, amenazas y riesgos del sistema de Seguridad del Sistema informático “Gestión Integrada de Bienestar Social”, se puede garantizar que la información almacenada está cumpliendo con los estándares de seguridad e integridad de datos personales, debido a que la información trata de la caracterización de la población del departamento de Caldas.

Los datos recolectados son sensibles y con niveles de riesgo tanto individual como colectivo (familia y entorno), por tal motivo no se pueda publicar y su manipulación requiera de usuario que pueda registrarse ante el aplicativo y hayan firmado el documento de confidencialidad de la información, lo que justifica la auditoría al sistema de seguridad del sistema informático “Gestión Integrada de Bienestar Social”.

Palabras Claves:

- Auditoría
- DTSC – Dirección Territorial de Salud de Caldas
- ISO/IEC 27001
- Plan de Mejoramiento
- Políticas de Seguridad Informática

INTRODUCCIÓN

El sistema “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas, es una plataforma tecnológica sobre la cual se desarrolla la estrategia APS (Atención Primara Social) que transciende el sector salud, puesto que garantiza la transectorialidad e intersectorialidad con un objetivo común y es la intervención del riesgo individual, familiar y comunitario de la población de acuerdo a unos determinantes sociales que determinen los niveles de riesgo de las familias; partiendo de la caracterización de los integrantes de cada núcleo familiar.

Esta caracterización implica la recolección y almacenamiento de información con datos personales que se deben proteger con niveles de seguridad informáticos y evitar que se filtren o sean manipulados de forma incorrecta y puedan generar daños a la privacidad de las personas encuestadas.

De acuerdo a lo anterior se elabora un plan de auditoría para implementar al sistema de seguridad del sistema “Gestión Integrada de Bienestar Social” para evaluar la seguridad del sistema; y por medio de este plan aplicar cada una de las acciones propuestas que permitan conocer los hallazgos en las vulnerabilidades, amenazas y riesgos a que está expuesto el sistema.

El plan de auditoría proporciona un informe final que contiene las recomendaciones y sugerencias para el plan de mejoramiento al sistema de seguridad del sistema “Gestión Integrada de Bienestar Social”.

1. EL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

La Dirección Territorial de Salud de Caldas, entre sus funciones de inspección vigilancia y control de la salud del departamento de Caldas, ha implementado un observatorio social de salud pública, y en este ha desarrollado un sistema de información Web denominado “Gestión Integrada de Bienestar Social”, enmarcado en la estrategia APS (Atención Primaria Social). Este sistema de información se encuentra en funcionamiento en los municipios del departamento con un número de usuarios de alcaldías, empresas sociales del estado (ESE), EPS, IPS que tienen acceso a la información. Esta información es sensible y tiene carácter de reserva ya se pueden encontrar datos personales y clínicos. Por tal motivo este sistema “Gestión Integrada de Bienestar Social” es objeto para realizar una auditoría al sistema de seguridad que presenta.

El sistema “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas, es un aplicativo Web en el que los 27 municipios del departamento de Caldas digitan la información de la población; esta caracterización se realiza a toda la comunidad con el fin de identificar niveles de riesgo de la población de acuerdo a determinantes de sociales (salud, bienestar, económicos, educación, seguridad, etc.) que por medio mecanismo de interoperabilidad de información interna y externa, se mantiene la información actualizada para la posterior toma de decisiones por parte de las mesas de técnicas.

El sistema es modular, lo que permite una rápida configuración y parametrización por medio de gestores de contenidos para poder atender las solicitudes de los usuarios. El aplicativo según los roles y privilegios de usuarios permite adicionar, modificar y eliminar datos de la caracterización, de usuarios, municipios, barrios.

El aplicativo realiza automáticamente una sumatoria de los puntos de riesgo de cada integrante de la familia y de su entorno de vivienda y le genera un puntaje; y de acuerdo a ese puntaje clasifica bien sea a la persona o a la familia en un riesgo bajo, medio o alto según sea el caso. Es así como se determina las acciones o intervenciones a realizar en la población de más alto riesgo de cada municipio.

El problema que se presenta en Sistema de Información “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas, evidenciado por varios usuarios quienes han manifestado la posibilidad de realizar actividades desde el aplicativo que pone en peligro la seguridad e integridad de los datos allí almacenados. Problemas mencionados como acceder sin autorización a la información de datos personales de salud, sociales, del hogar y del entorno familiar que reposas en bases de datos en el servidor de la institución y la posibilidad que permite el aplicativo de exportar cualquier tipo de información para

ser entregada a un tercero. Teniendo claro que esta información debe estar protegida y amparada bajo la ley de hábeas data que tiene toda persona. Por tratarse de información sensible siempre va a estar expuesta a delitos cibernéticos que en la actualidad se pueden ejecutar por medio de ataques de diversas formas.

1.2 FORMULACIÓN DEL PROBLEMA

Evidenciando los problemas en la seguridad del sistema informático “Gestión Integrada de Bienestar Social” que se tiene implementado en la Dirección Territorial de Salud de Caldas, es pertinente tomar acciones.
¿Cómo la auditoría a la seguridad del sistema “Gestión Integrada de Bienestar Social” permitirá identificar las vulnerabilidades, amenazas y riesgos a que está expuesto, para proponer un plan de mejoramiento a implementar que brinde seguridad al sistema?

1.3 OBJETIVOS

1.3.1 General

Aplicar una auditoría a la seguridad del sistema “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas para identificar las vulnerabilidades, amenazas y riesgos a que está expuesto el sistema.

1.3.2 Específicos

- Elaborar el plan de **auditoría de la seguridad informática** que permita evaluar la seguridad del sistema “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas.

- Aplicar el plan de auditoría diseñado para mejorar la seguridad del sistema “Gestión Integrada de Bienestar Social” implementando cada una de las acciones propuestas y las matrices de riesgo con los factores de amenaza e impacto.

- Conocer las medidas de seguridad informática vigentes del sistema “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas, para determinar la existencia de los controles y políticas de seguridad.

- Evaluar las diferentes vulnerabilidades, amenazas y riesgos que se hallaron en la auditoría realizada al sistema de seguridad del sistema “Gestión Integrada de Bienestar Social”

- Elaborar un informe final que contenga las recomendaciones y sugerencias a seguir para la implementación del plan de mejoramiento al sistema de seguridad.

1.4 JUSTIFICACIÓN

Es importante proponerle a la Dirección Territorial de Salud de Caldas la implementación de la Auditoría al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social" ya que la información que allí reposa es estrictamente confidencial porque los datos son de tipo personal, de salud, sociales y de entorno familiar utilizados solo para el estudio, análisis y detección de posibles focos de enfermedades o problemáticas sociales para poder intervenirlas o tomar decisiones al respecto. Se identificaron las vulnerabilidades para asegurar la confidencialidad de la información y la no manipulación de los datos por parte de delincuentes informáticos.

Los beneficiarios de la Auditoría al sistema de seguridad son todas las personas a quienes se les ha realizado la encuesta de caracterización en la cual ha depositado la información de cada uno de los integrantes de los núcleos familiares en los 27 municipios que integran el Departamento de Caldas unidos en la estrategia de Atención Primaria Social (APS).

También fueron beneficiados con la Auditoría al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social" los usuarios del aplicativo, ya que sobre ellos recae en primera instancia la culpabilidad de los posibles ataques y fuga a la información, la perdida de la confidencialidad y cualquier daño que se presente en la integridad de los datos.

La Dirección Territorial de Salud de Caldas con la Auditoíia al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social" propuso los planes de mejoramiento a implementar que corrigen las vulnerabilidades, amenazas y riesgos hallados en la institución para mejorar sus niveles de seguridad cumpliendo con el objetivo de confidencialidad de la información que se tiene establecido con los usuarios, ya que la información personal se rige por las leyes 266 de 2008 y Ley 1581 de 2012 que habla de la reserva de la información. De igual manera se tomaran medidas para proteger de los posibles ataques por parte de delincuentes informáticos quienes por medio de herramientas tecnológicas podrían acceder a la a información sensible y manipularla.

1.5 ALCANCE Y DELIMITACIÓN

La Auditoría al Sistema de Seguridad se aplica específicamente al Sistema "Gestión Integrada de Bienestar Social" en cuanto a los aspectos relacionados con

el control de acceso por parte de usuarios al aplicativo, configuración y parametrización de roles de usuarios, políticas de seguridad establecidas.

La Auditoría no contempla la configuración ni parametrización de red de datos, equipos de cómputo, servidores, conexiones inalámbricas, sistemas operativos, antivirus, ofimática, documentos físicos, capacitación al personal, manuales operativos, manuales técnicos, ni análisis, diseño e implementación de aplicativos.

La Auditoría se lleva a cabo en las instalaciones del Observatorio Social de Salud Pública de la Dirección Territorial de Salud de Caldas en la ciudad de Manizales – Caldas, debido a que en este sitio se encuentra centralizada la información de caracterización familiar de la población del Departamento de Caldas, el administrador del aplicativo y el servidor que soporta la plataforma. Se ejecuta sobre el Sistema de Seguridad del Sistema “Gestión Integrada de Bienestar Social” durante el periodo comprendido entre los meses de mayo a octubre de 2016.

2. MARCO DE REFERENCIA

2.1 ANTECEDENTES

La auditoría a los sistemas de seguridad informáticos para determinar vulnerabilidades en las políticas de seguridad y protección de datos personales en Colombia se ha realizado en varias entidades, tal es caso de:

La empresa Almera Information Management [1] con sede en el municipio de Manizales, en el año 2016 realizo una auditoría a la seguridad del sistema de Información denominado "Sistema de Información Integral" de la Gobernación de Caldas, que permite realizarlos procesos de gestión documental y seguimiento al plan de desarrollo departamental. Para tal fin utilizaron una línea de acción de la empresa denominada Almera Risk Manager. En conversación personal con el director de proyectos de Almera Information Management ingeniero Parra, Yesid. refiere que la auditoría realizada genero hallazgos importantes en las políticas de seguridad informática del aplicativo de la gobernación tales como el uso de conexiones Wifi desprotegidas que se conectaban a la red LAN; generación de contraseñas de bajo nivel a los usuarios del aplicativo; usuarios activos de personal que ya no laboraban en la institución. Estos hallazgos se iniciaron a corregir mediante planes de mejoramiento en el año 2017.

La Firma Ernst and Young realizo en el año 2011 la auditoría externa a la seguridad del sistema de información de la empresa DECEVAL [2] (Deposito Centralizado de Valores de Colombia) que es una sociedad anónima constituida con recursos de los sectores financiero y bursátil del país. Y basaron la auditoría en el marco de control Cobit empleando la metodología de evaluación ajustada a las necesidades de Deceval. Ernst & Young ha implementado herramientas que permitan generar programas de evaluación de configuraciones de seguridad en plataformas TIC, de igual formar ha implementado matrices de riesgo y controles de procesos. En el plan de mejoramiento sugerido se plantean medidas en la seguridad de la información en cuanto a claves de acceso, obsolescencia tecnológica de los sistemas basados en Windows 2000 y Generación de scripts en el sistema SIIDJ (Sistema Integrado de Información de la empresa DECEVAL).

Y a nivel internacional se puede nombra la auditoría Informática realizada a la alcaldía del distrito de Moquegua, provincia de mariscal Nieto, departamento de Moquegua en el país de Perú. Realizada por los ingenieros de sistemas de la Universidad José Carlos MariáTegui. [3] Donde se propone como objetivo principal

[1] PARRA. Yesid. Director proyectos. Almera Information Management. Manizales. 2017.

[2] DECEVAL. Sistema integrado de información de la empresa. Bogotá. Marzo de 2012. 20p.

[3] MAMANI POMA. Orlando Jimmy. AROHUANCA A. Michella. MAMANI CUTIPA. Willy. QUIÑONES MAYTA. Carmen. MUÑOZ ORTEGA. Madeleine. POCOHUANCA TURBO. Nelssy. Informe de gestión sobre el sistema de seguridad de control interno. Perú. Mariscal. 2003. 33p.

revisar y evaluar los controles, sistemas, procedimientos de informática mediante un plan de auditoría. Uno de los objetivos específicos trata de la Evaluación de nivel de riesgo de la seguridad lógica, seguridad física y confidencialidad de la información. Entre los principales hallazgos citados se encuentra la carencia de seguridad en acceso restringido sobre los equipos de cómputo, software de seguridad desactualizado.

2.2 MARCO TEÓRICO CONCEPTUAL

En esta sección del trabajo se procede a describir una serie de temas importantes como base fundamental para el desarrollo del proyecto.

2.2.1 Seguridad informática

La seguridad informática[4] es la ciencia especializada en proteger y mantener la integridad de la información y velar por que se cumpla la privacidad de los datos almacenados en un sistema informático. Es de gran importancia para todas las entidades, ya que la información se ha convertido en un bien preciado que se debe cuidar y preservar de posibles ataques por parte de delincuentes informáticos.

2.2.2 Auditoría

La auditoría[5] es el proceso en el cual se realiza una serie de actividades lógicas y cronológicas realizadas por una persona con experiencia sobre el tema que tiene como objetivo encontrar hallazgos de posibles fallas que se estén realizado en el desarrollo diario de la actividad y que permita implementar planes de acción para corregirlos.

2.2.3 Auditoría informática

La auditoría informática[6] consiste en la evaluación y verificación de las políticas, controles, procedimientos y la seguridad de los recursos informáticos por parte de los usuarios con el fin de asegurar que se estén utilizando adecuadamente con el fin específico.

---

[4] PÉREZ PORTO. Julián. MERINO. María. “Definición de Seguridad informática”. {En línea}. {2008}. Disponible en: (https://definicion.de/seguridad-informatica/).

[5] RESTREPO G. Jorge A. “Guía para la clase de auditoría de sistemas”. {En línea}. {2011}. Disponible en: (http://jorgearestrepog.comunidadcoomeva.com/blog/index.php).

[6] SOLARTE SOLARTE. Francisco Nicolás. “Auditoría informática y de sistemas”. {En línea}. {2011}. Disponible en: (http://auditordesistemas.blogspot.com.co/2011/11/conceptos.html).

2.2.4 Auditoría de sistemas

Auditoría de sistema[7] es la que se realiza a los sistemas de información que se utilizan en una entidad o empresa, a los aplicativos (software) que son las herramientas de trabajo y que están en constante contacto con los usuarios, no se aplica a los computadores (hardware). La auditoría de sistemas comprende la revisión y evaluación de los aspectos de los procesos automáticos y no automáticos.

2.2.5 Auditoría interna

Según el Instituto de Auditores de los Estados Unidos define la auditoría interna[8] como "una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de presentar un servicio a la dirección". Y se considerada como el examen crítico, sistemático y detallado de un sistema de información, realizado por un profesional con vínculos laborales con la misma empresa.

Entre las ventajas más relevantes están:

- Ayuda a la dirección a evaluar de forma relativamente independiente los sistemas de organización y administración.
- Facilita la evaluación global y objetiva de los problemas de la empresa.
- Dispone a la dirección un amplio conocimiento de las operaciones de la empresa debido a la verificación que se realizan a los datos.
- Favorece la protección de los intereses y bienes de la empresa frente a terceros.

2.2.6 Auditoría externa

La Auditoría externa[9] es el examen crítico, sistemático y detallado de un sistema de información, realizado por auditor o investigador sin vínculos laborales con la institución o empresa, aplicando técnicas precisas con el objeto de emitir una opinión independiente sobre el estado en que opera el sistema, las dependencias que ejercen control y formular planes de mejoramiento.

Una Auditoría externa se realiza cuando se tiene la firme intención de publicar un producto del sistema de información examinado con el fin de acompañar al mismo

---

[7] SOLARTE SOLARTE. Francisco Nicolás. "Auditoría informática y de sistemas". {En línea}. {2011}. Disponible en: (http://auditordesistemas.blogspot.com.co/2011/11/conceptos.html).

[8] GERENCIE. "Auditoría interna". {En línea}. {11 mayo 2017}. Disponible en: (https://www.gerencie.com/auditoria-interna.html).

[9] GERENCIE. "Auditoria interna". {En línea}. {11 mayo 2017}. Disponible en: (https://www.gerencie.com/auditoria-externa.html).

de una opinión independiente que le dé autenticidad y permita a los usuarios de dicha información tomar decisiones confiando en las declaraciones del Auditor.

2.2.7 Plan de auditoría

El plan de auditoría[10] planea como se va a desarrollar las actividades de manera efectiva mediante una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance que se espera obtener de la auditoría. Este documento deberá desarrollarse y documentarse sobre un plan global detallando los alcances esperados. Todo plan de auditoría debe ser aprobado por la alta dirección de la entidad y se contempla puntos importantes como:

- Fecha y hora de cada actividad de la auditoría.
- Elementos del sistema a auditar.
- Áreas de la entidad a auditar.
- Lista de verificación.

2.2.8 Sistema de gestión

Un sistema de gestión[11] es considerado un conjunto de etapas unidas en un proceso continuo, que permite trabajar ordenadamente una idea hasta lograr mejoras planteadas y mejoras continuas. Se establecen cuatro etapas que se repiten en un ciclo recurrente y que cada vez que se cumpla, dejara nuevas mejoras a implementar, las cuales son:

- Etapa de ideación: se trabajan las ideas para refinarlas y que se convertían en la guía.
- Etapa de planeación: se definen las estrategias que se utilizarán, la estructura organizacional requerida, el personal asignado, el tipo de tecnología requerida y recursos necesarios.
- Etapa de implementación: decisiones y acciones para alcanzar los objetivos trazados y lograr el propósito aplicando mecanismos o instrumentos administrativos.
- Etapa de control: es una función administrativa reguladora que permite verificar o evaluar si se está cumpliendo con los objetivos o alcanzado los resultados esperados.

[10] BUSINESS ASSURANCE & AUDIT. “Plan de auditoría”. {En línea}. {2011}. Disponible en: (*ecaths1.s3.amazonaws.com/aseguramiento/836662139.PLAN+DE+AUDITORIA.pdf*)

[11] MEJORA TU GESTIÓN. “¿Qué es un Sistema de Gestión?”. {En línea}. {marzo de 2015}. Disponible en: (http://mejoratugestion.com/mejora-tu-gestion/que-es-un-sistema-de-gestion/)

2.2.9 Metodología cuantitativa

La metodología cuantitativa[12] es aquella que permite examinar los datos de manera numérica, especialmente en el campo de la estadística. Esta metodología precisa que entre los elementos del problema de investigación exista una relación cuya naturaleza sea lineal. Es decir, que se posible definirlos, limitarlos y saber dónde inicia el problema, la dirección y la incidencia entre sus elementos.

Los datos cuantitativos son estadísticos, hace demostraciones con los aspectos separados de su todo, a los que se asigna significado numérico y hace inferencias.

Algunas de sus características principales son:

- La objetividad es la única forma de alcanzar el conocimiento, por tal motivo utiliza medición exhaustiva y controlada.
- El objeto de estudio es el elemento singular empírico.
- La teoría es el elemento fundamental de la investigación social.
- Comprensión explicativa y predictiva de la realidad.
- Concepción lineal de la investigación.
- Es de método hipotético – deductivo.

2.2.10 Metodología cualitativa

La metodología cualitativa[13] posee como objeto la descripción de las cualidades de un fenómeno. Busca un concepto que pueda abarcar una parte de la realidad. Esta metodología no tratad de probar o de medir acontecimientos o datos, lo que busca es descubrir la mayor cantidad de cualidades le sea posible del caso o fenómeno en estudio.

Algunas de las características más relevantes son:

- Es inductiva.
- Considera el fenómeno como un todo – holística.
- Estudios en pequeña escala.
- No prueba teorías o hipótesis, las genera,
- No posee reglas de procedimientos.

---

[12] MENDOZA PALACIOS. Rudy. “Investigación cualitativa y cuantitativa – diferencias y limitaciones”. {En línea}. {2006}. Disponible en: (http://www.monografias.com/trabajos38/investigacion-cualitativa/investigacion-cualitativa2.shtml)

[13] MENDOZA PALACIOS. Rudy. “Investigación cualitativa y cuantitativa – diferencias y limitaciones”. {En línea}. {2006}. Disponible en: (http://www.monografias.com/trabajos38/investigacion-cualitativa/investigacion-cualitativa.shtml)

- No especifica método de recolección de datos.
- No aplica análisis estadístico
- Permite incorporar nuevos hallazgos no previstos.
- Permite interactuar entre el investigador y los sujetos de estudio.
- Se basa en la intuición.

2.2.11 Políticas de seguridad informática

Las políticas de seguridad informática[14] son una serie de procedimientos, instrucciones, reglas y practicas debidamente documentadas y estandarizadas que indican la manera en que se deben direccionar, proteger, cuidar y distribuir los recursos informáticos de una entidad o empresa. Es así como estas políticas se convierten en pieza indispensable cuando se tratan temas de seguridad informática, debido a que en los documentos se encuentra la guía a seguir en caso de una falla, una amenaza o un riesgo que se pueda presentar en cualquier momento y bajo cualquier circunstancia. Es responsabilidad del área de TIC de la entidad velar que existan, que se apliquen y que estén en continua actualización y monitoreo.

2.2.12 Valoración del riesgo

La valoración del riesgo[15] es el procedimiento que permite identificar y valorar los riesgos de errores o inexactitudes relevantes que se hayan presentado. Es decir que cada hallazgo debe estimársele el riesgo y determinar la severidad del daño y la probabilidad de que ocurra. La severidad del daño está clasificada en leve, grave y muy grave. La Probabilidad de que ocurra el daño se clasifica en posible, probable e inevitable.

2.2.13 Observatorio social

Según la DTSC un observatorio social[16] se concibe como una entidad en la cual se investiga y registra información, objetos, eventos y situaciones de carácter natural y social. Por tal motivo se considera como una herramienta que permite la interoperabilidad de datos, la utilización de instrumentos de información y visualización, generación de unidades de análisis y de analítica basada en la evidencia que permitan las intervenciones y la toma de decisiones para el beneficio de la comunidad.

---

[14] SEGU.INFO. “Política de Seguridad”. {En línea}. {2009}. Disponible en: (http://www.segu-info.com.ar/politicas/)

[15] ALBERTO G. Alexander. “Análisis y evaluación del riesgo de información”. {En línea}. {2013}. Disponible en: (http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf)

[16] DIRECCIÓN TERRITORIAL DE SALUD DE CALDAS. “Observatorio Social”. {En línea}. {2016}. Disponible en: (https://saluddecaldas.gov.co/observatorio-social/)

2.3 MARCO CONTEXTUAL

2.3.1 Reseña Histórica

En 1913 mediante ordenanza No. 29 se crea la Oficina Médico legal y de Higiene Pública. En este mismo año y según ordenanza No. 32 se establece un Dispensario de Sanidad, el cual fue instalado en un local escogido por dos médicos nombrados por la Junta de Higiene.

En el mes de Abril de 1921, según consta en la ordenanza No. 34, la Asamblea Departamental de Caldas, crea en cada uno de los pueblos del departamento, una Junta de Sanidad, que sería la encargada de la higiene en su municipio y por supuesto, de los habitantes de los mismos.
En 1943 mediante ordenanza No. 03 se crea la Dirección de Higiene y Asistencia Pública.

Para el año de 1963, el Ministerio de Salud, ve la necesidad de realizar un estudio con el fin de diseñar un sistema nacional de salud, tomando como base los niveles de dirección nacional, seccional y regional y los de atención regionalizada.

Por Decreto Nacional No. 786 de marzo 25 de 1966, se entrega al Servicio Seccional de Salud de Caldas con la Beneficencia de Manizales, los hospitales de todo el departamento, los asilos de ancianos, las instituciones de rehabilitación, las entidades de asistencia social, los organismos dependientes de la Secretaría Departamental de Salud Pública de Caldas, los distritos de salud y los centros y puestos de salud en todo el Departamento.

Con la presencia del Ministerio de Salud Pública, se aprueba el 31 de julio de 1967, el contrato básico sobre descentralización administrativa, lo que implica alcanzar más autonomía para manejar el Servicio de Salud y que los problemas se puedan resolver acertadamente en las Juntas Seccionales de Salud.

Por medio de la ordenanza No. 02 del 19 de octubre de 1990, se le da el cambio de nombre al hasta entonces Servicio de Salud de Caldas en la Unidad Administrativa Especial denominada Dirección Seccional de Salud de Caldas (D.S.S.C.), con personería jurídica, autonomía administrativa y patrimonio propio, adscrita al despacho de la gobernación.

Luego de la promulgación de la ley 10 en 1990, la Dirección Seccional de Salud, desarrolla las actividades propias de la ley, e integra posteriormente las correspondientes a la ley 60 de 1993 y la ley 100 del mismo año. En este sentido su esfuerzo se dirige a la implementación del Sistema General de Seguridad Social en Salud.

A partir del año 1998, la DSSC para lograr las competencias que le corresponden como ente rector del Sistema de Seguridad Social en Salud del departamento, conforma grupos funcionales para asumir el desarrollo del Plan de Atención Básica, la Seguridad Social, especialmente en lo relacionado con el régimen subsidiado, la coordinación de la Red de Servicios, el apoyo a la Descentralización Municipal de Salud, los Grupos de Vigilancia y Control Promoción y Prevención del POS, Información y Estadística y de Contratación e Interventoría.
En el año 2002, la Dirección Seccional de Salud de Caldas requiere para su modernización reorganizarse como un ente que combine los enfoques de asesoría, asistencia técnica, vigilancia y control con el fin de ejercer funciones administrativas y de coordinación en pro del desarrollo del sector salud y del sistema de seguridad social en el departamento de Caldas.

Es por esto que por medio de la ordenanza 446 de abril 29 de 2002 se transforma la Unidad Administrativa Especial denominada Dirección Seccional de Salud de Caldas en Dirección Territorial de Salud de Caldas. [17]

2.3.2 Misión.

Realizar acciones de Asistencia Técnica e inspección vigilancia y control a los diferentes actores del Sistema General de Seguridad Social en Salud, así como gestionar la prestación de los servicios de salud para mejorar la calidad de vida de la población caldense.[18]

2.3.3 Visión.

Para 2020 seremos la entidad modelo en el desarrollo de los ejes articuladores de Atención Primaria Social, Observatorio Social y movilización social de actores, basándonos en el mejoramiento continuo de los procesos, participación ciudadana, gestión del conocimiento, uso eficiente de los recursos y desarrollo del talento humano, en armonía con el medio ambiente.[19]

[17] DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Quienes somos. Nuestra historia. {en línea}. {21 de febrero de 2014}. disponible en: (http://saluddecaldas.gov.co/nuestra-historia/#sub_menu_paginas).

[18] DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Quienes somos. Misión. {en línea}. {16 de enero de 2017}. Disponible en: (http://saluddecaldas.gov.co/quienes-somos/#sub_menu_paginas).

[19] DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Quienes somos. Visión. {en línea}. {16 de enero de 2017}. Disponible en: (http://saluddecaldas.gov.co/quienes-somos/#sub_menu_paginas).

2.3.4 Políticas de calidad.

La Dirección territorial de Salud de Caldas como entidad rectora del Sistema General de Seguridad Social en Salud en el Departamento, proporciona los servicios de Asistencia Técnica, Inspección, Vigilancia y Control y la Gestión para la presentación de servicios de Salud de su competencia con eficiencia, eficacia y efectividad, orientados al mejoramiento continuo de los procesos que permitan la movilización social y la satisfacción de los diferentes actores del sistema, a través de un talento humano competente y comprometido.

2.3.5 Objetivos de calidad.

- Garantizar la prestación de servicios de Asistencia Técnica, Inspección Vigilancia y Control y la Gestión para la prestación de servicios de salud con oportunidad, pertinencia y calidad.
- Fortalecer las competencias y el compromiso del talento humano de la entidad.

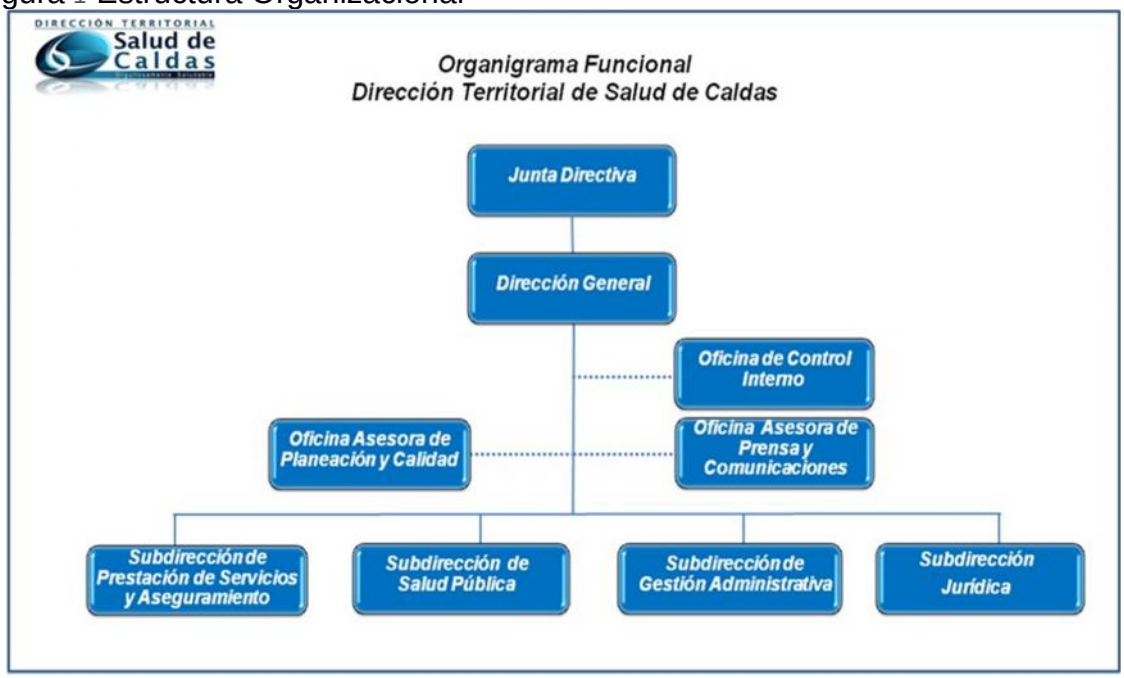
- Medir el nivel de satisfacción del usuario frente a los diferentes servicios que presta la Dirección Territorial de Salud de Caldas.

- Asegurar el mejoramiento continuo del Sistema de Gestión de Calidad de la Dirección Territorial de Salud de Caldas.[20]

[20] DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Sistema de gestión de calidad. {en línea}. {16 de enero de 2017}. Disponible en: (http://saluddecaldas.gov.co/politica-de-calidad/#sub_menu_paginas).

2.3.6 Estructura organizacional.

Figura 1 Estructura Organizacional



Fuente: http://saluddecaldas.gov.co/organigrama-funcional/#sub_menu_paginas

2.3.7 Referente Nacional.

La Política de Atención Integral en Salud, que trata sobre el Sistema General de Seguridad en Salud implantado por la Ley 100 de 1993 que ha sufrido modificaciones en su estructura por medio de varias normas, especialmente la última que es la Ley 1751 de 2015 o la denominada Ley Estatutaria de la Salud y la Ley 1753 de 2015 del Plan Nacional de Desarrollo.

La Ley Estatutaria contempla los principios e instrumentos para la protección de la enfermedad, también integra ampliamente las acciones intersectoriales que se requieren para intervenir los determinantes sociales. Es en este espacio donde la estrategia APS deja de ser solo de Salud e incorpora el aspecto Social para permitir que todas las acciones locales o nacionales sean dirigidas a la promoción de la salud y la prevención de la enfermedad.[21]

[21] MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Política de atención integral en salud. ”Un sistema de salud al servicio de la gente”. {en línea}. {enero de 2016}. Disponible en: (https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/modelo-pais-2016.pdf).

2.4 MARCO LEGAL

La Dirección Territorial de Salud de Caldas se rige por el siguiente marco normativo de acuerdo a las leyes establecidas y vigentes:

Cuadro *1*. Marco normativo rector

Ley y/o Decreto	***Descripción***
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un Nuevo País”
Ley 1751 de 2015	Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Ley 1616 de 2016	Por medio de la cual se expide la Ley de Salud Mental.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1562 de 2012	Por la cual se modifica el sistema de riegos laborales y se dictan otras disposiciones en materia de salud ocupacional.
Ley 1592 de 2015	Por medio de la cual se introduce modificaciones a la Ley 975 de 2005 “por la cual se dictan disposiciones para la reincorporación de miembros de grupos armados organizados al margen de la Ley, que contribuyan de manera efectiva a la consecución de la Paz nacional y se dictan otras disposiciones para acuerdos humanitarios”
Ley 1450 de 2011	Por la cual se adopta el Plan Nacional de Desarrollo 2010-2014.
Ley 1438 de 2011	Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones.
Ley 1468 de 2011	Por la cual se modifican los artículos 236, 239, 57 y 58 del Código Sustantivo de Trabajo y se dictan otras disposiciones.

Ley y/o Decreto	*Descripción*
Cuadro 1. (Continuación)	
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la Sociedad de la Información y la organización de las tecnologías – TIC-, se crea la agencia nacional de espectro y se dictan otras disposiciones.
Ley 0053 de 1990	Por la cual se modifican artículos de los Códigos de Régimen Departamental y Municipal; Los decretos – leyes números 1222 y 1333 de 1986; la Ley 78 de 1986 y el Decreto – Ley número 077 de 1987.
Decreto 2353 de 2015	Por el cual se unifican y actualizan las reglas de afiliación al Sistema General de Seguridad Social en Salud, se crea el Sistema de Afiliación Transaccional y se definen los instrumentos para garantizar la continuidad en la afiliación y el goce efectivo del derecho a salud.
Decreto 1681 de 2015	Por la cual se reglamenta la Subcuenta de Garantías para la Salud del Fondo de Solidaridad y Garantías FOSYGA.
Decreto 2459 de 2015	Por el cual se reglamenta la prestación de servicios de salud por los distritos creados con posterioridad a la expedición de la Ley 715 de 2001.
Decreto 0055 de 2015	Por la cual se reglamenta la afiliación de estudiantes al Sistema General de Riesgos Laborales y se dictan otras disposiciones.
Decreto 1953 de 2014	Por la cual se crea un régimen especial con el fin de poner en funcionamiento los Territorios Indígenas respecto de la administración de los sistemas propios de los pueblos indígenas hasta que el Congreso expida la Ley que trata el artículo 329 de la constitución Política.

Fuente: Dirección Territorial de Salud de Caldas, normatividad interna: http://saluddecaldas.gov.co/normatividad/#sub_menu_paginas y normatividad externa: https://www.minsalud.gov.co/Paginas/normativa-inicio.aspx

3. METODOLOGÍA

3.1 TIPO DE INVESTIGACIÓN

El tipo de investigación a realizar esta basado en un enfoque Cuantitativo, pues el objetivo principal es Identificar las vulnerabilidades, amenazas y riesgos a que está expuesto el sistema "Gestión Integrada de Bienestar Social" en cuanto a las variables de disponibilidad, confidencialidad e integridad de la información, que permita generar un informe final adoptado como plan de mejoramiento a implementar.

3.1.1 Investigación Cuantitativa.

Al tratarse de una investigación con enfoque cuantitativo con método descriptivo, se aplica una serie de fases para construir el proyecto.[22]

Partiendo de la idea principal que es la de Identificar las vulnerabilidades, amenazas y riesgos a que está expuesto el sistema "Gestión Integrada de Bienestar Social", para lo cual se realizó la auditoría interna por parte del investigador, quien basándose en varias sugerencias y evidencias por parte de los empleados usuarios de la aplicación, quienes manifiestan inconsistencias en el aplicativo. Por tal motivo realiza el planteamiento del problema expresado en ¿Como la auditoría a la seguridad del sistema, permitirá identificar las vulnerabilidades, amenazas y riesgos a que se encuentra expuesto y con los hallazgos generar un plan de mejoramiento a implementar con la aprobación del administrador del aplicativo, del director de sistemas y de la alta dirección de la entidad.

Se solicita al director general de la Dirección Territorial de Salud de Caldas la autorización para ejecutar la auditoría interna al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social", la cual es aprobada expidiendo un aval de aceptación y permitiendo la primera reunión del investigador con el grupo de apoyo colaborador conformado por empleados de la misma institución quienes tienen contacto directo y experiencia en el funcionamiento del aplicativo. Es así como se realiza una serie de reuniones, entrevistas, verificación de políticas de seguridad informática tanto a nivel de la institución como del aplicativo auditado; se selecciona la muestra de usuarios a quienes se va a tener contacto directo para verificar y comprobar el esquema de seguridad implementado.

Ya con la información suministrada por los usuarios se determina si se está cumpliendo con las políticas establecidas o si por el contrario existen algunas que no se están implementando y permiten generar algún tipo de vulnerabilidad,

[22] HERNÁNDEZ SAMPIERI. Roberto. FERNÁNDEZ COLLADO. Carlos. BAPTISTA LUCIO. María del Pilar. Metodología de la investigación. Quinta edición. Perú. Mc GRAW HILL. 2010. 276p.

amenaza o riesgo a la seguridad de la información que se encuentra en la aplicación. Con los datos analizados se genera un documento final que trata del plan de mejoramiento a implementar en la institución para corregir las vulnerabilidades y posterior verificación de cumplimiento por parte del administrador de la plataforma como del director de sistemas de la institución.

3.2 DISEÑO DE INVESTIGACIÓN

En reunión de apertura para el desarrollo de actividades de la auditoría el grupo conformado por el estudiante de la especialización en seguridad informática, el director general de la DTSC, la profesional universitaria de la estrategias APS, el profesional universitario del observatorio social de salud pública y el ingeniero administrador del aplicativo “Gestión Integrada de Bienestar Social”, se determina el plan de auditoría, los objetivos de la auditoría, los criterios de referencia, los alcances de la misma, el tipo de investigación, seleccionar las fechas y horarios para realizar las actividades propuestas y el detalle de la complejidad, funciones y responsabilidades del grupo de apoyo del auditor.

Con lo anterior se dispone realiza visita a las instalaciones del Observatorio Social de Salud Pública de la Dirección Territorial de Salud de Caldas, para conocer de primera mano el sistema y entablar una entrevista con el encargado de la administración del aplicativo Ing. Sebastián Martínez y se le pregunta si tiene conocimiento sobre el sistema de seguridad implementado al sistema de información quien expresa que la seguridad de la infraestructura tecnológica de la DTSC está bajo el esquema de políticas implementados por la institución y que depende del director de sistemas. El Ing. Martínez solo se encarga de la seguridad administrable sobre los usuarios del aplicativo “Gestión Integrada de Bienestar Social”, la cual ejerce desde su usuario administrador.

Para aplicar el plan de auditoría se establecen reuniones con el administrador del sistema “Gestión Integrada de Bienestar Familiar”, e iniciar el proceso para desarrollar los puntos propuestos en dicho plan. De acuerdo a lo establecido en las normas ISO/IEC 27000, ISO/IEC 27001 que permiten mejorar la seguridad informática ya implementada. Y la norma ISO 27007:2011 que trata de técnicas de seguridad y directrices para la gestión de los sistemas de seguridad de la información. Por lo cual se acuerda con el administrador trabajar con estas normas.

Para conocer las medidas de seguridad informática vigente se solicita al administrador del sistema “Gestión Integrada de Bienestar Social” la información pertinente a la implementación del sistema de seguridad y que medias realiza como administrador para verificar el correcto cumplimiento de las políticas de seguridad. Por medio de la entrevista, verificación y lista de cheque se comprueba que políticas están implementadas.

Aplicando ISO/IEC 27001 se realiza entrevistas a usuarios de acuerdo a la muestra seleccionada con anterioridad, para determinar que políticas de seguridad están implementadas a cada uno de ellos, los atributos de usuario, si se están cumpliendo con los acuerdos de confidencialidad de la información y con esta información se verifican posibles vulnerabilidades encontradas en las pruebas.

Para evaluar las diferentes vulnerabilidades, amenazas y riesgos, se realizan pruebas de ataques de infiltración al sistema de información con el fin de verificar las políticas de seguridad implementadas, posibles ataques para ingresar al sistema desde navegadores conectados a la red LAN de la institución, y comprobar la reacción del sistema. Por medio de lista de chequeo saber cuáles políticas y directivas de seguridad están aplicadas y en funcionamiento sobre el servidor donde está alojado el sistema de información "Gestión Integrada de Bienestar Social".

Como parte final de la auditoría se hace entrega del informe final al administrador del sistema y al director de la Dirección Territorial de Salud de Caldas los hallazgos encontrados al sistema de seguridad del sistema "Gestión Integrada de Bienestar Familiar", y se propone el plan de mejoramiento a implementar por parte de la entidad en las áreas del observatorio social, de sistemas y de calidad. En las sugerencias se propone en un plazo no superior a dos meses verificar que efectivamente se cumpla con el plan de mejoramiento sugerido.

3.2.1 Universo y muestra.

El Universo se define con el total de elementos que presentan determinadas características y son objeto de estudio. Para la auditoría al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social" de la Dirección Territorial de Salud de Caldas, el universo está determinado por el número de usuarios que para la fecha son 173 clasificados en 3 grupos (46 *Funcionarios* Dirección Territorial de Salud de Caldas, 109 en *Municipios* Alcaldías y Hospitales, 18 *EPS*) con perfiles de acuerdo al cargo, responsabilidad y funcionabilidad.

La muestra para el análisis se seleccionan de cada grupo el 20 por ciento de los usuarios (9 Funcionarios, 22 Municipios, 4 EPS) con acceso y suficiente interacción con el sistema de acuerdo a su perfil, ya que son quienes poseen las mayor cantidad de información sobre el uso y problemas que presenta al momento de estar laborando con el aplicativo.

3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN INFORMACIÓN

Como se cuenta con el Aval para el desarrollo de la Auditoría al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social", se puede obtener información de primera mano por medio de:

- Entrevistas con los directivos de la Dirección Territorial de Salud de Caldas

- Entrevista con usuarios del sistema “Gestión Integrada de Bienestar Social”

- Realizar a los usuarios Cuestionario con preguntas básicas sobre la forma de cómo interactúan con el sistema.

- Con el administrador del sistema realizar una lista de chequeo sobre:
    - Usuarios activos e inactivos
    - Usuarios que lleven más de 4 semanas sin utilizar el sistema

- Por medio de una encuesta conocer el estado de satisfacción y que percepción tienen del sistema.

- Técnica de observación documental, que consiste en verificar con el administrador del aplicativo que efectivamente existan los acuerdos de confidencialidad firmados por los usuarios; que existan los controles de seguridad establecidos en la entidad.

3.3.1 Validez.

Al utilizar instrumentos de recolección de información como las entrevistas, se realizaran de forma personal y puntuales, sobre el tema específico y brindando al entrevistado la seguridad sobre el tema tratado y reconociéndole que son parte importante en el desarrollo del proyecto de auditoría. Esto hace que la información recolectada sea de muy buena calidad y enfocada al tema específico.

Para la confiabilidad y calidad de los datos encuestados, se solicita el apoyo de personas con experiencia que sirvan de referentes en el proceso se recolección de la información.

ALVARES CASTRO. Juan Carlos. Director. Oficina asesora de planeación y calidad DTSC. 2017

ROMERO TORRES. Mariano Esteban. Director de proyecto. Universidad nacional abierta y a distancia – UNAD. 2016

3.3.2 Confiabilidad.

Las encuestas, entrevistas y verificación de acuerdo a listas de chequeo, se realizaran en varias etapas del desarrollo de la auditoría, y se medirá el grado de confiabilidad y confidencialidad en cada uno de esos momentos y se espera que siempre arroje los mismos resultados.

4. PRODUCTO RESULTADO A ENTREGAR

Al finalizar la auditoría se entrega a la Dirección Territorial de Salud de Caldas el informe final que contiene los hallazgos de vulnerabilidades, amenazas y riesgos encontrados y el plan de mejoramiento a implementar al Sistema de Seguridad del Sistema “Gestión Integrada de Bienestar Social”.

La Dirección Territorial de Salud de Caldas, como institución de inspección, vigilancia y control del área de salud del departamento de caldas, ha de estar siempre en continuo mejoramiento en pro de la seguridad, integridad y confidencialidad de la información con especial criterio sobre los datos de la caracterización de su población donde se especifican variables personales y sensibles que son objeto de posibles ataques por parte de personal no autorizado o divulgación de datos confidenciales.

Por tal motivo la auditoría al sistema de seguridad del sistema “Gestión Integrada de Bienestar Social” se realizó mediante la aplicación de una auditoría interna que consistió en una serie de actividades realizadas por un profesional del área de la ingeniería de sistemas que labora en la dependencia del observatorio social de salud pública de la Dirección Territorial de Salud de Caldas, quien realizó una inspección y evaluación del sistema de seguridad implementado al aplicativo objeto de la auditoría.

Se elaboró un plan de auditoría que permite la evaluación del sistema de seguridad del aplicativo para comprender los aspectos legales y políticas de internas que aplican en la institución y determinar características requeridas, herramientas necesarias y alcances de la auditoría. En entrevistas con personal encargado del área de informática de la entidad y con algunos usuarios del sistema se logró tener una idea clara de cómo proceder a realizar la auditoría interna ya definida.

Con la información recolectada se procedió a aplicar conceptos de seguridad de la información como medidas preventivas y reactivas que permitan resguardar y proteger los datos almacenados, la confidencialidad de los mismos por lo cual se aplica los establecido según las normas ISO/IEC 27000 e ISO/IEC 27001 que son estándares de seguridad a nivel internacional que permite mejorar la seguridad informática implementada, ya que ha sido probada en varios escenarios con excelentes resultados debido a que especifica los requisitos necesarios para establecer, implementar y mejorar los esquemas de las políticas de seguridad de la información de una entidad. De igual manera se aplicaron las normas ISO/IEC 27007:2011 que trata de las Técnicas de seguridad y Directrices para la gestión de los sistemas de seguridad de la información de auditoría, información y competencias de auditores de SGSI.

Al utilizar la norma ISO 27001, se implementa la Metodología MAGERIT que da lugar a los posibles riesgos que se están presentando para obtener una valoración y estimar las vulneraciones, amenazas y riesgos como el posible impacto que se genera en la información, en los empleados y en la empresa. Se clasifican las medidas a implementar para controlar, corregir y prevenir nuevas vulnerabilidades en el continuo proceso de manipulación, configuración y parametrización del sistema de seguridad del sistema "Gestión Integrada de Bienestar Social" de la Dirección Territorial de Salud de Caldas.

Después de realizados los anteriores procesos se generó un informe que contiene el plan de mejoramiento que consiste listar todas y cada una de las recomendaciones para controlar y evitar las vulnerabilidades encontradas en la auditoría de acuerdo a las nuevas tecnologías aplicadas. De igual manera se contempla un seguimiento y monitoreo al plan de mejoramiento planteado en la auditoría que permita estar seguro que los hallazgos se corrigieron en un corto y mediano plazo.

4.1 PLAN DE AUDITORÍA

En la presente actividad se elabora el plan de auditoría según los estándares establecidos en las normas ISO/IEC 27000, ISO/IEC 27001 que son estándares de seguridad a nivel internacional que permiten mejorar la seguridad informática ya implementada. Y la norma ISO 27007:2011 que trata de las Técnicas de seguridad y Directrices para la gestión de los sistemas de seguridad de la información de auditoría, información y competencias de auditores de SGSI.

Se aprueba el siguiente plan de auditoría.

Cuadro *2* Plan de auditoría

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
1. Análisis de la entidad	1.1 Reunión de apertura (presentación del grupo)	2016-09-05	09:30 h	JAPR	Director: Gerson Bermont APS: Mercedes Pineda Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
Cuadro 2 (continuación)					
	1.2 Análisis institucional. 1.3 Identificación de partes interesadas.	2016-09-05	14:30 h	JAPR	Observatorio: Isdruval Arengas
	1.2 Se determina los objetivos de la auditoría, los criterios de referencia, los alcances de la misma, seleccionar las fechas y horarios para realizar las actividades propuestas y el detalle de la complejidad, funciones y responsabilidades del grupo de apoyo del auditor.	2016-09-05	09:45 h	JAPR	APS: Mercedes Pineda Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	1.3 Se Realiza visita a las instalaciones del Observatorio Social de Salud Pública de la Dirección Territorial de Salud de Caldas, para conocer de primera mano el sistema "Gestión Integrada de Bienestar Familiar".	2016-09-19	08:30 h	JAPR	APS: Mercedes Pineda Observatorio: Isdruval Arengas, Sebastián Martínez
	1.4 Asignación de responsabilidades grupo investigador y de apoyo.	2016-09-19	11:00 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez
2. Análisis de información	2.1 Solicitud de inventario y clasificación de activos del área del observatorio al director de sistemas.	2016-10-01	09:30 h	JAPR	Sistemas: Alonso Jiménez.
	2.2 Entrevista con el encargado de la administración del sistema "Gestión Integrada de Bienestar Familiar". Y se pregunta si tiene conocimiento sobre el sistema de seguridad implementado al sistema de información. ISO/IEC 27000 - ISO/IEC 27001	2016-10-03	08:30 h	JAPR	Observatorio: Sebastián Martínez

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
Cuadro 2 (continuación)					
	2.3 En reuniones con el administrador del sistema “Gestión Integrada de Bienestar Familiar”, se desarrollan los puntos propuestos en el plan de auditoría. ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-10-07	08:30 h	JAPR	Observatorio: Sebastián Martínez
3. Análisis del riesgo	3.1 Solicitar al administrador del sistema “Gestión Integrada de Bienestar Social” la información pertinente a la implementación del sistema de seguridad y que medidas realiza como administrador para verificar el correcto cumplimiento de las políticas de seguridad. ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-10-14	08:30 h	JAPR	Sebastián Martínez
	3.2 Realizar entrevistas a usuarios aleatoriamente, para determinar que políticas de seguridad están implementadas. ISO/IEC 27001	2016-10-20	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
Cuadro 2 (continuación)					
4. Puesta en marcha	4.1 Establecer y verificar las vulnerabilidades que se encuentran en las pruebas. ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-10-24	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez
	4.2 Verificar los atributos que tiene parametrizados los roles de usuarios. ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-10-25	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	4.3 Determinar por qué motivo no se están aplicando ciertas políticas de seguridad si es el caso. ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-10-26	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	4.4 Realizar posibles ataques para determinar cómo reacciona el sistema. ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-10-28	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	4.5 Verificar por medio de lista de chequeo que políticas de seguridad implementadas se están cumpliendo y cuáles no.	2016-10-31	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
Cuadro 2 (continuación)					
	4.6 Con el administrador de la red de datos, verificar las directivas de seguridad que se establecen desde el servidor donde está alojado el sistema de información "Gestión Integrada de Bienestar Social". ISO/IEC 27000 - ISO/IEC 27001 - ISO/IEC 27007:2011	2016-11-02	08:30 h	JAPR	Observatorio: Sebastián Martínez
	4.7 Valoración del riesgo	2016-11-03	08:30 h	JAPR	Observatorio: Sebastián Martínez Sistemas: Alonso Jiménez
5. Mejora continua	5.1 Se elabora el informe final con los hallazgos encontrados en la auditoría y proponer el plan de mejoramiento. ISO/IEC 27001	2016-11-04	08:30 h	JAPR	Director: Gerson Bermont APS: Mercedes Pineda Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
Cuadro 2 (continuación)					
	5.2 Se propone el plan de mejoramiento a implementar. ISO/IEC 27001	2016-11-08	08:30 h	JAPR	Director: Gerson Bermont APS: Mercedes Pineda Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	5.3 Entregar al administrador del sistema y al director de la Dirección Territorial de Salud de Caldas, el informe final de los hallazgos encontrados en la auditoría al sistema de seguridad del sistema “Gestión Integrada de Bienestar Familiar” y plan de mejoramiento sugerido.	2016-11-18	10:30 h	JAPR	Director: Gerson Bermont Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	5.4 Verificar que efectivamente se cumpla con el plan de mejoramiento sugerido.	2016-11-29	08:30 h	JAPR	Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.

Fase	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	FECHA	HORA	AUDITOR	CARGO Y NOMBRE
Cuadro 2 (continuación)					
	5.5 Reunión de cierre	2016-11-29	14:30 h	JAPR	Director: Gerson Bermont APS: Mercedes Pineda Observatorio: Isdruval Arengas, Sebastián Martínez Sistemas: Alonso Jiménez.
	Observaciones:				
	Favor informarnos instrucciones de seguridad en lo que tenga que ver con vestuario y/o calzado.				
	La auditoría se desarrollara de acuerdo a los parámetros de espacio y tiempo previamente acordados con el Director de la DTSC. La auditoría por ser interna y realizada por un trabajador de la entidad, se permitieron horarios laborales y acuerdos de confidencialidad de información manipulada.				

Fuente: [23] http://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADaAuditoriaEntidadesPublicas+V2Octubre2015/fcf84a18-5c74-480a-83c4-2a25ec49bea1

4.2 DESARROLLO DE LA AUDITORÍA

En esta etapa se desarrolla el plan de auditoría previamente aprobado y se procede a ejecutar cada uno de los puntos, para reunir las suficientes evidencias que permitan emitir las respectivas conclusiones.

[23] FUNCIÓN PÚBLICA. “Guía de auditoría para entidades públicas”. {En línea}. {Octubre 2015}. Disponible en: (http://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADaAuditoriaEntidadesPublicas+V2Octubre2015/fcf84a18-5c74-480a-83c4-2a25ec49bea1)

4.2.1 Reunión de inicio

Se realiza reunión en la sede principal de la Dirección Territorial de Salud de Caldas entre el investigador y el grupo de apoyo integrado por funcionarios de la entidad y se acuerda adoptar el cronograma aprobado en el plan de auditoría. Es así como se traslada hasta la sede del observatorio social de la DTSC y en conversación con el Dr. Arengas Castilla, Ángel Isdruval[24], profesional especializado director del observatorio, realiza una exposición de como es el funcionamiento del Observatorio Social de Salud Publica explicando las bondades y ventajas de tener un software desarrollado a la medida y que ha causado gran interés a nivel nacional por la estrategia y metodología utilizada e implementada en Caldas, la caracterización de la población, la identificación de determinantes sociales y la rapidez con que se pueden tomar decisiones y realizar intervenciones provenientes de varios sectores de la administración departamental y estatal, quienes trabajan articuladas bajo la misma estrategia.

Posteriormente el Dr. Arengas reúne el grupo de empleados de la dependencia del Observatorio con quiénes se tiene una actividad de presentación individual y una conversación acerca del proyecto de auditoría interna a desarrolla y que involucra dicha dependencia en especial a quienes tienen relación directa con el Sistema de Información denominado “Gestión Integrada de Bienestar Familiar”. Se les comunica los objetivos planteados y los alcances esperados en el desarrollo del cronograma de trabajo.

Se identifica qué relación tiene cada empleado con el observatorio social y con el sistema “Gestión Integrada de Bienestar Familiar” y se quienes expresan como interviene cada uno de ellos con el aplicativo. Es de anotar que en este grupo de personas se encuentran:

- Ingenieros de Sistemas desarrolladores, encargados de las actualizaciones y requerimientos de Sistema de Información.

- Ingeniero de Sistema, encargado del desarrollo web

- Epidemiólogos, encargados de datos vulnerables y focos con determinantes en salud.

- Administradores de bases de datos que realizan interoperabilidad con el Sistema de Información “Gestión Integrada de Bienestar Familiar” como lo es:
    - Estadísticas Vitales
        - Defunciones: Certificados de Personas Fallecidas

[24] ARENGAS CASTILLA. Ángel Isdruval. Epidemiólogo. Dirección Territorial de Salud de Caldas. Director Observatorio Social de Salud de Caldas. {2017}

        - Nacidos Vivos: Certificados de Personas recién nacidas
    - Sivigila: Notificación de casos de enfermedades de salud pública confirmados.
    - RIPS: Registro Individual de Prestación de Servicios, que es el registro de cada una de las actividades que le realizan a un paciente desde el momento en que ingresa a un centro de salud (clínica, hospital), hasta que sale o es dado de alta.

En esta reunión se realiza un levantamiento de información importante, ya que se conoce de primera mano cómo es el funcionamiento del sistema de información "Gestión Integrada de Bienestar Familiar" y quienes intervienen en la administración, alimentación y procesamiento de la información del sistema.

Por último en esta actividad se identifica a las personas responsables de suministrar la información requerida, como el respectivo procedimiento de solicitud y entrega de la misma.

4.2.2 Solicitud de información

Se participa en reunión con el administrador del sistema "Gestión Integrada de Bienestar Familiar" ingeniero Martínez, Sebastián[25], quien expone el funcionamiento del sistema, la captura de la información, como se realizan los procesos de interoperabilidad de datos, bajo qué criterios y estándares. Resaltando las dos formas de actualizar la información.

1. Por medio de caracterización en terreno, es decir que un personal que pueden ser promotoras de salud o auxiliares de enfermería, van casa a casa realizando el levantamiento de información en un formato preestablecido y se denomina línea base y con este mismo formato se realizan actualizaciones constantes con una periodicidad aproximadamente de 1 a 2 meses.

2. Por medio de interoperabilidad de datos el procedimiento es recolectar la cantidad de información interna y externa que permita actualizar los campos recolectados en la línea base, y cruzarlos utilizando como llave principal el número de identificación de la persona. Así se puede tener constante actualización de la información recolectada.

El ingeniero Martínez expresa que las medidas de seguridad del sistema "Gestión Integrada de Bienestar Social", desde la administración del aplicativo a su cargo son:

[25] MARTÍNEZ. Sebastián. Ingeniero de sistemas. Dirección Territorial de Salud de Caldas. Observatorio Social de Salud de Caldas. {2017}

- Políticas de reserva y manejo de la información sensible.
- Políticas de privacidad y protección de datos personales.
- Políticas de continuidad, contingencia y recuperación de información.
- Políticas de desarrollo seguro.
- Políticas de adquisición, desarrollo y mantenimiento.
- Políticas de intercambio de información.
- Políticas para la creación de usuarios.
- Políticas de parametrización.
- Políticas de copias de respaldo de la información.

Se solicita al ingeniero Martínez información sobre las políticas y controles de seguridad del aplicativo y datos nominales que administra, acuerdos de confidencialidad firmados con los usuarios finales y entidades con que comparten información.

Este procedimiento aporta un documento soporte de la reunión y una lista de chequeo, que permite con la información suministrada generar un cuadro de valoración del riesgo determinando si se aplica o no la políticas y controles de seguridad establecidos en los protocolos de directivas de seguridad informática. Y aporta también un reporte con el plan de acción y mejora.

Posteriormente se procede a tener una reunión con el director de TIC de la Dirección Territorial de Salud de Caldas, Jiménez, Alonso[26], quien explica que la institución tiene implementadas Normas ISO de Calidad y por lo tanto el área de sistemas tiene implementados protocolos y políticas se seguridad de información de acuerdo a lo solicitado por el manual de políticas de seguridad informática de ICONTEC.

Las medidas de seguridad del sistema “Gestión Integrada de Bienestar Social”, desde las políticas de seguridad administradas por la dirección de sistemas de la

[26] JIMÉNEZ. Alonso. Ingeniero en telecomunicaciones. Dirección Territorial de Salud de Caldas. Director Tecnología de la información y las comunicaciones. {2017}

institución a cargo del ingeniero Jiménez y que cubren todos los procesos y aplicadas a la red en general son.

- Políticas para el uso de dispositivos móviles.
- Políticas para el uso de conexiones remotas.
- Políticas de seguridad del personal.
- Políticas de gestión de activos de información.
- Políticas de clasificación y manejo de la información.
- Políticas para el uso de Token de seguridad.
- Políticas de uso de periféricos y medios de almacenamiento.
- Políticas de control de acceso a redes y recursos de red.
- Políticas de administración de acceso de usuarios.
- Políticas de control de acceso a sistemas y aplicativos.
- Políticas de seguridad física y medioambiental.
- Políticas de seguridad frente a software malicioso.
- Políticas de copias de respaldo de la información.
- Política de uso de correo electrónico.
- Política de uso adecuado de internet.

Igualmente este procedimiento aporta un documento soporte de la reunión realizada y brinda una lista de chequeo, que permite con la información aportada realizar un cuadro de valoración del riesgo determinando si se aplica o no la políticas y controles de seguridad establecidos en los protocolos de directivas de seguridad informática. Y a su vez se genera también un reporte con el plan de acción y mejora.

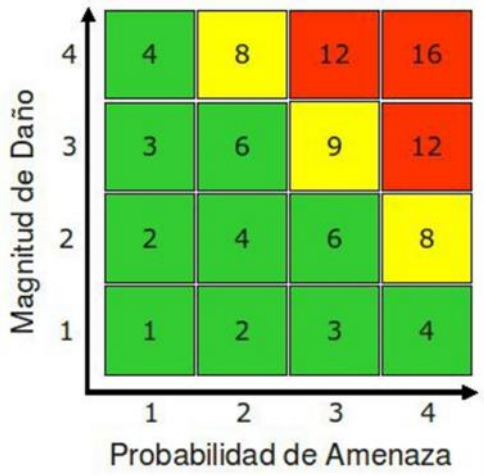
Al culminar la anteriores reuniones programadas, se confirma que el principal objetivo de la auditoría interna es encontrar posibles vulnerabilidades, amenazas y riesgos en el sistema de seguridad del sistema “Gestión Integrada de Bienestar

Social" de la Dirección Territorial de Salud de Caldas, que pongan en riesgo la integridad, disponibilidad y confidencialidad de la información.

En esta fase de solicitud de información se generan la valoración de riesgo, para lo cual el investigador con el grupo de apoyo (administrador del aplicativo, empleados de la DTSC y usuarios), se determinan las matrices de riesgo aplicables a la seguridad informática de la entidad y a la seguridad del aplicativo.

Se determina utiliza la siguiente escala para medir la magnitud del daño y la probabilidad de amenaza.

- 1 = Insignificante
- 2 = Baja
- 3 = Mediana
- 4 = Alta



El riesgo es el resultado de la multiplicación de la Probabilidad de Amenaza por la Magnitud del Daño. Y se clasifica en tres niveles.

- Bajo Riesgo = 1 – 6 Verde
- Medio Riesgo = 8 – 9 Amarillo
- Alto Riesgo = 12 – 16 Rojo

Desde la seguridad informática de la Dirección Territorial de Salud de Caldas.

Cuadro *3* Seguridad informática DTSC

RIESGO	Aparición (Probabilidad)	Gravedad (Impacto)	Valor del Riesgo	Nivel del Riesgo
Software No licenciado	2	4	8	Medio

Cuadro 3 (continuación)				
Antivirus No actualizado	3	4	12	Alto
Wifi públicos sin contraseñas	2	4	8	Medio
Falta de copias de seguridad	1	4	4	Bajo
Fallas en el sistema eléctrico	3	4	12	Alto
Daños físicos y lógicos equipos de computo	3	4	12	Alto
Sabotaje a página Web	2	3	6	Bajo
Infiltración a la red LAN	2	4	8	Medio
Pérdida o Robo de PC	2	3	6	Bajo
Falla en el canal de internet	1	2	2	Bajo

Desde la seguridad del sistema “Gestión Integrada de Bienestar Social”

Cuadro *4* Seguridad informática sistema auditado

RIESGO	Aparición (Probabilidad)	Gravedad (Impacto)	Valor del Riesgo	Nivel del Riesgo
Parametrización en contraseñas de usuarios	4	4	16	Alto
Usuarios no puedan cambiar su contraseña	3	4	12	Alto
Infiltración al servidor de BD del aplicativo	3	4	12	Alto
Falta de copias de seguridad	3	4	12	Alto
Sabotaje a página Web	1	4	4	Bajo
Exportar datos sensible desde aplicativo	4	4	16	Alto
Usuarios con privilegios no autorizados	2	4	8	Medio
Intermitencia en el canal de internet	1	3	3	Bajo
Préstamo de datos entre usuarios	2	2	4	Bajo
Acceder a datos de tipo personal y sensibles	4	4	16	Alto

4.2.3 Determinación de la muestra de auditoría

Para el desarrollo de la auditoría al Sistema de Seguridad del Sistema “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas, del universo anteriormente mencionado en la metodología de investigación se ha determinado la muestra de auditoría como un muestreo no estadístico, es decir que el investigador ha seleccionado usuarios del sistema que cumplen una característica específica y es que ingresen diariamente al aplicativo a realizar actividades propias de su rol.

La muestra para el análisis queda establecida de la siguiente manera, 9 usuarios funcionarios de la TDSC, 22 usuarios de municipios (alcaldías y hospitales), 4 usuarios de las EPS con acceso y suficiente interacción con el sistema de acuerdo a su perfil, ya que son quienes poseen las mayor cantidad de información sobre el uso y problemas que presenta al momento de estar laborando con el aplicativo.

4.2.4 Papeles de trabajo

En esta etapa del desarrollo la auditoría al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social" de la Dirección Territorial de Salud de Caldas, se elaboran por parte del auditor los documentos que se generan como soporte en el transcurso de cada una de las etapas del proceso. Es así como se elaboran listas de chequeo y cuestionarios (ver lista de anexos), que arrojan información indispensable en los hallazgos.

En especial los papeles de trabajo generados soportes documentales que se realizaron a:

- Director de sistemas de la DTSC: Listas de chequeo para verificar si se cumplen o no las políticas y controles de seguridad. Entrevistas para determinar grado de compromiso con el desarrollo de la auditoría, conocimiento sobre el tema, implementación existente, aceptación de mejoras.
- Administrador del sistema "Gestión Integrada de Bienestar Social": Lista de chequeo para verificar si se cumple con las políticas y controles de seguridad en el sistema que está a su cargo. Entrevistas para determinar si está de acuerdo con el proceso de auditoría, conocer si algún nivel de seguridad independiente al de la entidad.

Se generan notas de sugerencias y recomendaciones por parte de los usuarios que se entrevistaron, quienes expresan algunos riesgos que por su trabajo continuo en el sistema experimenta y que consideran no debería ser así. Algunos de ellos comentan que ha realizado la respectiva recomendación al administrador del aplicativo.

4.2.5 Diseño de las pruebas de auditoría

Esta etapa contempla las técnicas utilizadas por el auditor para obtener las evidencias que le permitirán emitir las conclusiones respectivas de acuerdo al impacto.

Lista de controles y políticas de seguridad

- Políticas de reserva y manejo de la información sensible.

En sistema “Gestión Integrada de Bienestar Social” desde el momento que crea el usuario, se toman unos datos básicos como nombre completo, correo electrónico y cargo, y posterior a esto se envía un correo al nuevo usuario con los datos del usuario y adjunto un documento donde se compromete a cumplir con la Ley de reserva de la información tales como la Ley 1712 de 2014, Ley estatutaria 1581 de octubre 17 de 2012, Decreto 1377 de junio 27 de 2013, y que sanciones puede llegar a tener por el incumplimiento de las mismas (ver anexo 2).

- Políticas de privacidad y protección de datos personales.

Se establece que la información recolectada de cada persona para la creación del usuario que podrá ingresar al sistema “Gestión Integrada de Bienestar Social” será únicamente para este fin, y no se utilizara para otros fines, ni se compartirá con otras personas e instituciones.

- Políticas de continuidad, contingencia y recuperación de información.

Si se llegara a presentar algún inconveniente en el correcto funcionamiento del sistema “Gestión Integrada de Bienestar Social” el sistema posee la opción de configuración de disco espejo en su servidor, lo que brinda continuidad, contingencia y posibilidad de recuperación, totalmente trasparente para el usuario final, que en este caso seria los digitadores y administradores en los municipios del departamento.

- Políticas de desarrollo seguro.

Como se trata de un desarrollo a la medida, van surgiendo nuevas solicitudes de actualización al sistema y nuevos componentes integradores de información, para lo cual se protege la información sensible con autorización y autenticación de los usuarios. Además de generar un log del usuario que permite convertirse en una bitácora que sirve para saber que está realizando cada usuario en el sistema. Por tal motivo los perfiles de usuario permiten niveles y hasta el más básico está bajo las políticas claras. Se tiene establecido que por ser desarrollo a la medida, va a ir creciendo por lo tanto en su estructura, espacio de almacenamiento y aplicabilidad se han considerado posibles cambios futuros que se van desarrollando con actualizaciones constantes.

- Políticas de adquisición, desarrollo y mantenimiento.

Se tiene establecido que el sistema “Gestión Integrada de Bienestar Social” requiere desarrollo continuo y mantenimientos constantes, para lo cual el grupo de desarrollo y mantenimiento del sistema es consciente de que se deben

implementar todos los protocolos para hacer seguro el manejo de la información, por eso utilizan métodos de cifrado hash MD5.

Figura 2. Cifrado de usuario

File Edit View Tools Help

No limit

	ing(255)	email character varying(255)	password character varying(255)	remember_token character varying(255)	linea integer
1	r	Admin@saluddecaldas.gov.co	$2y$10$RI/z2oLLFuM2m0aU4V2RLueAvVS3vdELzx1f0NNN0Zb02z7pILZ0q	1TCm6g7nx9YPQfOkvkM7KgnvixqTmk4vnK8IJA69NM3ILopSDWxbF8WKK18L	9
2	o Gomez M	Observatorio@saluddecaldas.gov.co	$2y$10$8J9hZAtWxLHkCLus8mMkAup8VtBTAIyEC1E3bZzau9iW5NxFvYpr.	ino1QDyEWuWKxt3CGq5BJQnIUDUuMdZDOpDjgPWuT0SENpBYOzktyq1KHefx	1

Fuente: Gestión Integrada de Bienestar Social

- Políticas de intercambio de información.

Se han establecido contratos interadministrativos entre la Dirección Territorial de Salud de Caldas y otros entes de como Alcaldías, Empresas Sociales del Estado, EPS, Secretarias de la Gobernación, donde se establece como es el proceso de intercambio de información, que debe cumplir ambas partes, a que se compromete cada uno, como está protegida la información sensible, la periodicidad de la entrega de información, y que beneficios recibirá cada una de las partes.

- Políticas para la creación de usuarios.

La creación de usuarios se realiza solicitando que se le envía un correo al administrador del sistema “Gestión Integrada de Bienestar Social” con los datos de nombre, teléfono, correo electrónico, entidad y cargo del usuario a crear. Con esta información desde el administrador de usuarios, se crea un usuario, se le asigna una contraseña y un rol con los privilegios; y posteriormente se le envía un correo a la persona con los datos del nombre de usuario y contraseña.

Figura 3. Información de usuario

Fuente: Gestión Integrada de Bienestar Social

- Políticas de Parametrización.

El sistema “Gestión Integrada de Bienestar Social” tiene un módulo de parametrización con el cual se establece la información de:

- Municipios: Lista de 27 municipios que conforma el departamento de Caldas.
- Barrios: Lista que conforman los municipios
- EPS: Lista de EPS que tiene presencia en el departamento de Caldas.
- IPS: Lista de IPS que existen en cada uno de los municipios.
- Bases de Datos: permite crear las estructuras para las BD con las que se puede realizar interoperabilidad.
- Temas: donde se puede parametrizar las secciones del sistema
- Grupos: Distribución por grupos etarios
- Componente: Distribución de variables de personas y del entorno social
- Clasificación: Clasificación de las viviendas.

Figura 4. Parametrización Municipios

Fuente: Gestión Integrada de Bienestar Social.

Imagen de la parametrización de bases de datos y componentes

Figura 5. Parametrización de BD.

Fuente: Gestión Integrada de Bienestar Social

- Políticas de copias de respaldo de la información.

El sistema “Gestión Integrada de Bienestar Social” tiene una política de copias de seguridad distribuida de la siguiente manera:

- Copia Completa los días domingo a las 6 am.

- Copia Incremental los días de lunes a sábado a las 6 am.

La copia incremental de todos los días se conserva por espacio de 2 meses, y a partir de ahí se conserva el último día del mes. Se estima que en la actualizada la copia incremental tiene una duración de aproximadamente 5 minutos y la copia completa aproximadamente 2 horas.

Se tiene configurado un sistema Raid de disco espejo, que permite tener como contingencia que si un disco falla, el otro va a funcionar inmediatamente y será transparente para el usuario final.

La Dirección Territorial de Salud de Caldas, tiene alquilada una pequeña bodega en un banco, donde guarda las copias de seguridad, las cuales son trasladadas con cadena de custodia por el personal de sistemas de la institución.

4.2.6 Desarrollo de observaciones

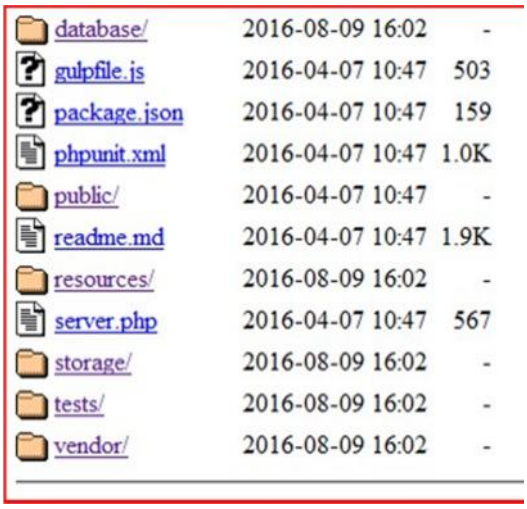
En esta fase se resaltan los hallazgos encontrados en el desarrollo de las actividades propias de la auditoría del sistema de seguridad del sistema “Gestión Integrada de Bienestar Social”.

Al realizar una prueba para verificar si se puede ingresar al árbol de directorios de una sección del sistema de la Dirección Territorial de Salud de Caldas, se verificar que efectivamente se puede ingresar a la sección del banco de ofertas que está en la página Web del sistema “Gestión Integrada de Bienestar Social” del Observatorio Social de Salud Pública.

Figura 6. Árbol de Directorio

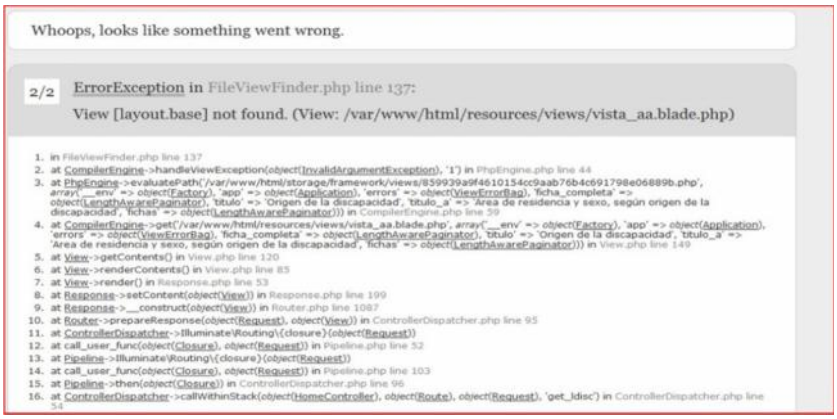
Fuente: El autor.

Figura 7. Archivos



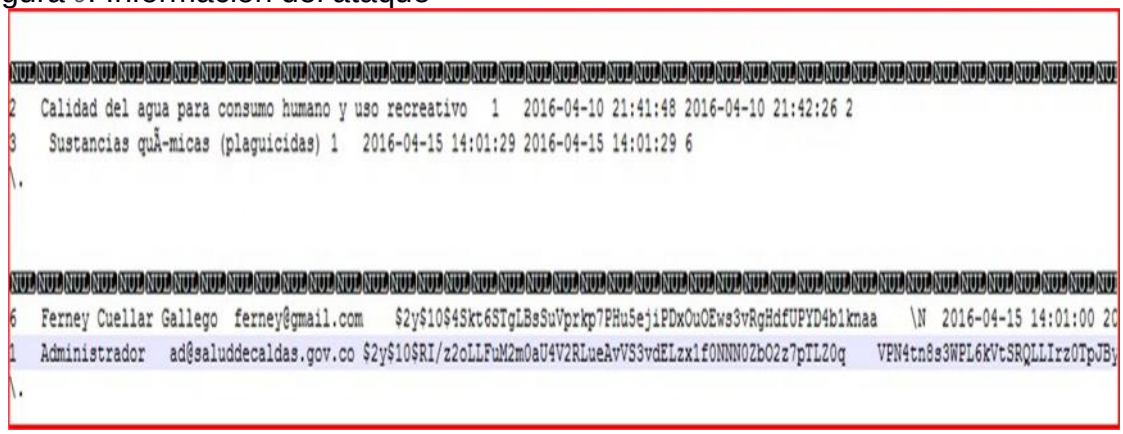
Fuente: El autor.

Figura 8. Ruta



Fuente: El autor.

Figura 9. Información del ataque



Fuente: El autor.

Al intentar ingresar al árbol de directorio de sistema “Gestión Integrada de Bienestar Social” nos muestra lo siguiente.

Figura 10. Ataque Sistema

Fuente: El autor.

Se verifican las vulnerabilidades y se puede establecer que la política de seguridad de protección y bloqueo de página Web de YouTube no está parametrizada en el programa de filtrado de DNS, por tal motivo permite el ingreso a dicha URL.

Se puede verificar e ingresar al árbol de directorio, debido a la falta de parametrización de privilegio de algunos usuarios. Que al momentos de crearlo no se delimito sus funciones por medio de los privilegios.

El sistema “Gestión Integrada de Bienestar Social” posee un módulo de parametrización de roles de usuario, los cuales según la característica solicitada, así mismo se le asignan privilegios.

La siguiente imagen muestra los tipos de usuarios que se pueden parametrizar.

Figura 11. Roles usuarios

Fuente: El autor.

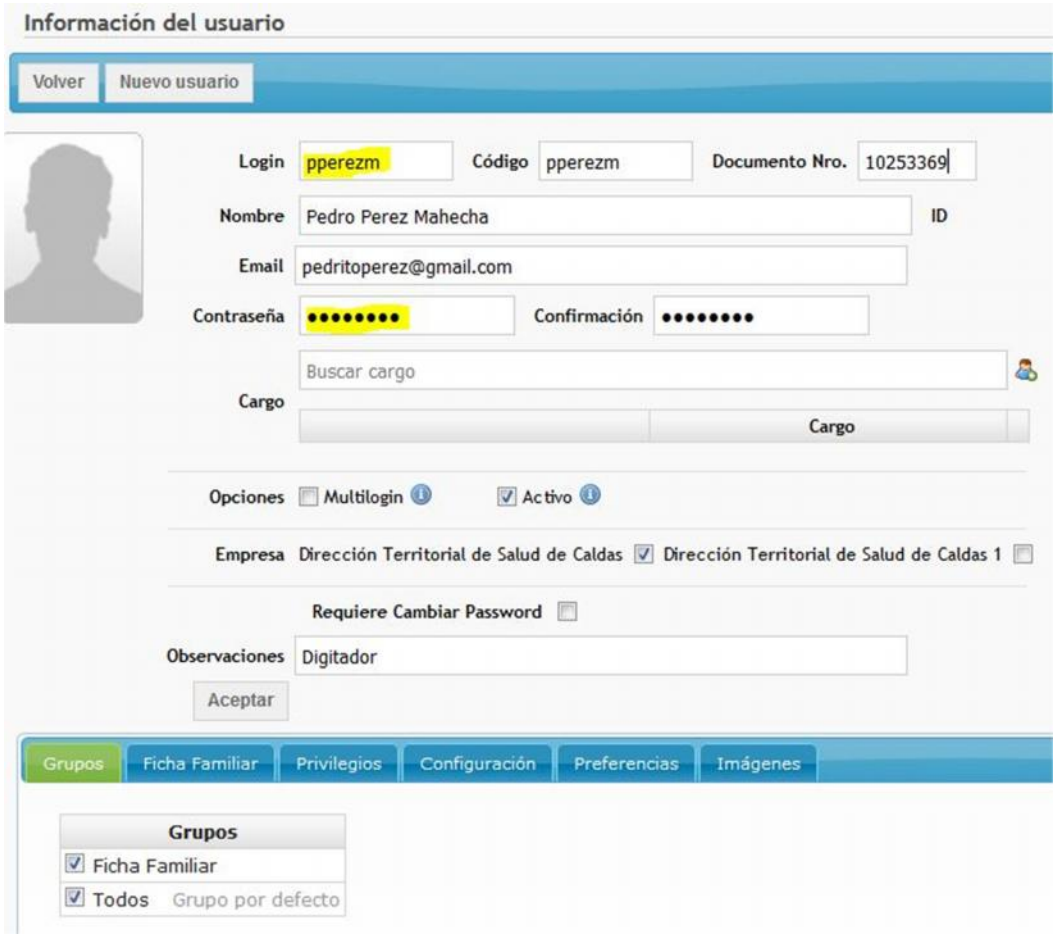
La siguiente imagen muestra los privilegios que se pueden parametrizar a cada usuario.

Figura 12. Privilegios de usuarios

Fuente: El autor.

Al verificar la parametrización y estándar que se utiliza para la creación de usuarios, se puede evidenciar que la contraseña es el mismo nombre de usuario, seguido de un numero1. Así por ejemplo, si el usuario se llama Pedro Pérez Mahecha, el usuario será: *pperezm* y la contraseña que le asigna el administrador será: *pperezm1*. Lo que es extremadamente fácil de evidenciar para cualquier usuario y no cumple con ninguna regla de validación ni de clave segura.

Figura 13. Parametrización de usuarios



Fuente: El administrador.

Se evidencia que no se solicita cambio de contraseña al primer ingreso del usuario, por lo que deja una alta vulnerabilidad, ya que quienes tengan acceso a la plataforma y se conozcan el nombre de otra persona usaría del sistema, fácilmente pueden detectar el usuario y la contraseña.

Evidencia que se envía al correo del nuevo usuario, confirmando que se ha creado el usuario.

Figura 14. Envío al correo del usuario

Buenas Tardes

Se ha creado un usuario para el municipio de La Dorada

URL: http://190.14.226.21/sgi/index.php?conid=sigdtscprd

Pedro perez Mahecha

pedritoperez@gmail.com

Celular: 3113115252

Usuario: pperezm
Contraseña: pperezm1

Cargo: Digitador

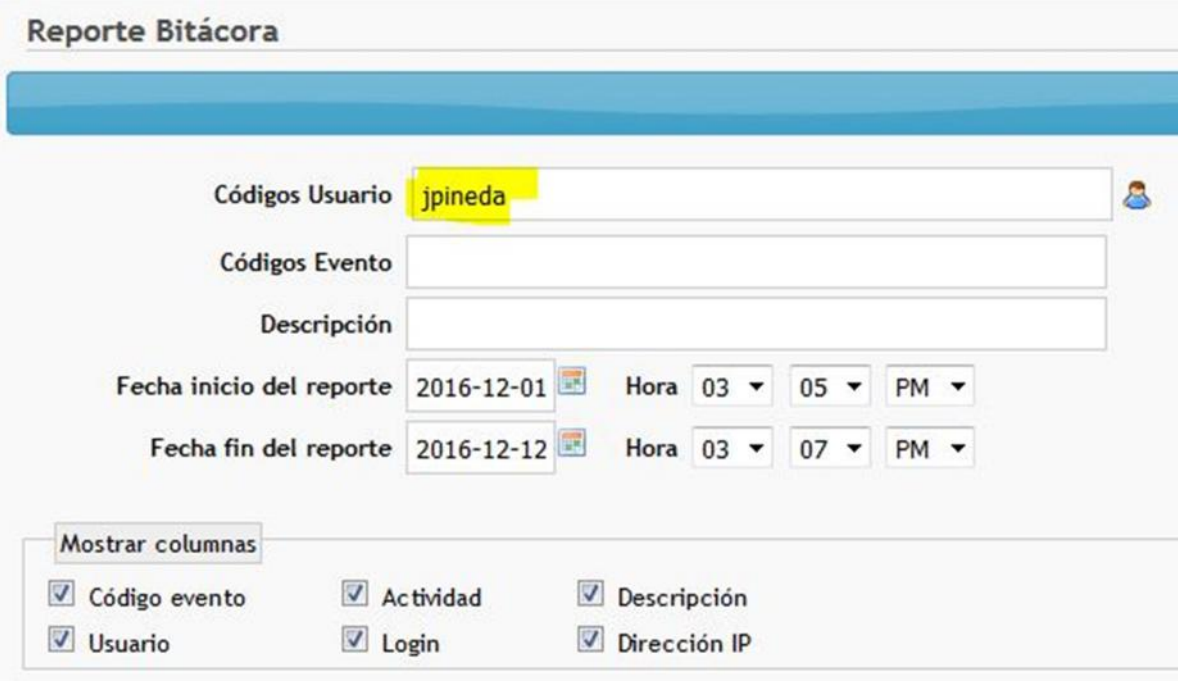
Saludos
.....

Fuente: El administrador.

Generación de eventos por Bitácora.

Relación de eventos de cada usuario, por medio del log se puede llevar una bitácora de actividades de los usuarios del sistema, lo que permite saber que actividades desarrolla cada usuario que ingresa a la plataforma.

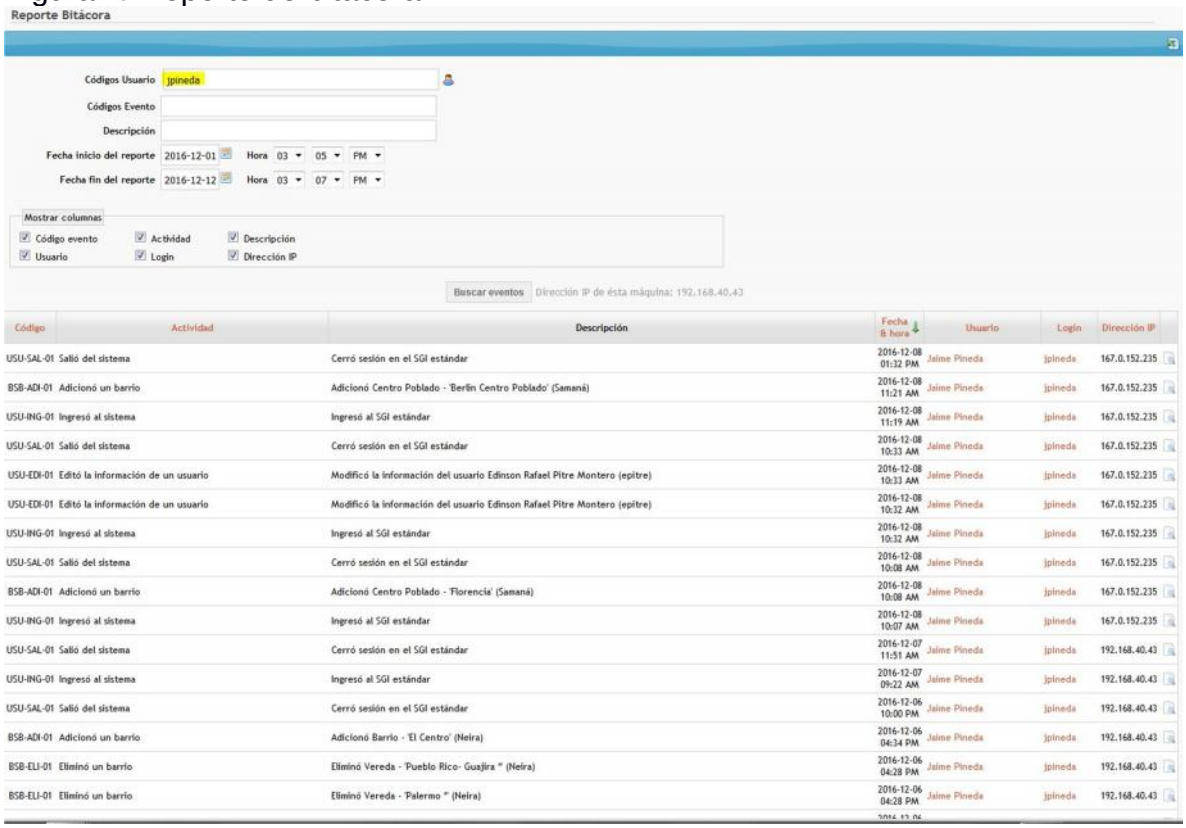
Figura 15 Generación reporte bitácora



Fuente: El administrador.

Reporte de actividades realizadas por el usuario entre un rango de fechas, según la bitácora.

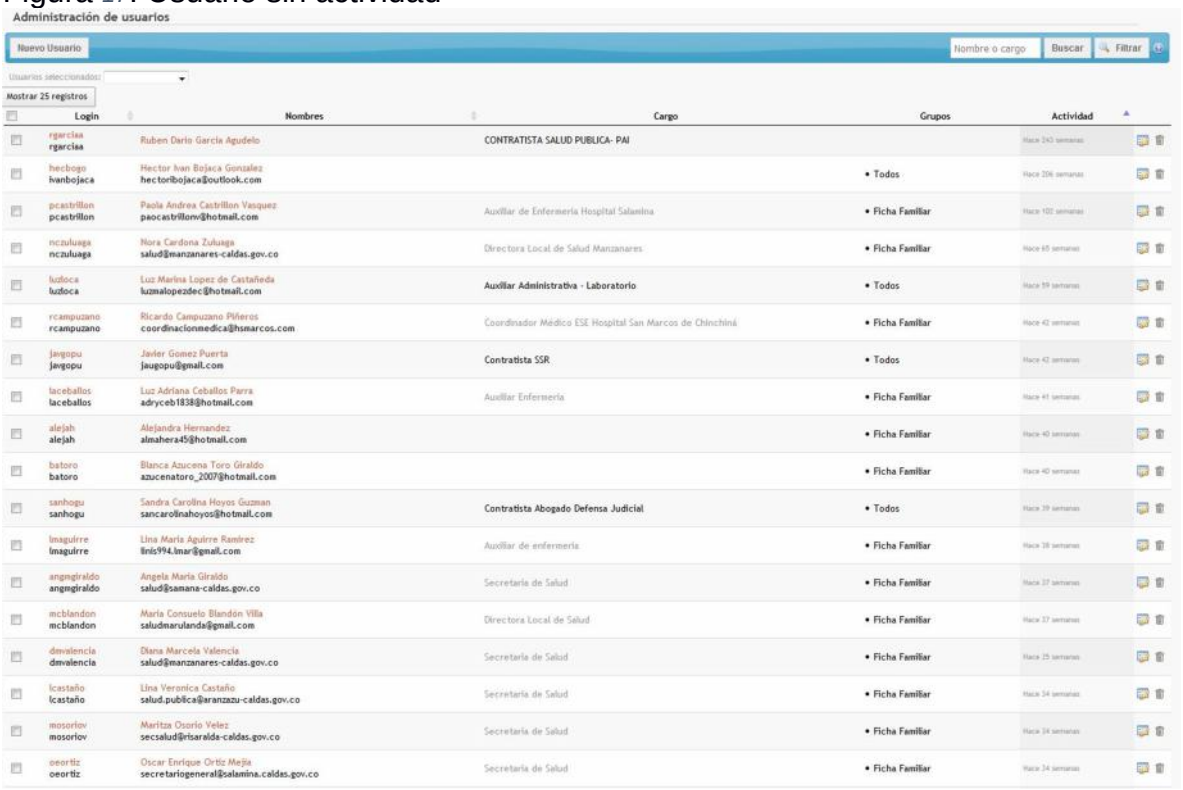
Figura *16* Reporte de bitácora



Fuente: El administrador.

Se puede generar un listado de usuarios que no han registrado actividad por semanas, para identificar quienes han dejado de utilizar la plataforma. En la siguiente imagen se pueden observar usuario que hace más de 34 semanas no ingresan a la plataforma.

Figura 17. Usuario sin actividad

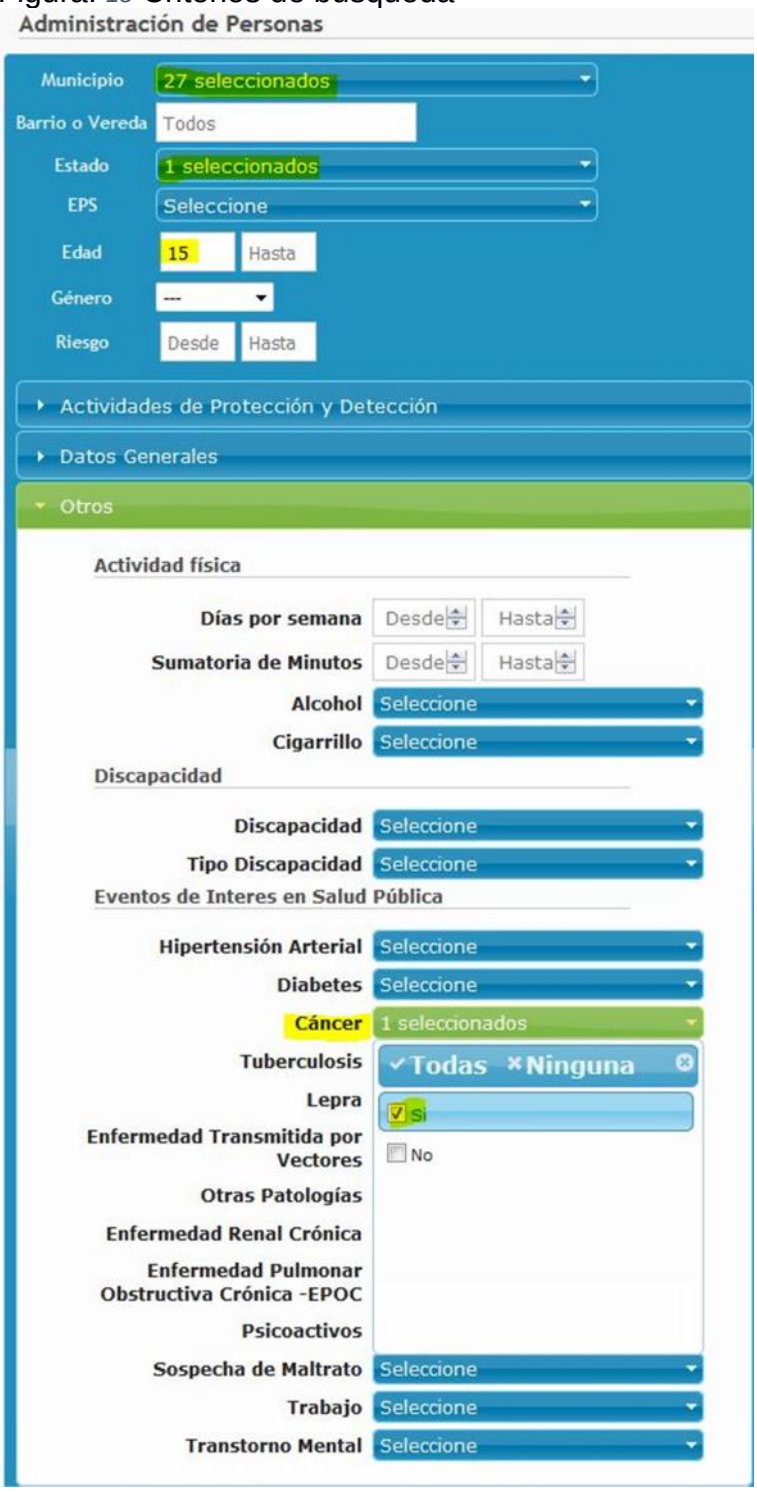


Fuente: El administrador.

Generación de archivos para exportar.

El aplicativo permite realizar consultas según criterios de búsqueda, y esta información se puede exportar a archivos de Excel, para su posterior manipulación e intervención. Un ejemplo puede ser, generar el listado de personas del departamento de caldas, que sean mayores de 15 años, y que tengan Cáncer.

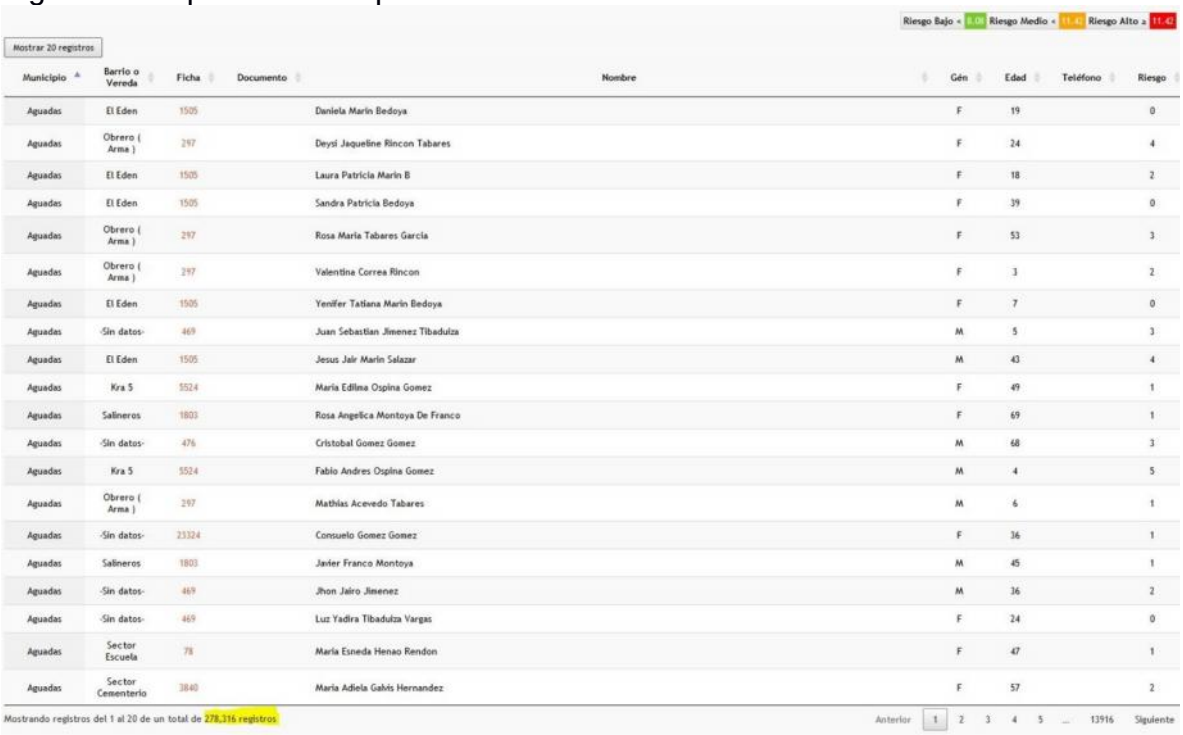
Figura. *18* Criterios de búsqueda



Fuente: El administrador.

Se genera un reporte o listado con las personas que cumplen las anteriores condiciones. (La imagen se edita y los datos de identificación se ocultan por seguridad).

Figura *19*. Reporte de búsqueda



Riesgo Bajo < 8.08 Riesgo Medio < 11.42 Riesgo Alto ≥ 11.42

Mostrar 20 registros

Municipio	Barrio o Vereda	Ficha	Documento	Nombre	Gén	Edad	Teléfono	Riesgo
Aguadas	El Eden	1505		Daniela Marin Bedoya	F	19		0
Aguadas	Obrero (Arma)	297		Deysi Jaqueline Rincon Tabares	F	24		4
Aguadas	El Eden	1505		Laura Patricia Marin B	F	18		2
Aguadas	El Eden	1505		Sandra Patricia Bedoya	F	39		0
Aguadas	Obrero (Arma)	297		Rosa Maria Tabares Garcia	F	53		3
Aguadas	Obrero (Arma)	297		Valentina Correa Rincon	F	3		2
Aguadas	El Eden	1505		Yenifer Tatiana Marin Bedoya	F	7		0
Aguadas	-Sin datos-	469		Juan Sebastian Jimenez Tibaduiza	M	5		3
Aguadas	El Eden	1505		Jesus Jair Marin Salazar	M	43		4
Aguadas	Kra 5	5524		Maria Edilma Ospina Gomez	F	49		1
Aguadas	Salineros	1803		Rosa Angelica Montoya De Franco	F	69		1
Aguadas	-Sin datos-	476		Cristobal Gomez Gomez	M	68		3
Aguadas	Kra 5	5524		Fabio Andres Ospina Gomez	M	4		5
Aguadas	Obrero (Arma)	297		Mathias Acevedo Tabares	M	6		1
Aguadas	-Sin datos-	23324		Consuelo Gomez Gomez	F	36		1
Aguadas	Salineros	1803		Javier Franco Montoya	M	45		1
Aguadas	-Sin datos-	469		Jhon Jairo Jimenez	M	36		2
Aguadas	-Sin datos-	469		Luz Yadira Tibaduiza Vargas	F	24		0
Aguadas	Sector Escuela	78		Maria Esneda Henao Rendon	F	47		1
Aguadas	Sector Cementerio	3840		Maria Adiela Galvis Hernandez	F	57		2

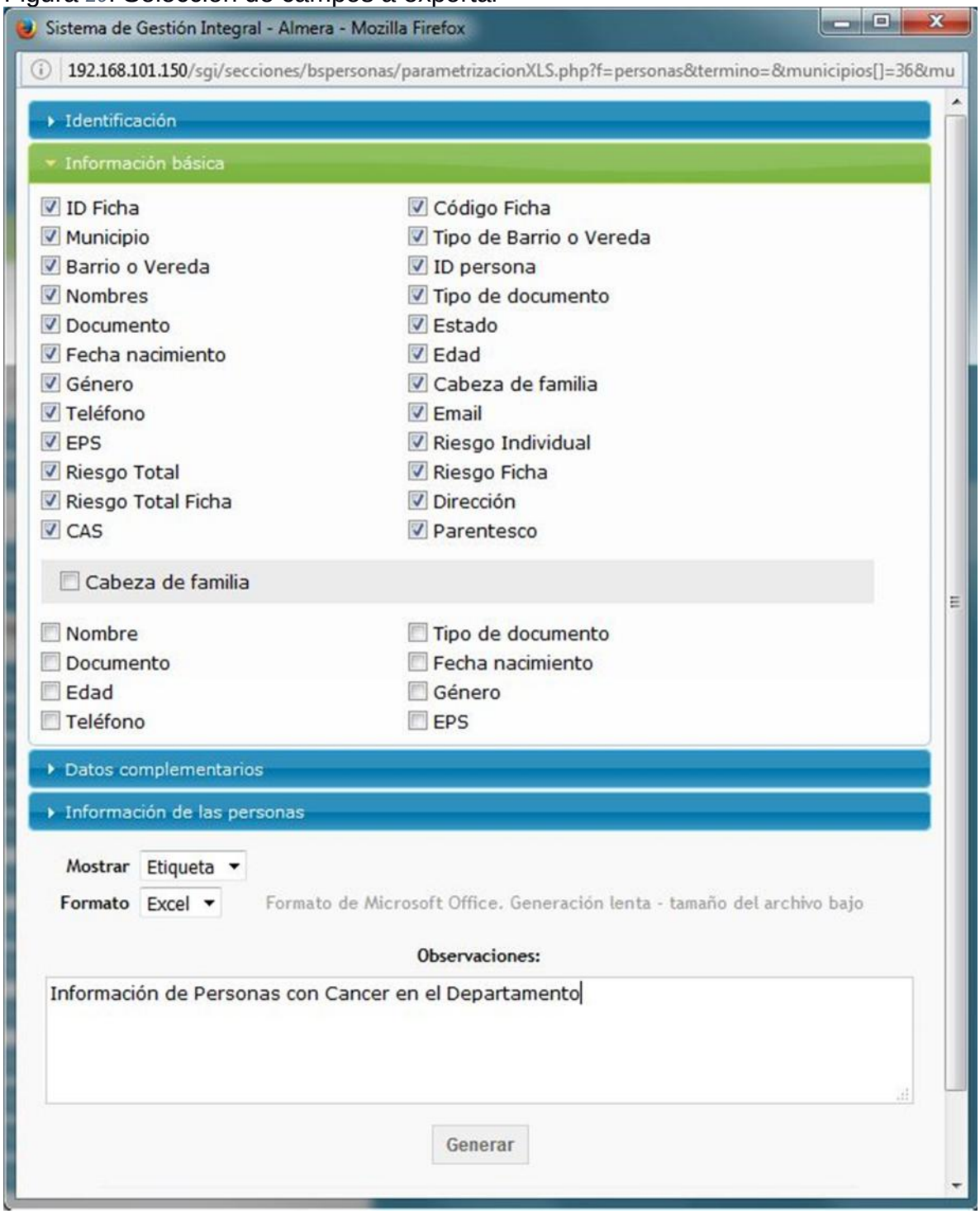
Mostrando registros del 1 al 20 de un total de 278,316 registros

Anterior 1 2 3 4 5 ... 13916 Siguiente

Fuente: El administrador.

Con este reporte se puede generar un archivo de Excel, para su análisis, manipulación e intervención. Se seleccionan los campos que se requieran en el archivo de Excel.

Figura 20. Selección de campos a exportar

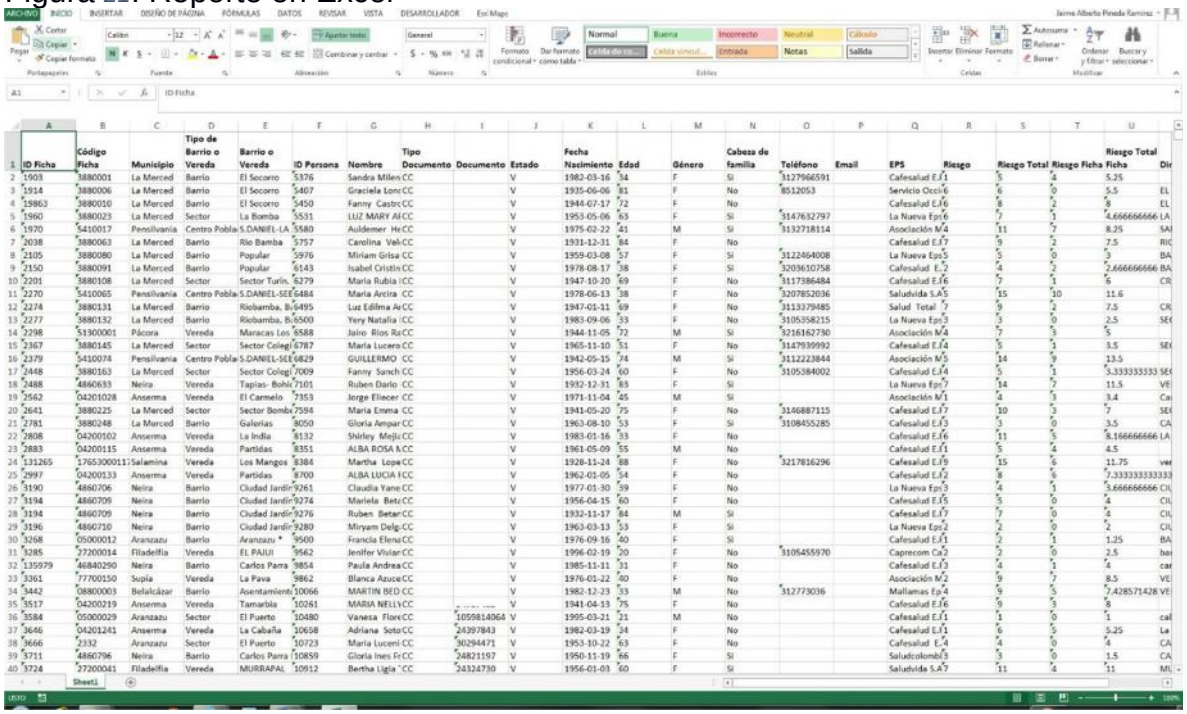


Fuente: El administrador.

Se genera un archivo de Excel con la información seleccionada y con los registros de las personas de acuerdo a los criterios de búsqueda. Este archivo contiene

información personal y sensible de las personas que padecen cáncer. (La imagen se edita y los datos de identificación se ocultan por seguridad).

Figura *21*. Reporte en Excel



ID Ficha	Código Ficha	Municipio	Tipo de Barrio o Vereda	Barrio o Vereda	ID Persona	Nombre	Tipo Documento	Documento	Estado	Fecha Nacimiento	Edad	Género	Cabeza de familia	Teléfono	Email	EPS	Riesgo	Riesgo Total	Riesgo Ficha	Riesgo Total Ficha
1903	3880001	La Merced	Barrio	El Socorro	5376	Sandra Milen	CC		V	1982-03-16	34	F	Si	3127966591		Cafesalud E.I	1	5	4	5.25
1914	3880006	La Merced	Barrio	El Socorro	5407	Graciela Lonc	CC		V	1935-06-06	81	F	No	8512053		Servicio Occi	1	6	0	5.5
19863	3880010	La Merced	Barrio	El Socorro	5450	Fanny Castro	CC		V	1944-07-17	72	F	No			Cafesalud E.I	1	8	2	8
1960	3880023	La Merced	Sector	La Bomba	5531	LUZ MARY AI	CC		V	1953-05-06	63	F	Si	3147632797		La Nueva Eps	1	7	1	4.666666666
1970	5410017	Pensilvania	Centro Pobla	S.DANIEL-LA	5580	Auldemer He	CC		V	1975-02-22	41	M	Si	3132718114		Asociación M	1	11	7	8.25
2038	3880063	La Merced	Barrio	Rio Bamba	5757	Carolina Vel	CC		V	1931-12-31	84	F	No			Cafesalud E.I	1	9	2	7.5
2105	3880080	La Merced	Barrio	Popular	5976	Miriam Grisa	CC		V	1959-03-08	57	F	Si	3122464008		La Nueva Eps	1	5	0	3
2150	3880091	La Merced	Barrio	Popular	6143	Isabel Cristin	CC		V	1978-08-17	38	F	Si	3203610758		Cafesalud E.I	2	4	2	2.666666666
2201	3880108	La Merced	Sector	Sector Turin	6279	Maria Rubia	CC		V	1947-10-20	69	F	No	3117386484		Cafesalud E.I	1	7	1	6
2270	5410065	Pensilvania	Centro Pobla	S.DANIEL-SE	6484	Maria Areira	CC		V	1978-06-13	38	F	No	3207852036		Saludvida S.A	5	15	10	11.6
2274	3880131	La Merced	Barrio	Riobamba, B	6495	Luz Edilma Ar	CC		V	1947-01-11	69	F	No	3133379485		Salud Total	1	9	2	7.5
2277	3880132	La Merced	Barrio	Riobamba, B	6500	Yery Natalia	CC		V	1983-09-06	33	F	No	3105358215		La Nueva Eps	3	3	0	2.5
2298	51300001	Pácora	Vereda	Maracas Los	6588	Jairo Rios Ra	CC		V	1944-11-05	72	M	Si	3216162730		Asociación M	4	7	3	5
2367	3880145	La Merced	Sector	Sector Colegi	6787	Maria Lucero	CC		V	1965-11-10	51	F	No	3147939992		Cafesalud E.I	4	5	1	3.5
2379	5410074	Pensilvania	Centro Pobla	S.DANIEL-SE	6829	GUILLERMO	CC		V	1942-05-15	74	M	Si	3112223844		Asociación M	5	14	9	13.5
2448	3880163	La Merced	Sector	Sector Colegi	7009	Fanny Sanch	CC		V	1956-03-24	60	F	No	3105384002		Cafesalud E.I	4	5	1	3.333333333
2488	4860633	Neira	Vereda	Tapias- Bohí	7101	Ruben Dario	CC		V	1932-12-31	83	F	Si			La Nueva Eps	7	14	7	11.5
2562	04201028	Anserma	Vereda	El Carmelo	7353	Jorge Eliecer	CC		V	1971-11-04	45	M	Si			Asociación M	1	4	3	3.4
2641	3880225	La Merced	Sector	Sector Bomb	7594	Maria Emma	CC		V	1941-05-20	75	F	No	3146887115		Cafesalud E.I	7	10	3	7
2781	3880248	La Merced	Barrio	Galerias	8050	Gloria Ampar	CC		V	1963-08-10	53	F	Si	3108455285		Cafesalud E.I	3	3	0	3.5
2808	04200102	Anserma	Vereda	La India	8132	Shirley Mejía	CC		V	1983-01-16	33	F	No			Cafesalud E.I	6	11	5	8.166666666
2883	04200115	Anserma	Vereda	Partidas	8351	ALBA ROSA M	CC		V	1961-05-09	55	M	No			Cafesalud E.I	1	5	4	4.5
131265	17653000115	Salamina	Vereda	Los Mangos	8384	Martha Lopez	CC		V	1928-11-24	88	F	No	3217816296		Cafesalud E.I	9	15	6	11.75
2997	04200133	Anserma	Vereda	Partidas	8700	ALBA LUCIA H	CC		V	1962-01-05	54	F	No			Cafesalud E.I	2	8	6	7.333333333
3190	4860706	Neira	Barrio	Ciudad Jardín	9261	Claudia Yane	CC		V	1977-01-30	59	F	No			La Nueva Eps	3	4	1	5.666666666
3194	4860709	Neira	Barrio	Ciudad Jardín	9274	Mariela Betz	CC		V	1956-04-15	60	F	No			Cafesalud E.I	5	5	0	4
3194	4860709	Neira	Barrio	Ciudad Jardín	9276	Ruben Betar	CC		V	1932-11-17	84	M	Si			Cafesalud E.I	7	7	0	4
3196	4860710	Neira	Barrio	Ciudad Jardín	9280	Miryam Delg	CC		V	1963-03-13	53	F	Si			La Nueva Eps	2	2	0	2
3268	05000012	Aranzazu	Barrio	Aranzazu *	9500	Francia Elena	CC		V	1976-09-16	40	F	Si			Cafesalud E.I	1	2	1	1.25
3285	27200014	Filadelfia	Vereda	EL PAIUI	9562	Jenifer Vivian	CC		V	1996-02-19	20	F	No	3105455970		Caprecom Ca	2	2	0	2.5
135979	46840290	Neira	Barrio	Carlos Parra	9854	Paula Andrea	CC		V	1985-11-11	31	F	No			Cafesalud E.I	3	4	1	4
3361	77700150	Supía	Vereda	La Pava	9862	Blanca Azuce	CC		V	1976-01-22	40	F	No			Asociación M	2	9	7	8.5
3442	08800003	Belalcázar	Barrio	Asentamiento	10066	MARTIN BEO	CC		V	1982-12-23	33	M	No	312773036		Mallamas Ep	4	9	5	7.428571428
3517	04200219	Anserma	Vereda	Tamarbla	10261	MARIA NELLY	CC		V	1941-04-13	75	F	No			Cafesalud E.I	6	9	3	8
3584	05000029	Aranzazu	Sector	El Puerto	10480	Vanesa Flore	CC	1059814064	V	1995-03-21	21	M	No			Cafesalud E.I	1	1	0	1
3646	04201241	Anserma	Vereda	La Cabaña	10658	Adriana Soto	CC	24397843	V	1982-03-19	34	F	No			Cafesalud E.I	1	6	5	5.25
3666	2332	Aranzazu	Sector	El Puerto	10723	Maria Lucen	CC	30294471	V	1953-10-22	63	F	No			Cafesalud E.A	4	4	0	4
3711	4860796	Neira	Barrio	Carlos Parra	10859	Gloria Ines Fr	CC	24821197	V	1950-11-19	66	F	Si			Saludcolombi	5	5	0	1.5
3724	27200041	Filadelfia	Vereda	MURRAPAL	10912	Bertha Ligia	CC	24324730	V	1956-01-03	60	F	Si			Saludvida S.A	7	11	4	11

Fuente: El administrador.

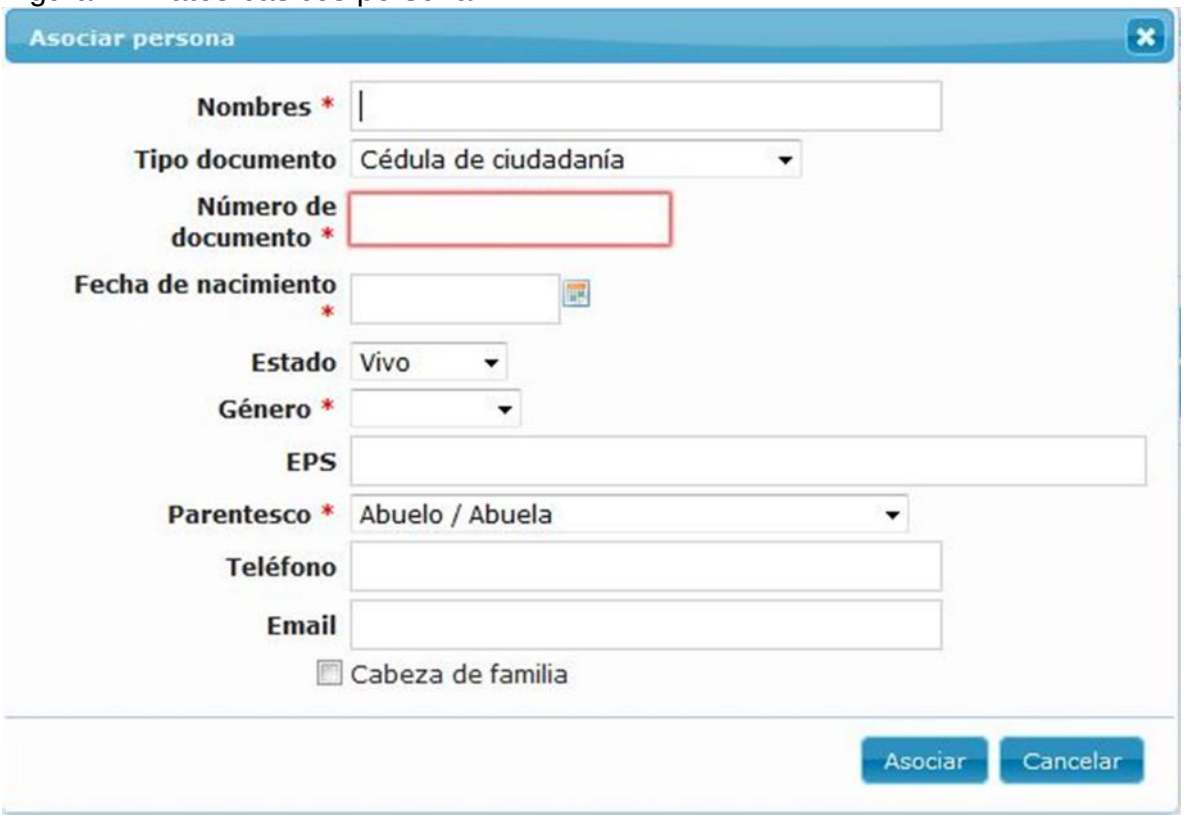
Como el anterior ejemplo se puede generar información de personas con criterios de búsqueda por:

- Municipio
- Barrio
- EPS
- Eventos de interés en salud pública (hipertensión arterial, diabetes, cáncer, tuberculosis, lepra, enfermedad transmitida por vectores, enfermedad renal crónica, enfermedad pulmonar crónica, sospecha de maltrato, consumo de sustancias psicoactivas, trastorno mental).
- Analfabetismo (lee, escribe)
- Ausentismo escolar
- Esquema de vacunación
- Estado nutricional
- Gestación
- Lactancia
- Planificación familiar
- Citología
- Discapacidad

- Entorno de la vivienda (acueducto, alcantarillado, estado de vivienda, etc.)

Al momento de la caracterización se toman datos básicos de la persona como nombre, identificación, fecha de nacimiento, sexo, parentesco, EPS a la que pertenece, numero celular, correo electrónico, dirección, barrio, ciudad.

Figura 22. Datos básicos persona



Fuente: El administrador.

- **Valoración política de seguridad física.**

Cuadro 5. Valoración política de seguridad física.

Política	***Se cumple***	
	Si	***No***
Acceso Físico		
La entidad dispone de un área exclusiva para el centro de cómputo y comunicaciones, donde se ubicarán los sistemas de telecomunicaciones y servidores	X	
Los sistemas de comunicaciones están protegidos de tal forma que no se tenga acceso físico fácilmente.	X	

Política	***Se cumple***	
	Si	***No***
Cuadro 5 (continuación)		
El acceso de terceras personas debe ser registrado, debidamente identificado y vigilado, portara un carnet que le es asignado por el área de seguridad de las instalaciones.		X
Las visitas de personas internas o externas de la institución, a las áreas seguras de los centros de cómputo procesamiento y comunicaciones, serán supervisadas por un empleado de la dependencia de sistemas.		X
Las visitas a los centros de cómputo, procesamiento y comunicaciones se realizaran en un horario establecido por la dirección de sistemas.		X
El personal responsable y autorizado de mover, cambiar, extrae cualquier elemento de computo será únicamente empleados del área de sistemas.	X	
Data Center		
Tener una puerta de acceso de vidrio templado transparente.	X	
Ser un área restringida, con control de acceso, el acceso será solo del personal autorizado.	X	
Mantener libre de polvo.	X	
Poseer elementos para medir temperatura.	X	
Mantener temperatura a 21 grados centígrados.	X	
Respaldo de energía redúndate.	X	
Estándares de protección eléctrica vigente.	X	
Sistema de tierra y protección e instalaciones eléctricas.	X	
Control de humedad		X
Prevención y protección de incendios.	X	
Sistema de Extinción.	X	
Infraestructura		
Cableado estructurado con estándares vigentes		X
Resguardo de equipos de cómputo bajo supervisión del área de sistemas.	X	
Instalaciones de equipos de cómputo		
Contar con planos actualizados de las instalaciones eléctricas y de comunicaciones de la red.	X	
Las instalaciones eléctricas y de comunicaciones están resguardadas del paso de personas y libres de interferencias electromagnéticas.	X	

Política	***Se cumple***	
	Si	***No***
Cuadro 5 (continuación)		
Control		
Se lleva un control total y sistematizado de los recursos de cómputo y licenciamiento.	X	
Cuando ingresa o se retira un empleado a la estructura orgánica de la institución el área de talento humano le avisa al área de sistemas para activar o desactivar el respectivo usuario.		X
Respaldos		
Las Bases de Datos serán respaldadas según plan de respaldos implementado por la entidad. Contemplando copias completas e incrementales.	X	
Las Bases de Datos deberán de tener una réplica en uno o más equipos remotos en lugares seguros.	X	
Copias de los respaldos deberán estar almacenados en un lugar seguro y distante a la institución.	X	
Los usuarios tendrán un árbol de directorios configurado para realizar respaldo de forma automática, debidamente configurado por el área de sistemas.		X
Los usuarios deberán solicitar al área de sistemas realizar respaldo de información que este por fuera de las anteriores proposiciones.		X
Uso		
Los usuarios deberán hacer uso adecuado de los recursos tecnológicos de cómputo y de red que la institución ha puesto a su disposición y de los demás empleados.	X	
Los usuarios solo solicitaran apoyo en problemas tecnológicos al personal autorizado del área de sistemas.	X	
El correo electrónico institucional será de uso exclusivo para las actividades laborales.		X
Derechos de Autor		
Se establece como prohibición la inspección, copia y almacenamiento de programas, software o fuentes que vayan contra las leyes de derecho de autor.	X	
Se establece como prohibición realizar copias de los programas propios o utilitarios instalados en la institución.	X	

Política	***Se cumple***	
	Si	***No***
Cuadro 5 (continuación)		
Se prohíbe instalar programas o software, solo el personal autorizado del área de sistemas lo puede realzar.	X	
Si se va a utilizar software libre, solo el personal del área de sistemas tendrá la faculta de instalarlo, y con previa solicitud para verificar el sistema de licenciamiento.		X
Se prohíbe descargar música y videos de internet.		X
Se prohíbe utilizar el interne de la entidad para escuchar música, ver videos o TV en línea.		X
Si se descubre a algún empleado realizando copias del software de la institución se procede a iniciar un proceso disciplinario.	X	
El personal del área de sistemas realizara periódicamente una revisión a los equipos de cómputo de los usuarios para verificar el inventario del software instalado.		X
Se establece desde la configuración del usuario que no pueda instalar ningún software.	X	
Si por algún motivo se encuentra software que no cumpla con los requisitos de licenciamiento, se procede a desinstalar e iniciar proceso de control interno contra el usuario.	X	
Lo usuarios NO utilizan la intranet para compartir música, videos o información personal		X
Lo usuarios que se enteren que alguno de sus compañeros está realizando actos que van en contra de los políticas aquí estipuladas deberán notificar al superior o al área de sistemas directamente.		X
Los usuarios que no apliquen las anteriores políticas anteriormente estipuladas serán sujetos a sanciones disciplinarias de la oficina de control interno.		

Fuente: Dirección Territorial de Salud de Caldas.

- **Valoración política de seguridad lógica.**

Cuadro *6*. Valoración política de seguridad lógica.

Política	***Se cumple***	
	Si	***No***
Red		
Cuadro 6 (continuación)		
La responsabilidad de los datos que se transmitan por la red, y emitidos desde un equipo de cómputo será únicamente responsabilidad del usuario	X	
No se puede destruir, eliminar o barrar información de los equipos de cómputo, sin la debida autorización del usuario propietario de los datos.		X
La red de datos será exclusivamente para las actividades laborales.		X
Las cuentas de usuarios serán controladas y configuradas únicamente por el área de sistemas.	X	
Software para realizar análisis del comportamiento de la red, será una actividad solo del área de sistemas.	X	
El mantenimiento preventivo y correctivo de la red de datos será realizado únicamente por el personal de sistemas.	X	
Todos los equipos portátiles y dispositivos móviles que se conecten al wifi, deben hacer la respectiva solicitud al área de sistemas.	X	
Los equipos conectados a los wifi de la institución están debidamente registrados en la bitácora de la oficina de sistemas.		X
Para los empleados se utilizar la red de wifi de PC-DTSC		X
Para los visitantes se utilizara la red de wifi PC-Visitantes		X
Correo electrónico		
Solo se utilizaran correos electrónicos institucionales		X
La creación de correos institucionales solo se realizara por parte del personal del área de sistemas.	X	
Para crear una cuenta de correo institucional a un empleado de la institución, la oficina de talento humano deberá expedir al área de sistemas una certificación de la vinculación laboral.	X	
Al ingresar a la cuenta de correo electrónico por primera vez, se le solicitara al usuario cambiar la contraseña.		X

Política	*Se cumple*	
	Si	*No*
Cuadro 6 (continuación)		
La longitud de las contraseñas será igual o superior a ocho caracteres influyendo alfanuméricos y caracteres especiales.		X
La información enviada desde la institución a correos electrónicos será de cuentas oficiales.		X
Ingeniero de soporte		
Podrán ingresar de forma remota a los equipos, únicamente cuando se reporte un daño por parte de usuario responsable.	X	
Utilizaran analizadores de información y software, bajo la presencia y autorización del usuario propietario.	X	
Ayudar al control de los respaldos de los usuarios e institución	X	
Registraran cada una de los elementos de cómputo en el inventario de activos de sistemas, con su respectiva hoja de vida.		X
Realiza la instalación de los equipos de cómputo y comunicaciones.	X	
Son las únicas personas autorizadas para mover o cambiar de sitio los equipos de cómputo y comunicaciones.	X	
Son los encargados de informar a su superior, a la dirección general o dirección de sistemas sobre los hallazgos realizados.	X	

Fuente: Dirección Territorial de Salud de Caldas.

- **Valoración uso de servicios de la Red.**

Cuadro 7. Valoración uso de servicios de la Red.

Política	*Se cumple*	
	Si	*No*
Gerencias		
No se darán usuarios, ni contraseñas a quienes estén desarrollando pasantías de universidades.	X	
Revisar logs constantemente		X
Monitoria los recursos de red		X

Política	*Se cumple*	
	Si	*No*
Identificación de usuarios y contraseñas		
Cuadro 7 (continuación)		
Todos y cada uno de los usuarios de la red o sistemas de información tendrán un solo acceso con información de nombre de usuario y contraseña	X	
Ningún empleado recibirá usuarios o contraseñas sin que la oficina de talento humano expida la respectiva certificación de que existe una relación contractual.	X	
El empleado deberá aceptar y conocer las políticas de seguridad establecidas por la entidad, hasta ese momento se le configurara usuario y contraseña.		X
La oficina de sistemas le definirá el nombre de usuario.	X	
El usuario definirá su propia contraseña de acuerdo al estándar de longitud y caracteres especiales.	X	
Se configuraran los usuarios para que cada dos meses se les solicite cambio de contraseña		
Los usuarios solo podrán ingresar a los datos que se le parametrizen con el usuario, de acuerdo al rol.	X	

Fuente: Dirección Territorial de Salud de Caldas.

- **Valoración directivas servidor**

Cuadro *8*. Valoración directiva del servidor.

Directivas	*Se cumple*	
	Si	*No*
Una sola cuenta por cada usuario	X	
Contraseñas con longitud y caracteres especiales de acuerdo al estándar solicitado		X
Bloqueo de lectura de medios de almacenamiento removibles.	X	
Bloque de página de Facebook	X	
Bloque de página de YouTube		X
Bloqueo de páginas para adultos	X	
Bloqueo de páginas de no interés.	X	
Bloqueo de descarga de música y videos		X
Cambio de contraseña obligatorio cada dos mese	X	
Límite de usuarios del sistema.		X

Directivas	Se cumple	
	Si	No
Cuadro 7 (continuación)		
Límite de usuarios para ingreso a la plataforma “Gestión Integrada de Bienestar Social”		X
Configuración de respaldos en sitio	X	
Configuración de respaldos remotos	X	
Perfiles de usuarios según requerimientos		X
Perfiles con privilegios según requerimientos		X

Fuente: Dirección Territorial de Salud de Caldas.

Pruebas para determinar y verificar las vulnerabilidades que se puedan encontrar

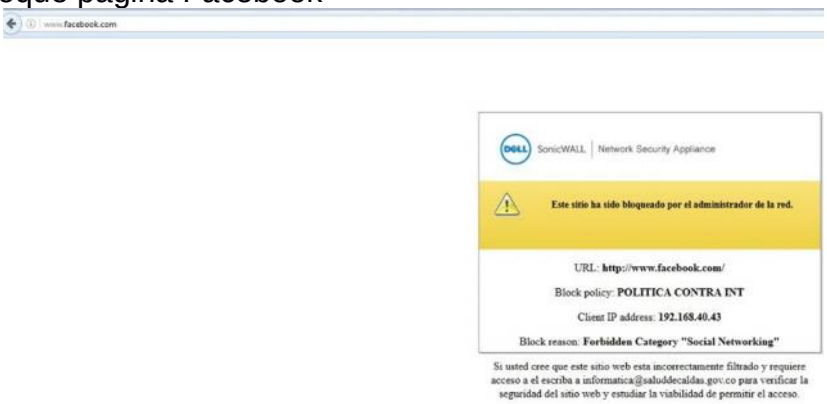
Usuario: Jaime Alberto Pineda, ingeniero de sistemas del observatorio social de salud pública.

Figura 23. Usuario Jaime Pineda

Fuente: Usuario Jaime Pineda

Intento de ingresar a la página de Facebook desde la cuenta del usuario Jaime Pineda.

Figura *24*. Bloque página Facebook



Fuente: Usuario Jaime Pineda

Ingreso a correos personales desde el usuario Jaime Pineda.

Figura *25*. Correo usuario Jaime Pineda

Fuente: Usuario Jaime Pineda

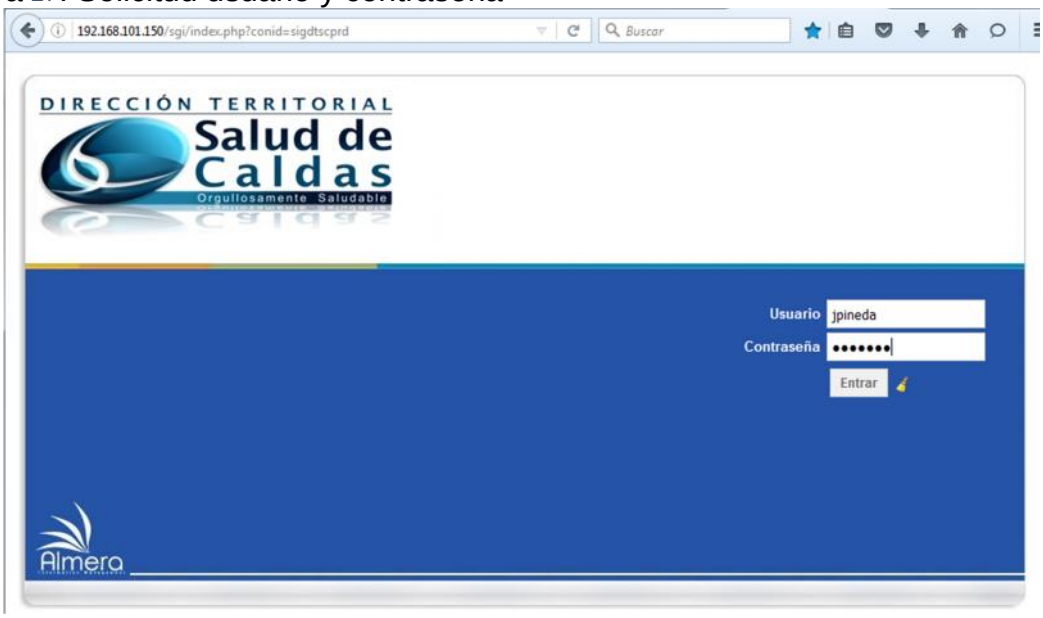
Protección con antivirus en los PCs de escritorio, portátiles y servidores, se evidencia que la institución utiliza el antivirus ESET Antivirus, y se encuentra actualizado en los equipos que se verificaron en forma aleatoria.

Figura 26. Antivirus ejecutándose.

Fuente: Usuario Jaime Pineda

Ingreso al sistema “Gestión Integrada de Bienestar Social” desde el usuario Jaime Pineda, se puede observar que utilizan un estándar de nombre y contraseña de usuario.

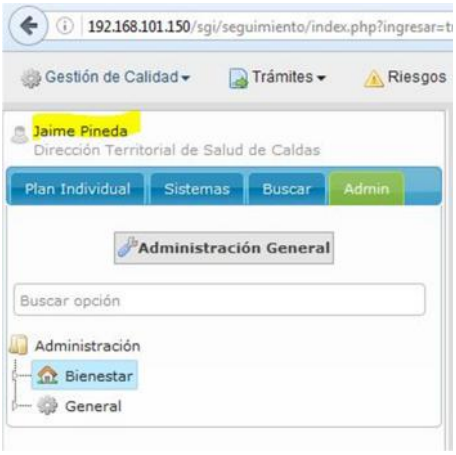
Figura 27. Solicitud usuario y contraseña



Fuente: Usuario Jaime Pineda

Usuario Jaime Pineda en el sistema “Gestión Integrada de Bienestar Social”.

Figura *28*. Usuario Jaime Pineda



Fuente: Usuario Jaime Pineda.

- Usuario: Carmenza Osorio Gómez, epidemióloga de la institución quien cumple funciones en el sistema de vigilancia de las enfermedades de salud pública y esta alerta de las cantidades y porcentajes de personas que está padeciendo alguna de esas enfermedades.

Figura *29*. Usuario Carmenza Osorio

Fuente: Usuario Carmenza Osorio.

En la siguiente imagen se pude apreciar que el equipo del usuario Carmenza Osorio permite leer memorias USB y discos duros extraíbles.

Figura *30*. Unidades Extraíbles.

Fuente: El autor.

En la siguiente imagen se evidencia que el usuario Carmenza Osorio puede navegar en YouTube y se encuentra escuchando música conectada desde la red de la institución.

Figura *31*. Página de YouTube.

Fuente: El autor.

Conclusiones de las pruebas realizadas

- Desde un navegador web se puede ingresar al árbol de directorios, lo que implica que la toda la información tanto del aplicativo como de los bases de datos esta expuestas a cualquier intruso. Se debería tener controles de seguridad de bloqueos implementados.

- Se puede ingresar a correos personales utilizando los usuarios, equipos y red de la institución, lo que no debería suceder para este fin y más si es una institución que maneja información sensible. Para lo cual debería esta implementada una política o normatividad.

- Se puede navegar en YouTube y están reproduciendo videos desde un usuario, equipo y red de la institución. Para lo cual debería estar implementada una política o normatividad.

- Permite conectar memorias USB o disco duros extraíbles a los Pc de la institución, los cuales permiten extraer información sensible, permite el ingreso de virus y está considerado como una vulnerabilidad y amenaza. Para lo cual debería estar implementada una política o normatividad.

Se determina que no se están aplicando ciertas políticas de seguridad por que no están implementadas en todos los usuarios y PCs de la institución, y el personal de sistemas no se ha percatado de las vulnerabilidades que se están presentando.

Cuadro *9* Valoración vulnerabilidad

Vulnerabilidad	Severidad del daño	Posibilidad de ocurrencia del daño	Nivel del riesgo
Permite ingreso al árbol de directorios	4	4	Alto
Se permite ingreso a correos electrónicos personales	3	3	Medio
Permite ingresar a página de YouTube	2	3	Bajo
Permite uso de unidades de almacenamiento externas	3	4	Alto

Fuente: El autor.

4.3 INFORME FINAL DE AUDITORÍA

Después de haber realizado las respectivas visitas, reuniones, pruebas, verificaciones, inspecciones y análisis, matrices de riesgo e impacto, se puede evidenciar que la Dirección Territorial de Salud de caldas tiene implementado un sistema de seguridad al sistema “Gestión Integrada de Bienestar Familiar”, con políticas de seguridad claras y funcionando. Pero que realizada la auditoría al sistema de seguridad, se evidencias vulnerabilidades y se procede a realizar una lista de hallazgos.

- **Análisis de Vulnerabilidades**

  - **Hallazgo 1.**

Se puede evidenciar que desde una navegador y con la dirección IP se puede acceder a del árbol de directorios del banco de ofertas, que hace parte de sistema “Gestión Integrada de Bienestar Familiar”, encargado de brindar información de ayudas disponibles a la comunidad. Esto sucede porque los datos enviados en las URLs utilizadas por la aplicación Web son enviados por el método GET, lo que posibilita acceder al árbol de directorios y a la información.

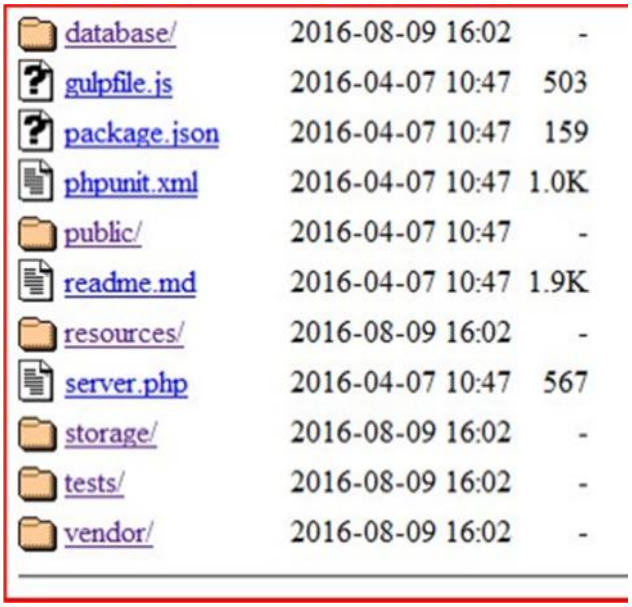
Árbol de directorios.

Figura 32. Información del árbol de directorios

Fuente: El autor.

Archivos

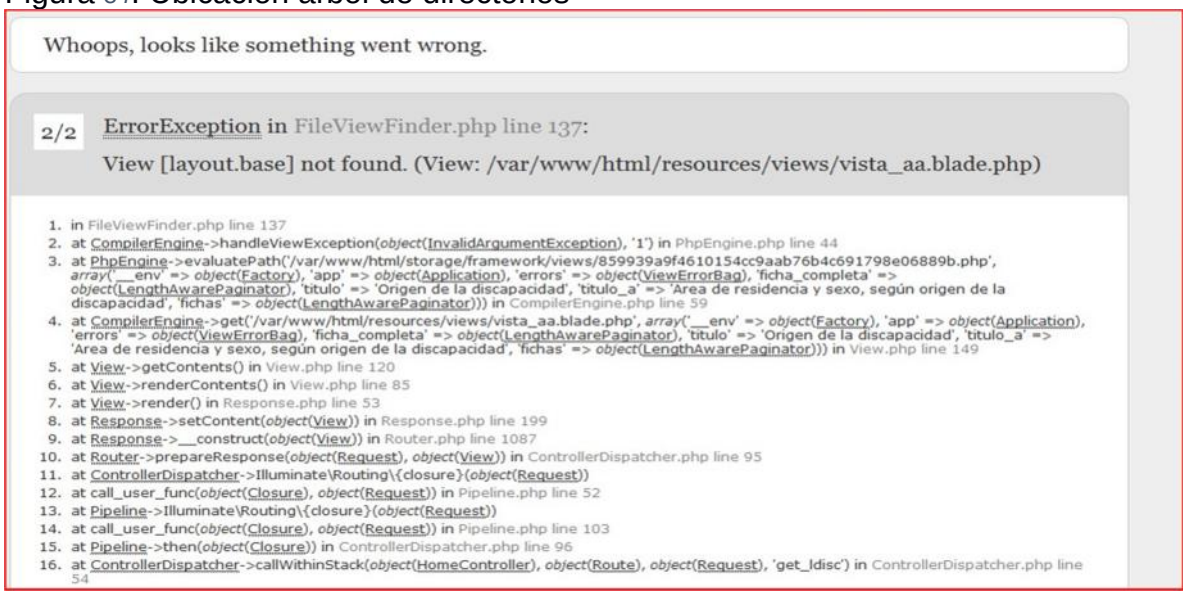
Figura 33. Archivos árbol de directorio



Fuente: El autor.

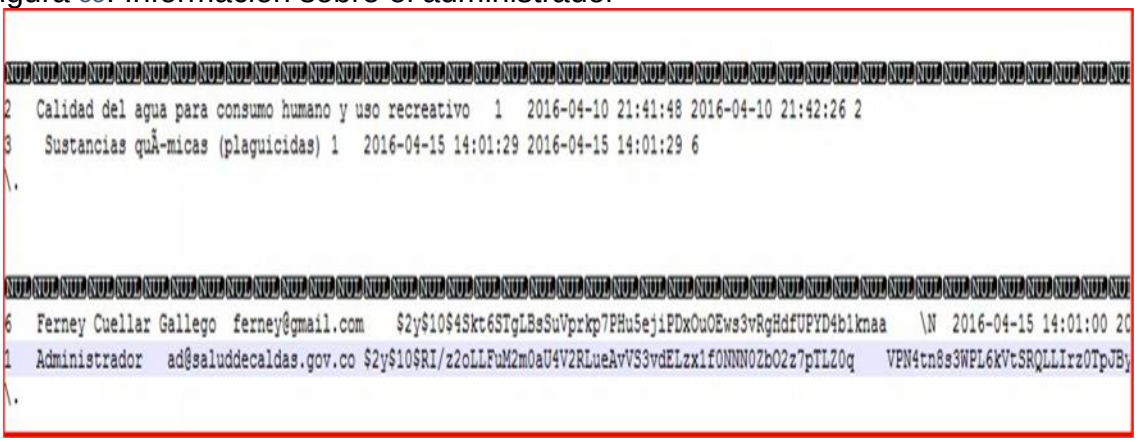
Ruta de la ubicación del árbol de directorios.

Figura 34. Ubicación árbol de directorios



Fuente: El autor.

Figura 35. Información sobre el administrador



Fuente: El autor.

- **Hallazgo 2.**

Se evidencia que se puede navegar en páginas no permitidas y que deberían estar bloqueadas desde el software de administración de navegación, como lo especifica el manual de políticas de calidad. Se comprueba navegación de la página YouTube, lo que implica que muchos usuarios de la red de la entidad estén escuchando música constantemente y utilicen parte del ancho de banda, necesario para actividades propias o de interés de la empresa.

Figura 36. Navegación en páginas que deben estar bloqueada

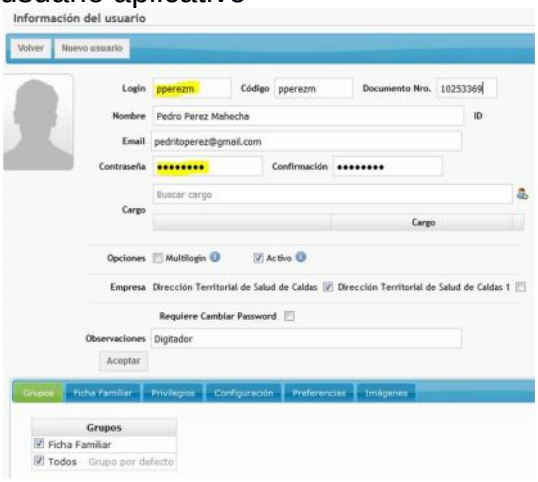
Fuente: El autor.

- **Hallazgo 3**

Se evidencia que no existen criterios establecido para la creación de usuarios para ingresar al sistema “Gestión Integrada de Bienestar Familiar”, ya que la normalización que establecen no es acorde a las políticas de seguridad y no cumple con los parámetros de contraseñas seguras. Siempre se toma como nombre de usuario la primera letra del nombre, seguido del primer apellido y primera letra del segundo apellido. Y la contraseña que se aplica es el mismo nombre de usuario y le adicionan un numero 1.

Ejemplo: Para crear el usuario a la persona Pedro Pérez Mahecha, le establecen como nombre de usuario pperezm. Y la contraseña es pperezm1.

Figura 37. Información usuario aplicativo



Fuente: El administrador.

Información que se envía al correo del nuevo usuario, donde se vuelve a evidenciar que el nombre del usuario y la contraseña solo se diferencia por un numero 1. Y contempla la información del nombre de la persona. Si alguna persona detalla la forma como se estructuran los nombres de los usuarios y las contraseñas, fácilmente va a poder ingresar a la plataforma con la información de otro usuario activo que puede ser otro digitador o el mismo administrador. No se está aplicando la política de seguridad de creación de usuarios.

Figura 38. Información enviada al correo del usuario

Buenas Tardes

Se ha creado un usuario para el municipio de La Dorada

URL: http://190.14.226.21/sgi/index.php?conid=sigdtscprd

Pedro perez Mahecha

pedritoperez@gmail.com

Celular: 3113115252

Usuario: pperezm
Contraseña: pperezm1

Cargo: Digitador

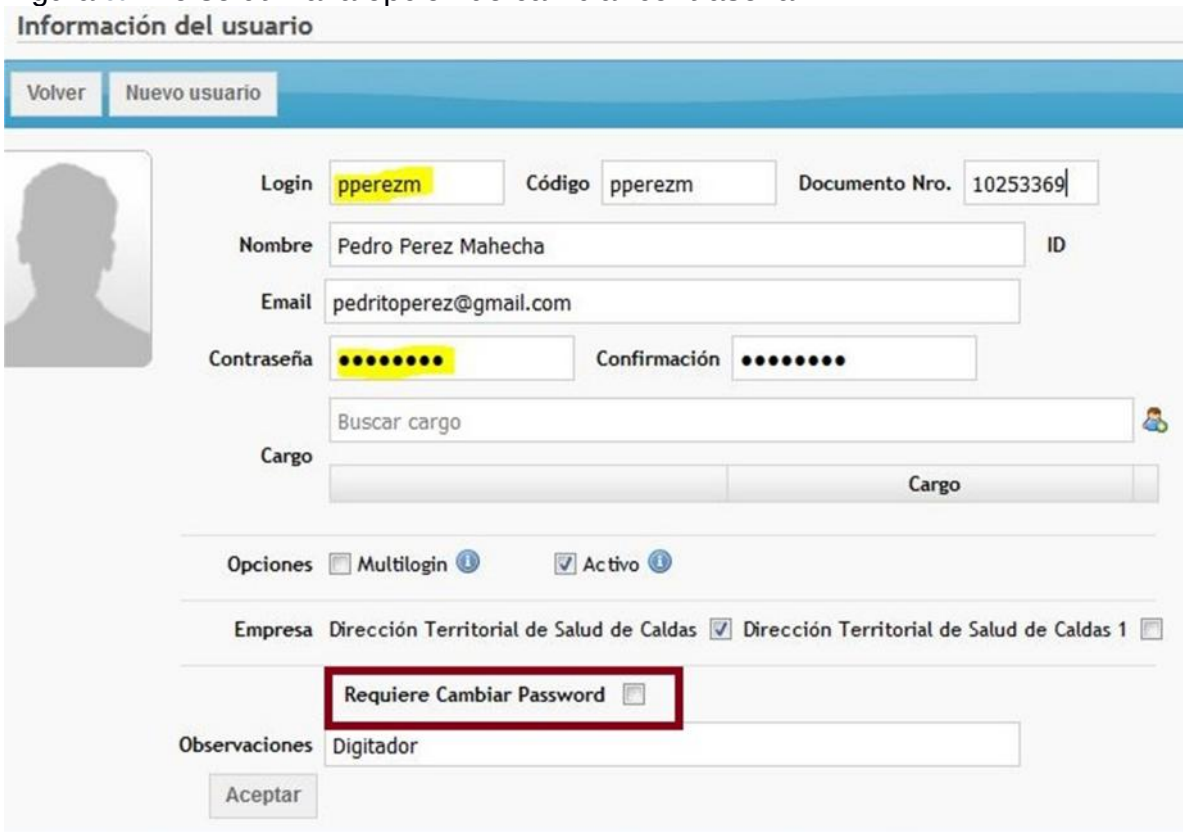
Saludos
.....

Fuente: El administrador.

- **Hallazgo 4**

Se puede evidenciar que al momento de crear los usuarios en sistema “Gestión Integrada de Bienestar Familiar”, no se activa la opción de “Requiere cambiar password”, lo que hace que al ingresar por primera vez al sistema, le solicite cambiar de contraseña, por tal motivo siguen utilizando la contraseña que le proporciono el administrador del sistema.

Figura 39. No se utiliza la opción de cambiar contraseña

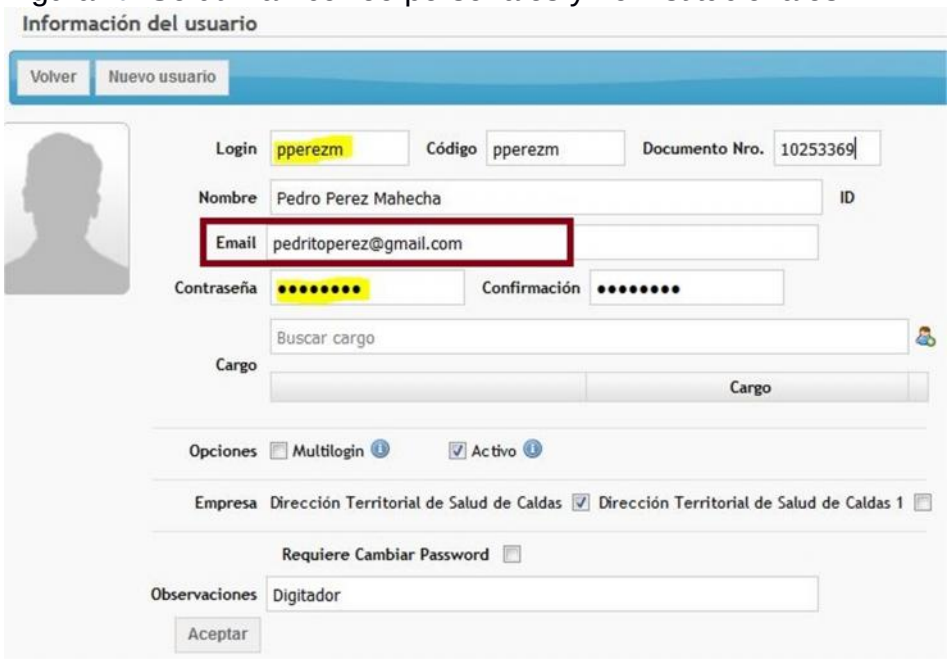


Fuente: El administrador.

- **Hallazgo 5**

Se evidencia que al momento de crear los usuarios, en la información solicitada por el administrador del sistema, solicita correo electrónico. Este correo es el personal de usuario, no un correo institucional, para garantizar que efectivamente esta persona si labora en una de las entidades autorizadas para ingresar a la plataforma y por otro lado se le pueda hacer llegar el documento de confidencialidad personal de la información que va a manipular y se verifique por parte de la entidad y la DTSC el convenio interadministrativo.

Figura 40. Se utilizan correo personales y no institucionales

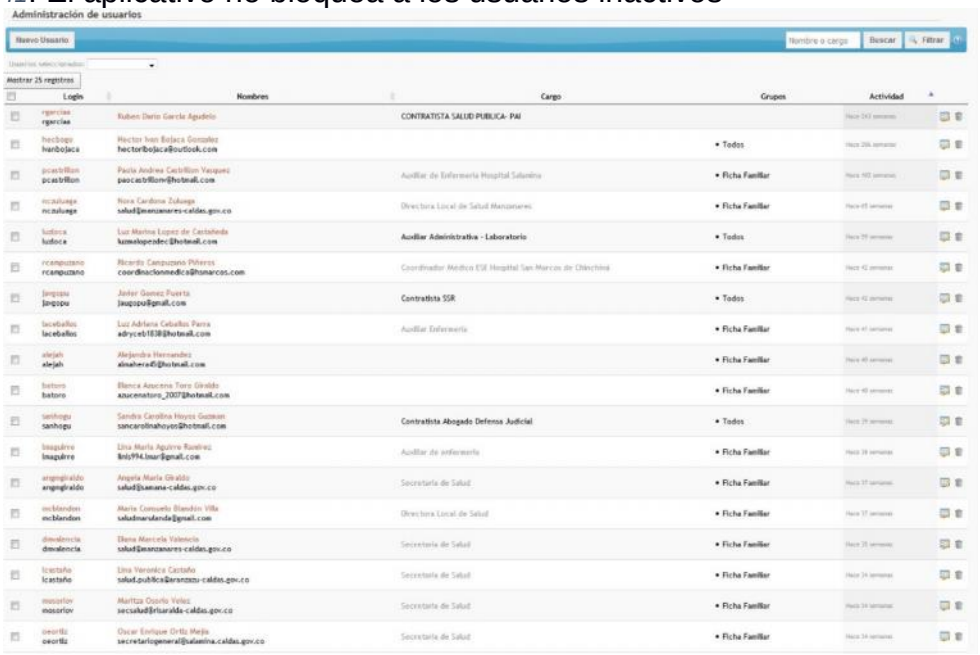


Fuente: El administrador.

- **Hallazgo 6.**

Con la ayuda del administrador del sistema, se genera un reporte de usuarios para verificar la actividad en el sistema de cada uno de ellos, lo que evidencia que existen usuarios que hace más de 12 semanas no ingresan a la plataforma. Esto puede suceder porque la persona ya no labora para la entidad que solicito la creación de ese usuario. Ya que tanto tiempo no se está en vacaciones o en alguna licencia o permiso especial. El estar activo el usuario en el sistema le permite ingresar a cualquier momento desde cualquier sitio.

Figura 41. El aplicativo no bloquea a los usuarios inactivos



Fuente: El administrador.

- **Hallazgo 7.**

No se obliga desde el sistema “Gestión Integrada de Bienestar Familiar” a crear contraseñas seguras o robustas, ya que se puede ingresar cualquier cadena de caracteres. No se cumple con la política de seguridad de creación de contraseñas que contempla letras, números, caracteres especiales y una longitud establecida.

Figura 42. No se solicita contraseñas con niveles de seguridad

Fuente: El administrador.

- **Hallazgo 8.**

El aplicativo permite seleccionar los campos que se deseen para exportar, esta información posee datos sensibles y de reserva como son enfermedades de alto costo y de salud pública que por su característica no se debe divulgar y se convierte en información de reserva y de confidencialidad.

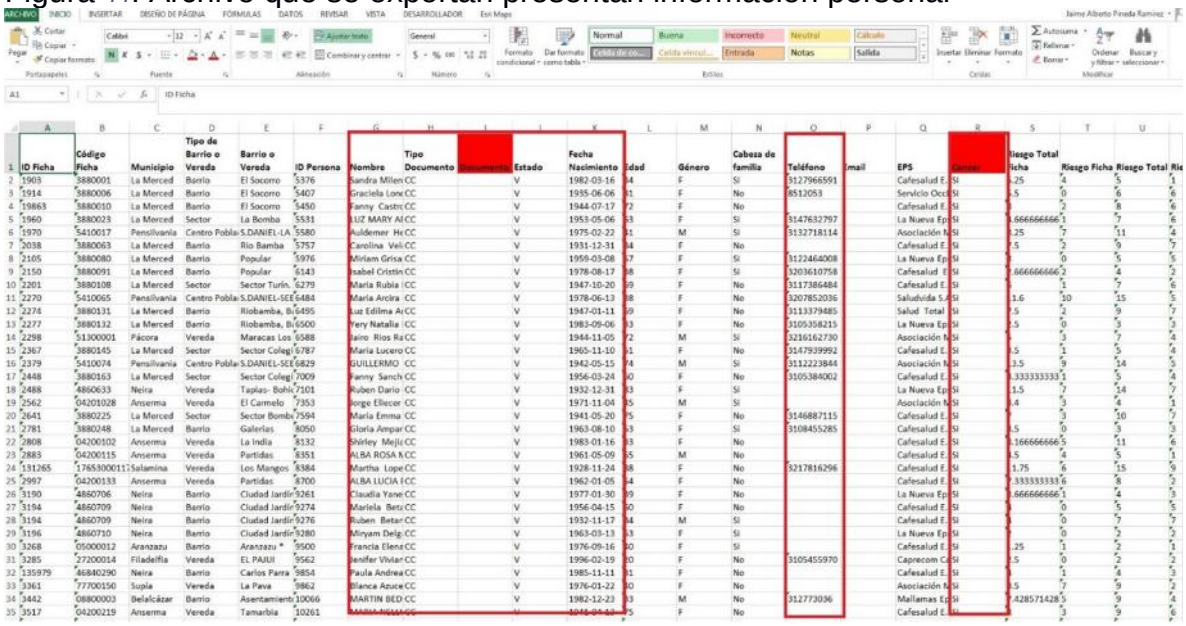
Figura 43. Permite exportar información sensible

Fuente: El administrador.

- **Hallazgo 9.**

Se evidencia en los archivos que se exportan a Excel, que se suministra información de tipo personal (nombre, identificación, teléfono, dirección, fecha de nacimiento), y también se suministra información sensible o reservada como en el ejemplo personas con cáncer. Esta información no puede ser de uso público y se debe respetar la confidencialidad y cadena de custodia. (La imagen se editó para ocultar el número de identificación de las personas).

Figura *44*. Archivo que se exportan presentan información personal



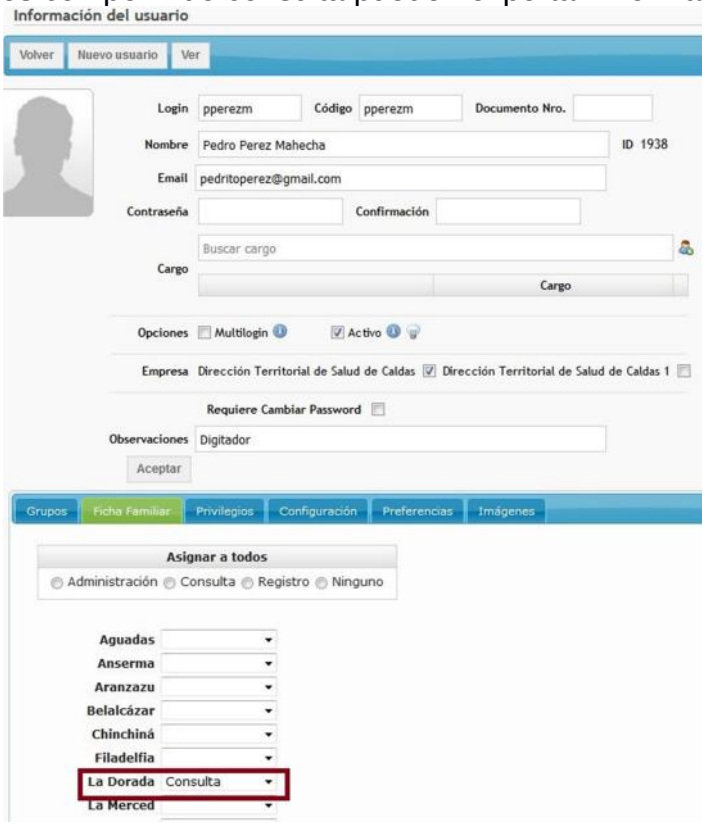
ID Ficha	Código Ficha	Municipio	Tipo de Barrio o Vereda	Barrio o Vereda	ID Persona	Nombre	Tipo Documento	[redacted]	Estado	Fecha Nacimiento	Edad	Género	Cabeza de familia	Teléfono	Email	EPS	[redacted]	Riesgo Total Ficha	Riesgo Ficha	Riesgo Total	Ri
1903	3880001	La Merced	Barrio	El Socorro	5376	Sandra Milen	CC		V	1982-03-16	44	F	SI	3127966591		Cafesalud E	SI	1.25	4	5	1
1914	3880006	La Merced	Barrio	El Socorro	5407	Graciela Lone	CC		V	1955-06-06	71	F	No	8512053		Servicio Occ	SI	1.5	0	6	6
19863	3880010	La Merced	Barrio	El Socorro	5450	Fanny Castro	CC		V	1944-07-17	72	F	No			Cafesalud E	SI	1	0	6	6
1960	3880023	La Merced	Sector	La Bomba	5531	LUZ MARY AI	CC		V	1953-05-06	63	F	SI	3147632797		La Nueva Ep	SI	1.666666666	1	7	6
1970	5410017	Pensilvania	Centro Pobla	S.DANIEL-LA	5580	Auldemer Hc	CC		V	1975-02-22	51	M	SI	3132718114		Asociación M	SI	1.25	7	11	4
2038	3880063	La Merced	Barrio	Rio Bamba	5757	Carolina Vel	CC		V	1931-12-31	94	F	No			Cafesalud E	SI	1.5	2	9	7
2105	3880080	La Merced	Barrio	Popular	5976	Miriam Grisa	CC		V	1959-03-08	67	F	SI	3122464008		La Nueva Ep	SI	1	0	5	5
2150	3880091	La Merced	Barrio	Popular	6143	Isabel Cristin	CC		V	1978-08-17	48	F	SI	3203610758		Cafesalud E	SI	1.666666666	2	4	2
2201	3880108	La Merced	Sector	Sector Turín.	6279	Maria Rubia	CC		V	1947-10-20	79	F	No	3117386484		Cafesalud E	SI	1	1	7	6
2270	5410065	Pensilvania	Centro Pobla	S.DANIEL-SE	6484	Maria Arcira	CC		V	1978-06-13	48	F	No	3207852036		Saludvida S.A	SI	1.6	10	15	5
2274	3880131	La Merced	Barrio	Riobamba, B	6495	Luz Edilma Ar	CC		V	1947-01-11	79	F	No	3113379485		Salud Total	SI	1.5	2	9	7
2277	3880132	La Merced	Barrio	Riobamba, B	6500	Yery Natalia	CC		V	1983-09-06	43	F	No	3105358215		La Nueva Ep	SI	1.5	0	3	3
2298	51300001	Pácora	Vereda	Maracas Los	6588	Jairo Rios Ra	CC		V	1944-11-05	72	M	SI	3216162730		Asociación M	SI	1	3	7	4
2367	3880145	La Merced	Sector	Sector Colegi	6787	Maria Lucero	CC		V	1965-11-10	51	F	No	3147939992		Cafesalud E	SI	1.5	1	5	4
2379	5410074	Pensilvania	Centro Pobla	S.DANIEL-SE	6829	GUILLERMO	CC		V	1942-05-15	74	M	SI	3112223844		Asociación M	SI	1.5	9	14	5
2448	3880163	La Merced	Sector	Sector Colegi	7009	Fanny Sanch	CC		V	1956-03-24	60	F	No	3105384002		Cafesalud E	SI	1.333333333	1	5	4
2488	4860633	Neira	Vereda	Taplas- Bohí	7101	Ruben Dario	CC		V	1932-12-31	83	F	SI			La Nueva Ep	SI	1.5	7	14	7
2562	04201028	Anserma	Vereda	El Carmelo	7353	Jorge Eliecer	CC		V	1971-11-04	45	M	SI			Asociación M	SI	1.4	3	4	1
2641	3880225	La Merced	Sector	Sector Bomb	7594	Maria Emma	CC		V	1941-05-20	75	F	No	3146887115		Cafesalud E	SI	1	3	10	7
2781	3880248	La Merced	Barrio	Galerías	8050	Gloria Ampar	CC		V	1963-08-10	53	F	SI	3108455285		Cafesalud E	SI	1.5	0	3	3
2808	04200102	Anserma	Vereda	La India	8132	Shirley Mejía	CC		V	1983-01-16	33	F	No			Cafesalud E	SI	1.166666666	5	11	6
2883	04200115	Anserma	Vereda	Partidas	8351	ALBA ROSA N	CC		V	1961-05-09	55	M	No			Cafesalud E	SI	1.5	4	5	1
131265	17653000115	Salamina	Vereda	Los Mangos	8384	Martha Lope	CC		V	1928-11-24	88	F	No	3217816296		Cafesalud E	SI	1.75	6	15	9
2997	04200133	Anserma	Vereda	Partidas	8700	ALBA LUCIA I	CC		V	1962-01-05	54	F	No			Cafesalud E	SI	1.333333333	6	8	2
3190	4860706	Neira	Barrio	Ciudad Jardín	9261	Claudia Yane	CC		V	1977-01-30	39	F	No			La Nueva Ep	SI	1.666666666	1	4	3
3194	4860709	Neira	Barrio	Ciudad Jardín	9274	Marlela Betz	CC		V	1956-04-15	60	F	No			Cafesalud E	SI	1	0	5	5
3194	4860709	Neira	Barrio	Ciudad Jardín	9276	Ruben Betar	CC		V	1932-11-17	84	M	SI			Cafesalud E	SI	1	0	7	7
3196	4860710	Neira	Barrio	Ciudad Jardín	9280	Miryam Delg	CC		V	1963-03-13	53	F	SI			La Nueva Ep	SI	1	0	2	2
3268	05000012	Aranzazu	Barrio	Aranzazu *	9500	Francia Elena	CC		V	1976-09-16	40	F	SI			Cafesalud E	SI	1.25	1	2	1
3285	27200014	Filadelfia	Vereda	EL PAUJI	9562	Jenifer Vivian	CC		V	1996-02-19	20	F	No	3105455970		Caprecom Ca	SI	1.5	0	2	2
135979	46840290	Neira	Barrio	Carlos Parra	9854	Paula Andrea	CC		V	1985-11-11	31	F	No			Cafesalud E	SI	1	1	4	3
3361	77700150	Supía	Vereda	La Pava	9862	Blanca Azuce	CC		V	1976-01-22	40	F	No			Asociación M	SI	1.5	7	9	2
3442	08800003	Belalcázar	Barrio	Asentamiento	10066	MARTIN BED	CC		V	1982-12-23	33	M	No	312773036		Mallamas Ep	SI	1.428571428	5	9	4
3517	04200219	Anserma	Vereda	Tamarbia	10261	MARIA NIMA	CC		V	1948-04-10	75	F	No			Cafesalud E	SI		5	9	6

Fuente: El administrador.

- **Hallazgo 10.**

Se evidencia que los usuarios de consulta, pueden exportar información a Excel. Por políticas de seguridad se establece que los usuarios de consulta son quienes pueden ver información, pero no pueden realizar actividades que comprometan la integridad y confidencialidad de la información.

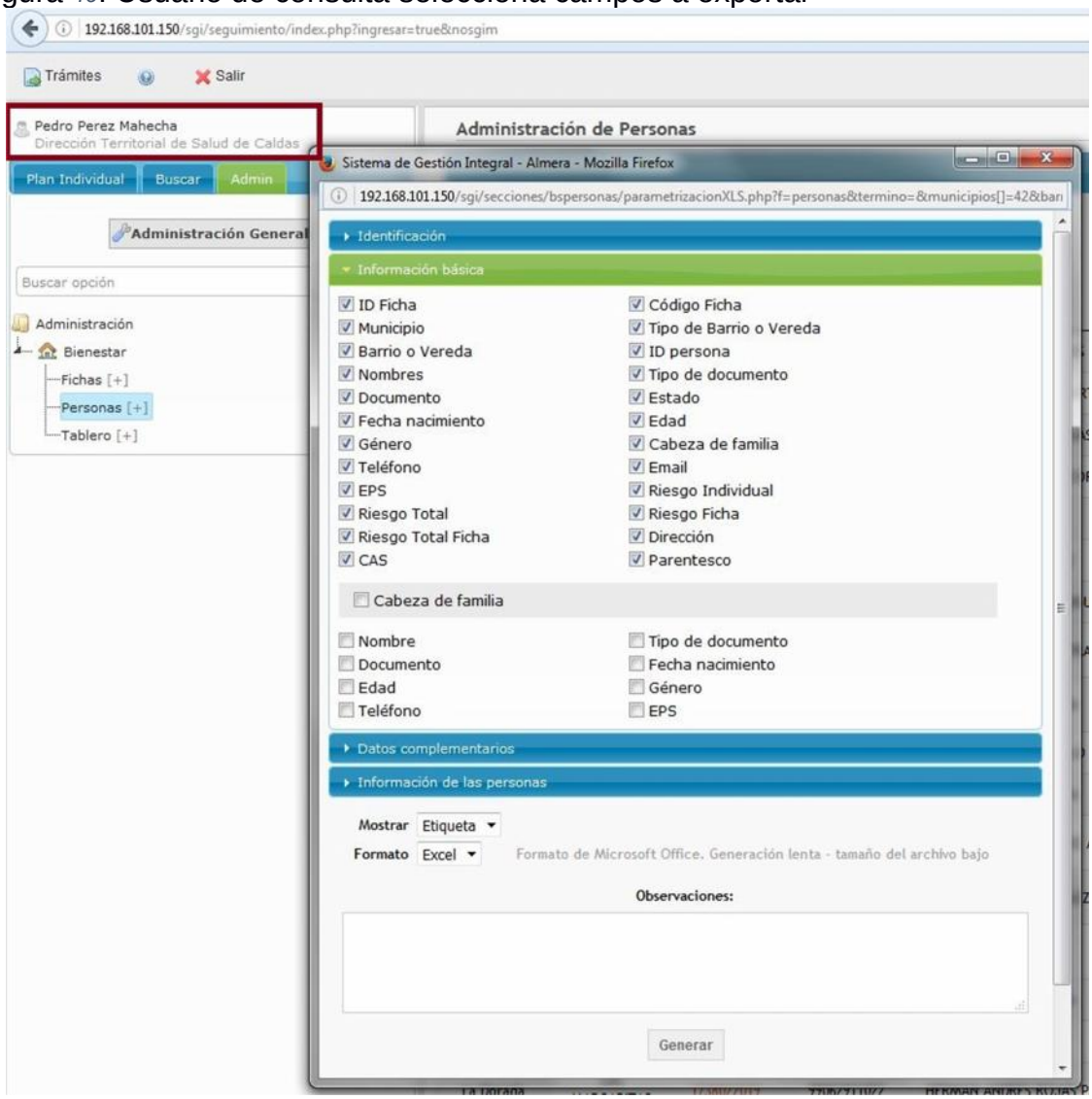
Figura 45. Usuarios con perfil de consulta pueden exportar información personal



Fuente: El administrador.

Selección de campos a exportar desde el usuario de consulta, el sistema “Gestión Integrada de Bienestar Familiar”, no debería permitir realizar esta actividad ya que es información personal en manos de personas no autorizadas.

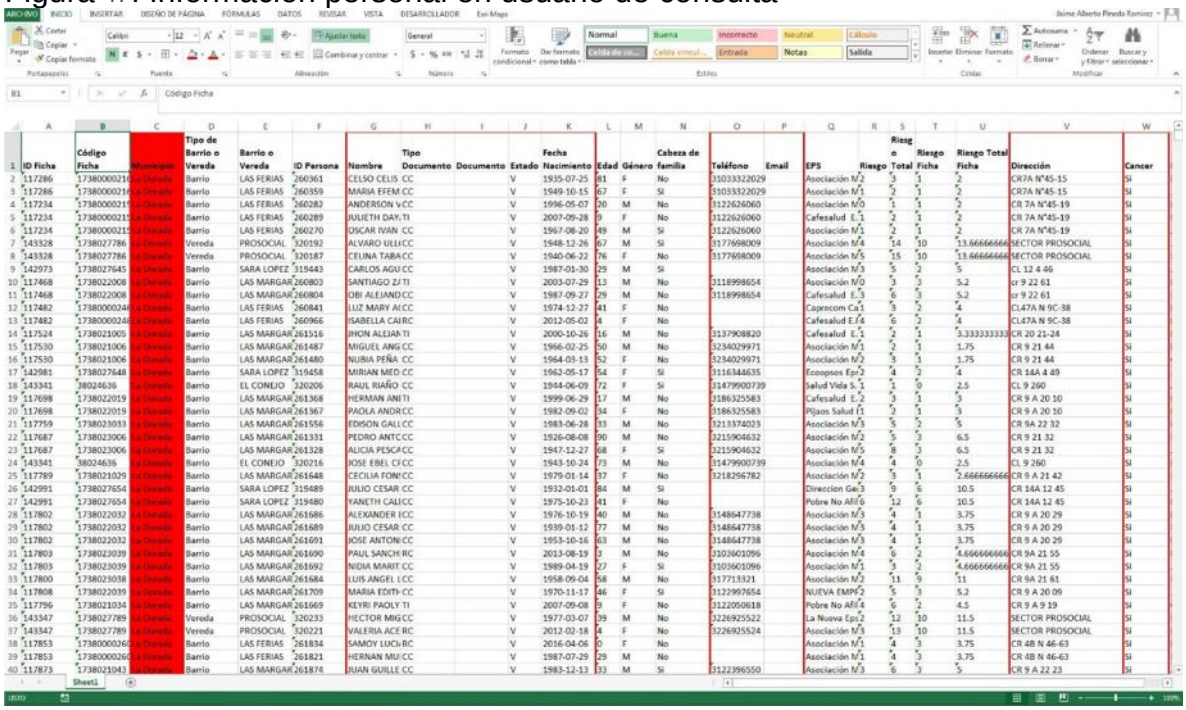
Figura 46. Usuario de consulta selecciona campos a exportar



Fuente: El administrador.

Se evidencia desde el archivo de Excel generado por el usuario de consulta la información personal y sensible, este usuario no está autorizado para manipular o intervenir. La información suministrada pertenece solo al municipio de La Dorada, ya que el usuario está asignado a ese municipio. (Se demarca la información personal y sensible desde el archivo exportado a Excel).

Figura 47. Información personal en usuario de consulta



ID Ficha	Código Ficha	Municipio	Tipo de Barrio o Vereda	Barrio o Vereda	ID Persona	Nombre	Tipo Documento	Documento	Estado	Fecha Nacimiento	Edad	Género	Cabeza de familia	Teléfono	Email	EPS	Riesgo	Riesgo Total	Riesgo Ficha	Riesgo Total Ficha	Dirección	Cancer
117286	173800002107	La Dorada	Barrio	LAS FERIAS	260361	CELSO CELIS	CC		V	1935-07-25	81	F	No	31033322029		Asociación M	2	3	1	2	CR7A N°45-15	Si
117286	173800002107	La Dorada	Barrio	LAS FERIAS	260359	MARIA EFEM	CC		V	1949-10-15	67	F	Si	31033322029		Asociación M	1	2	1	2	CR7A N°45-15	Si
117234	173800002107	La Dorada	Barrio	LAS FERIAS	260282	ANDERSON V	CC		V	1996-05-07	20	M	No	3122626060		Asociación M	0	1	1	2	CR 7A N°45-19	Si
117234	173800002107	La Dorada	Barrio	LAS FERIAS	260289	JULIETH DAY	TI		V	2007-09-28	9	F	No	3122626060		Cafesalud E	1	2	1	2	CR 7A N°45-19	Si
117234	173800002107	La Dorada	Barrio	LAS FERIAS	260270	OSCAR IVAN	CC		V	1967-08-20	49	M	Si	3122626060		Asociación M	1	2	1	2	CR 7A N°45-19	Si
143328	1738027786	La Dorada	Vereda	PROSOCIAL	320192	ALVARO ULL	CC		V	1948-12-26	67	M	Si	3177698009		Asociación M	4	14	10	13.66666666	SECTOR PROSOCIAL	Si
143328	1738027786	La Dorada	Vereda	PROSOCIAL	320187	CELINA TABA	CC		V	1940-06-22	76	F	No	3177698009		Asociación M	5	15	10	13.66666666	SECTOR PROSOCIAL	Si
142973	1738027645	La Dorada	Barrio	SARA LOPEZ	319443	CARLOS AGU	CC		V	1987-01-30	29	M	Si			Asociación M	3	5	2	5	CL 12 4 46	Si
117468	1738022008	La Dorada	Barrio	LAS MARGARI	260803	SANTIAGO ZA	TI		V	2003-07-29	13	M	No	3118998654		Asociación M	0	3	3	5.2	cr 9 22 61	Si
117468	1738022008	La Dorada	Barrio	LAS MARGARI	260804	OBI ALEJAND	CC		V	1987-09-27	29	M	No	3118998654		Cafesalud E	3	6	3	5.2	cr 9 22 61	Si
117482	1738000024	La Dorada	Barrio	LAS FERIAS	260841	LUZ MARY A	CC		V	1974-12-27	41	F	No			Caprecom Ca	1	3	2	4	CL47A N 9C-38	Si
117482	1738000024	La Dorada	Barrio	LAS FERIAS	260966	ISABELLA CA	RC		V	2012-05-02	4	F	No			Cafesalud E	4	6	2	4	CL47A N 9C-38	Si
117524	1738021005	La Dorada	Barrio	LAS MARGARI	261516	JHON ALEJAN	TI		V	2000-10-26	16	M	No	3137908820		Cafesalud E	1	2	1	3.333333333	CR 20 21-24	Si
117530	1738021006	La Dorada	Barrio	LAS MARGARI	261487	MIGUEL ANG	CC		V	1966-02-25	50	M	No	3234029971		Asociación M	1	2	1	1.75	CR 9 21 44	Si
117530	1738021006	La Dorada	Barrio	LAS MARGARI	261480	NUBIA PEÑA	CC		V	1964-03-13	52	F	No	3234029971		Asociación M	2	3	1	1.75	CR 9 21 44	Si
142981	1738027648	La Dorada	Barrio	SARA LOPEZ	319458	MIRIAN MED	CC		V	1962-05-17	54	F	Si	3116344635		Ecoopsos Epr	2	4	2	4	CR 14A 4 49	Si
143341	38024636	La Dorada	Barrio	EL CONEJO	320206	RAUL RIAÑO	CC		V	1944-06-09	72	F	Si	31479900739		Salud Vida S	1	1	0	2.5	CL 9 260	Si
117698	1738022019	La Dorada	Barrio	LAS MARGARI	261368	HERMAN ANI	TI		V	1999-06-29	17	M	No	3186325583		Cafesalud E	2	3	1	3	CR 9 A 20 10	Si
117698	1738022019	La Dorada	Barrio	LAS MARGARI	261367	PAOLA ANDR	CC		V	1982-09-02	34	F	No	3186325583		Pijaos Salud	1	2	1	3	CR 9 A 20 10	Si
117759	1738023033	La Dorada	Barrio	LAS MARGARI	261556	EDISON GALL	CC		V	1983-06-28	33	M	No	3213374023		Asociación M	3	5	2	5	CR 9A 22 32	Si
117687	1738023006	La Dorada	Barrio	LAS MARGARI	261331	PEDRO ANTC	CC		V	1926-08-08	90	M	No	3215904632		Asociación M	2	5	3	6.5	CR 9 21 32	Si
117687	1738023006	La Dorada	Barrio	LAS MARGARI	261328	ALICIA PESC	CC		V	1947-12-27	68	F	Si	3215904632		Asociación M	5	8	3	6.5	CR 9 21 32	Si
143341	38024636	La Dorada	Barrio	EL CONEJO	320216	JOSE EBEL C	CC		V	1943-10-24	73	M	No	31479900739		Asociación M	4	4	0	2.5	CL 9 260	Si
117789	1738021029	La Dorada	Barrio	LAS MARGARI	261648	CECILIA FON	CC		V	1979-01-14	37	F	No	3218296782		Asociación M	2	3	1	2.666666666	CR 9 A 21 42	Si
142991	1738027654	La Dorada	Barrio	SARA LOPEZ	319480	JULIO CESAR	CC		V	1932-01-01	84	M	Si			Direccion Ge	3	9	6	10.5	CR 14A 12 45	Si
142991	1738027654	La Dorada	Barrio	SARA LOPEZ	319480	YANETH CALI	CC		V	1975-10-23	41	F	No			Pobre No Afil	6	12	6	10.5	CR 14A 12 45	Si
117802	1738022032	La Dorada	Barrio	LAS MARGARI	261686	ALEXANDER I	CC		V	1976-10-19	40	M	No	3148647738		Asociación M	3	4	1	3.75	CR 9 A 20 29	Si
117802	1738022032	La Dorada	Barrio	LAS MARGARI	261689	JULIO CESAR	CC		V	1939-01-12	77	M	No	3148647738		Asociación M	5	4	1	3.75	CR 9 A 20 29	Si
117802	1738022032	La Dorada	Barrio	LAS MARGARI	261691	JOSE ANTON	CC		V	1953-10-16	63	M	No	3148647738		Asociación M	3	4	1	3.75	CR 9 A 20 29	Si
117803	1738023039	La Dorada	Barrio	LAS MARGARI	261690	PAUL SANCH	RC		V	2013-08-19	3	M	No	3103601096		Asociación M	4	6	2	4.666666666	CR 9A 21 55	Si
117803	1738023039	La Dorada	Barrio	LAS MARGARI	261692	NIDIA MARIT	CC		V	1989-04-19	27	F	Si	3103601096		Asociación M	1	3	2	4.666666666	CR 9A 21 55	Si
117800	1738023038	La Dorada	Barrio	LAS MARGARI	261684	LUIS ANGEL	CC		V	1958-09-04	58	M	No	317713321		Asociación M	2	11	9	11	CR 9A 21 61	Si
117808	1738022039	La Dorada	Barrio	LAS MARGARI	261709	MARIA EDITH	CC		V	1970-11-17	46	F	Si	3122997654		NUEVA EMPI	2	5	3	5.2	CR 9 A 20 09	Si
117796	1738021034	La Dorada	Barrio	LAS MARGARI	261669	KEYRI PAOLY	TI		V	2007-09-08	9	F	No	3122050618		Pobre No Afil	4	6	2	4.5	CR 9 A 9 19	Si
143347	1738027789	La Dorada	Vereda	PROSOCIAL	320233	HECTOR MIG	CC		V	1977-03-07	39	M	No	3226925522		La Nueva Epr	2	12	10	11.5	SECTOR PROSOCIAL	Si
143347	1738027789	La Dorada	Vereda	PROSOCIAL	320221	VALERIA ACE	RC		V	2012-02-18	4	F	No	3226925524		Asociación M	3	13	10	11.5	SECTOR PROSOCIAL	Si
117853	1738000026	La Dorada	Barrio	LAS FERIAS	261834	SAMOY LUCI	RC		V	2016-04-06	0	F	No			Asociación M	1	4	3	3.75	CR 48 N 46-63	Si
117853	1738000026	La Dorada	Barrio	LAS FERIAS	261821	HERNAN MU	CC		V	1987-07-29	29	M	No			Asociación M	1	4	3	3.75	CR 48 N 46-63	Si
117873	1738021043	La Dorada	Barrio	LAS MARGARI	261874	JUAN GUILLE	CC		V	1983-12-13	33	M	Si	3122396550		Asociación M	3	6	3	5	CR 9 A 22 23	Si

Fuente: El administrador.

- **Plan de Mejoramiento a implementar**

A continuación se especifican las acciones a tomar en cada uno de los hallazgos como plan de mejoramiento a implementar para solucionar las vulnerabilidades encontradas y así cumplir con el objetivo de la auditoría a la seguridad del sistema de información “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas.

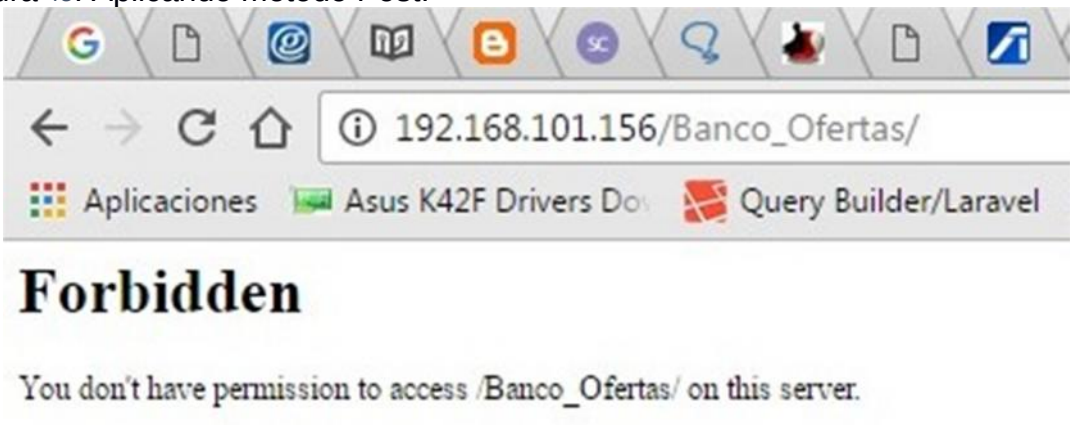
- **Hallazgo 1.**

Para evitar ingresar al árbol de directorios desde un navegador y la IP o dirección de la plataforma, se propone como solución enviar los datos encriptados a través de la entrada STDIO utilizando el método Post. La diferencia radica la forma como se envían los datos a la página, en el método GET utilizado actualmente se envían los datos usando la URL, y con el método POST los datos se envían por la entrada estándar STDIO.

Los datos enviados a través del método Post fluyen por la cabecera HTTP lo que da más seguridad. No tiene restricción por el tamaño de los datos a enviar; este método también se puede utilizar para enviar información en código ASCII y binaria.

Con la ayuda del Ingeniero Martínez, Sebastián programador del observatorio social de salud pública de la Dirección Territorial de Salud de Caldas, se realiza un ejercicio aplicando método Post de la misma página del de sistema “Gestión Integrada de Bienestar Familiar”, sección banco de ofertas, donde se puede evidenciar que ya no permite ingresar al árbol de directorios, ya se bloquea esta entrada.

Figura 48. Aplicando método Post.



Fuente: El autor.

- **Hallazgo 2.**

Para evitar la navegación por paginas no deseadas y en especial las que consumen gran cantidad de ancho de banda como es el caso de YouTube, se sugiere verificar la configuración del aplicativo de control de navegación y adicionar estas páginas en la misma sección donde se encuentra la de Facebook, ya que son las más solicitadas por los usuarios de la red. Así se controla el tráfico en la red y se evitan posibles ataques por medio de estos canales ya que se podría descargar virus que afecten el normal funcionamiento del sistema. Un ejemplo de bloqueo de página puede ser como está la del Facebook.

Figura 49. Página bloqueada desde el administrador.

Fuente: El autor.

- **Hallazgo 3.**

Establecer criterios para la creación de usuarios y sus respectivas contraseñas. Los nombres de los usuarios deben tener criterios definidos por el área de sistemas de acurdo a las políticas de seguridad de creación de usuarios que por lo regular van con acordes al nombre de la persona, pero a las contraseñas se les aplica normas establecidas como:

- Longitud mínimo de 8 caracteres, aunque ideal sería 14 caracteres.
- Combinación entre letras, números y símbolos, utilizar diversos tipos de caracteres y símbolos del teclado.
- La contraseña la debe establecer el usuario, no el administrador.
- No admitir datos como nombre propios o número de identificación o celular del usuario.
- Las contraseñas deben cumplir con criterios de encriptación.

Un ejemplo de esta última norma puede ser:

Figura 50. Contraseña encriptada.

Fuente: El autor.

- **Hallazgo 4.**

El Sistema “Gestión Integrada de Bienestar Familiar”, cumple con los requisitos de la política de seguridad de solicitar al usuario cuando ingresa por primera vez, cambiar la contraseña. Este proceso hace seguro el sistema, ya que la contraseña solo queda a responsabilidad del usuario. Se evidencia que el administrador del Sistema no está aplicando esta regla, por tal motivo se solicita al Ingeniero Martínez, Sebastián que realice esta actividad a todos y cada uno de los usuarios del sistema.

Figura 51. Opción cambiar password activada.

Fuente: El autor.

Al momento del usuario volver a ingresar al sistema “Gestión Integrada de Bienestar Familiar”, se le solicita cambiar la contraseña.

Figura 52. Requiere cambio de contraseña.

Fuente: El autor.

- **Hallazgo 5.**

Al momento de reportar la información para crear usuarios del sistema “Gestión Integrada de Bienestar Familiar”, se solicita correo electrónico de la persona. Se sugiere que se solicite un correo institucional, lo que hace que la información sea más confiable y quede bajo el marco de los convenios establecidos entre la entidad solicitante y la Dirección Territorial de Salud de Caldas. Para fines de

aplicar lo establecido en el documento de confidencialidad. Se solicita al administrador realizar estos cambios.

Figura 53. Cambiar correos personales de usuarios.

Fuente: El autor.

- **Hallazgo 6.**

Se solicita al administrador del "Gestión Integrada de Bienestar Familiar" que verifique y realice un filtro de los usuarios que lleven más de 12 semanas sin ingresar a la plataforma para evitar que empleado que ya no laboren con la entidad solicitante continúen con usuarios activos y puedan ingresar a la plataforma. El proceso consiste en desactivar la opción de Activo de la configuración del usuario. Este procedimiento se realiza a quienes cumplan la condición de inactividad por más de 3 meses que puede ser el tiempo máximo que un empleado puede estar en vacaciones o alguna licencia.

Si por algún motivo después de ese tiempo aparece un usuario informando que esta por fuera del sistema, se hace la aclaración del porque este lapso de tiempo sin utilizar la plataforma y se vuelve a activar las opciones del usuario, verificando perfil y privilegios del mismo.

Figura 54. Usuario Inactivo.

Fuente: El autor.

- **Hallazgo 7.**

Se sugiere aplicar criterios establecidos en las políticas de seguridad en la sección de creación de usuarios y contraseñas, que especifican los criterios a contemplar al momento de crear usuarios de sistemas de información. Al nombre del usuario hace falta aplicar números y la contraseña no puede seguir siendo el mismo nombre del usuario seguido de un numero 1. Y aplicar rotación de contraseñas.

Se propone contraseñas seguras que contemple letras, números, caracteres especiales, y una longitud mínima de 8 caracteres.

Figura 55. Propuesta criterios para contraseñas.

Fuente: El autor.

- **Hallazgo 8.**

La propuesta consiste en deshabilitar la opción de seleccionar información sensible como lo es la de enfermedades de salud pública y alto costos, ya que no se está protegiendo la información reservada y puede causar inconvenientes a la entidad por el tema de la privacidad de la información.

Siempre se debe proteger la información de personas inescrupulosas que andan buscando datos de este tipo para proceder de mala fe. Solo será de uso de los administradores y de los referentes de las líneas de acción, cuando se desarrollen mesas de análisis, Coves de salud y unidades de crisis, que requieren datos más amplios de los pacientes.

- **Hallazgo 9.**

De igual manera se procederá a desactivar las anteriores opciones del reporte que se genera en Excel al momento de exportar la información tanto de información sensible como de datos personales de número de identificación, teléfono y dirección, debido a se corre el riesgo que esos archivos se puedan enviar o trasportar de una entidad a otra o entre empleados de la instituciones. Los archivos que se exportan deben contener información básica y de fácil entendimiento.

- **Hallazgo 10.**

Se solicita al administrador de sistema "Gestión Integrada de Bienestar Familiar", verificar que los usuarios con roles y privilegios de consulta, no presenten la opción de exporta información, ya que este tipo de usuario no está facultado para poseer esta información, y los convenios interadministrativos entre las entidades y la dirección territorial de salud de caldas, así lo disponen.

Por lo regular un usuario de consulta es quien simplemente cumple las funciones de ingresar al sistema y ver algunos datos específicos, pero no se le permite digitar, crear, modificar, actualizar, eliminar, importar y exportar información de ningún tipo.

- **Entrega de hallazgos de vulnerabilidades al administrador del sistema "Gestión Integrada de Bienestar Familiar" y al Director de la DTSC.**

Se realiza entrega al ingeniero Martínez, Sebastián y al Director de la Dirección Territorial de Salud de Caldas, Dr. Bermont Galavis, Gerson Orlando[27] del informe final que contiene los hallazgos de las vulnerabilidades encontradas en la en la auditoría al sistema de seguridad sistema "Gestión Integrada de Bienestar Familiar", de igual manera se sugiere un plan de mejoramiento a implementar de acuerdo a los objetivos y propuestas trazadas para realizar dicha actividad en la entidad.

Se dan los más sinceros agradecimientos a todos los empleados que colaboraron en el desarrollo de las actividades y hacer posible llevar a fin esta auditoría que será de mucha ayuda para proteger la integridad y disponibilidad de la información del sistema "Gestión Integrada de Bienestar Familiar". Anexo 3 (Informe vulnerabilidades y plan de mejoramiento).

[27] BERMONT GALAVIS. Gerson Orlando. Optómetra. Dirección Territorial de Salud de Caldas. Director General. {2017}

Por último se realiza solicitud al Doctor Bermont Galavis, de permitir en un plazo no superior de 2 meses verificar si efectivamente los planes de mejoramiento entregados en el informe final, se implementaron correctamente y así haber contribuido a mejorar el esquema de seguridad del sistema “Gestión Integrada de Bienestar Familiar”, implementado en la Dirección Territorial de Salud de Caldas, y así dar por terminada la Auditoría propuesta.

5. CONCLUSIONES

El presente trabajo permitió desarrollar actividades reales aplicadas a una problemática real que se presenta en una empresa pública que tiene entre sus principales objetivos la confidencialidad de la información, y por tal motivo permite que se ejecuten auditorías internas que brinde aprendizajes continuos.

Al desarrollar la auditoría se presentan barreras que hay que solucionar en la marcha, tal es caso de algunos funcionarios que por falta de tiempo, por falta de cultura o simplemente por miedo al cambio se oponen a brindar información de gran importancia y relevancia, pero que gracias al apoyo de la dirección de la entidad se logra superar.

La auditoría realizada a la seguridad del sistema de información “Gestión Integrada de Bienestar Social” de la Dirección Territorial de Salud de Caldas, arrojo los resultados esperados por el grupo de trabajo que consistían en determinar las vulnerabilidades, amenazas y riesgos a que se encuentra expuesto el sistema desde el punto de vista de la seguridad informática.

Con respecto a los objetivos iniciales, se puede concluir lo siguiente:

El plan de auditoría permitió crear una carta en navegación en cuanto a actividades a desarrollar, tiempos y responsables con roles específicos de acuerdo a su relación con el aplicativo objeto de la auditoría.

El desarrollo del plan de auditoría se ejecutó sin ningún cambio y de acuerdo a lo planteado y propuesto, dejando claro el compromiso por parte de investigador, del grupo de apoyo de la entidad y de la dirección general de la Dirección Territorial de Salud de Caldas.

Se logró conocer de primera mano y de la fuente original los controles y políticas del esquema de seguridad existentes tanto de la seguridad informática de la institución como del sistema “Gestión Integrada de Bienestar Social”, permitiendo analizar la información y emitiendo conceptos al respecto. Algunos de estos conceptos fueron los entregados como hallazgos de vulnerabilidades, amenazas y riesgos.

Un aspecto que cabe destacar en este proyecto, es el informe final que se presentó que contiene el plan de mejoramiento a implementar que propone corregir las vulnerabilidades encontradas y la posterior verificación por parte del auditor a la implementación.

6. RECOMENDACIONES

Acoger las recomendaciones del plan de mejoramiento entregado a la dirección general y al área de sistemas en cada uno de sus puntos y aprovechar los conocimientos adquiridos por el grupo auditor para mejorar otros aspectos internos de la institución, siempre acompañados del área de calidad.

En un plazo no superior a dos meses después de entregado el informe final de hallazgos y el plan de mejoramiento realizar una verificación que permita comprobar si efectivamente se tomaron las medidas pertinentes y sugeridas.

Proponer una auditoría externa a realizar el próximo año, que involucre aspectos en el área de sistemas y permitan determinar la seguridad tanto de los aplicativos existentes en la institución como las políticas implementadas, si están acordes y si se están verificando continuamente.

7. BIBLIOGRAFÍA

ALBERTO G. Alexander. CENTRUM. Análisis y evaluación del riesgo de información, [en línea], 2013. Disponible en internet: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf

ALVARES CASTRO. Juan Carlos. Director. Oficina asesora de planeación y calidad DTSC. 2017

ARENGAS CASTILLA. Ángel Isdruval. Epidemiólogo. Dirección Territorial de Salud de Caldas. Director Observatorio Social de Salud de Caldas. 2017.

BERMONT GALAVIS. Gerson Orlando. Optómetra. Dirección Territorial de Salud de Caldas. Director General. 2017.

BUSINESS ASSURANCE & AUDIT. Plan de auditoria, [en línea], 2011. Disponible en internet: *ecaths1.s3.amazonaws.com/aseguramiento/836662139.PLAN+DE+AUDITORIA.pdf*

DECEVAL. Sistema integrado de información de la empresa. Bogotá. Marzo de 2012. 20p.

DIRECCIÓN TERRITORIAL DE SALUD DE CALDAS. Observatorio Social, [en línea], 2016. Disponible en internet: https://saluddecaldas.gov.co/observatorio-social/

DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Quienes somos. Misión, [en línea], enero 16 de 2017. Disponible en internet: (http://saluddecaldas.gov.co/quienes-somos/#sub_menu_paginas

DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Quienes somos. Nuestra historia, [en línea], febrero 21 de 2014. Disponible en internet: http://saluddecaldas.gov.co/nuestra-historia/#sub_menu_paginas

DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Quienes somos. Visión, [en línea], enero 16 de 2017. Disponible en internet: http://saluddecaldas.gov.co/quienes-somos/#sub_menu_paginas

DIRECCIÓN TERRIOTRIAL DE SALUD DE CALDAS. Sistema de gestión de calidad, [en línea], enero 16 de 2017. Disponible en internet: http://saluddecaldas.gov.co/politica-de-calidad/#sub_menu_paginas

FUNCIÓN PÚBLICA. Guía de auditoría para entidades públicas, [en línea], octubre de 2015. Disponible en internet:

http://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADaAuditoriaEntidadesPublicas+V2Octubre2015/fcf84a18-5c74-480a-83c4-2a25ec49bea1

GERENCIE. GERENCIE.COM. Auditoría interna, [en línea], mayo 11 de 2011. Disponible en Internet: https://www.gerencie.com/auditoria-interna.html

HERNÁNDEZ SAMPIERI. Roberto. FERNÁNDEZ COLLADO. Carlos. BAPTISTA LUCIO. María del Pilar. Metodología de la investigación. Quinta edición. Perú. Mc GRAW HILL. 2010. 276p.

JIMÉNEZ. Alonso. Ingeniero en telecomunicaciones. Dirección Territorial de Salud de Caldas. Director Tecnología de la información y las comunicaciones. 2017.

MAMANI POMA. Orlando Jimmy. AROHUANCA A. Michella. MAMANI CUTIPA. Willy. QUIÑONES MAYTA. Carmen. MUÑOZ ORTEGA. Madeleine. POCOHUANCA TURBO. Nelssy. Informe de gestión sobre el sistema de seguridad de control interno. Perú. Mariscal. 2003. 33p.

MARTÍNEZ. Sebastián. Ingeniero de sistemas. Dirección Territorial de Salud de Caldas. Observatorio Social de Salud de Caldas. 2017.

MEJORA TU GESTIÓN. ¿Qué es un Sistema de Gestión?, [en línea], marzo de 2015. Disponible en internet: http://mejoratugestion.com/mejora-tu-gestion/que-es-un-sistema-de-gestion/

MENDOZA PALACIOS. Rudy. Monografías.com. Investigación cualitativa y cuantitativa – diferencias y limitaciones, [en línea], 2006. Disponible en internet: http://www.monografias.com/trabajos38/investigacion-cualitativa/investigacion-cualitativa.shtml

MENDOZA PALACIOS. Rudy. Monografías.com. Investigación cualitativa y cuantitativa – diferencias y limitaciones, [en línea], 2006. Disponible en internet: http://www.monografias.com/trabajos38/investigacion-cualitativa/investigacion-cualitativa2.shtml

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. MINSALUD. Política de atención integral en salud. Un sistema de salud al servicio de la gente, [en línea], enero de 2016. Disponible en internet: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/modelo-pais-2016.pdf

PARRA. Yesid. Director proyectos. Almera Information Management. Manizales. 2017.

PÉREZ PORTO. Julián. MERINO. Definición.de. María. Definición de Seguridad informática, [en línea], 2008. Disponible en Internet: https://definicion.de/seguridad-informatica/

RESTREPO G. Jorge A. JORGE A. RESTREPO G. Guía para la clase de auditoría de sistemas, [en línea], 2011. Disponible en Internet: http://jorgearestrepog.comunidadcoomeva.com/blog/index.php

ROMERO TORRES. Mariano Esteban. Director de proyecto. Universidad nacional abierta y a distancia – UNAD. 2016

SEGU.INFO. Seguridad Informática. Política de Seguridad, [en línea], 2009. Disponible en internet: http://www.segu-info.com.ar/politicas/

SOLARTE SOLARTE. Francisco Nicolás. Auditoría Informática y de Sistemas. Conceptos de Auditoría, [en línea], 2011. Disponible en Internet: http://auditordesistemas.blogspot.com.co/2011/11/conceptos.html

ANEXOS

Anexo 1. Carta de aval del proyecto

DIRECCIÓN TERRITORIAL Salud de Caldas

Nit. 800114312-5

CUÍDATE - CUÍDAME

Manizales, Caldas, 27 de abril de 2016

Ingeniero
JAIME ALBERTO PINEDA RAMIREZ
Manizales, Caldas

Ref.: Autorización Auditoria

Cordial saludo Ingeniero Pineda

En respuesta a su solicitud de autorización para la realización de la AUDITORIA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN "GESTIÓN INTEGRADA DE BIENESTAR SOCIAL" EN LA DIRECCIÓN TERRITORIAL DE SALUD DE CALDAS, dentro del marco de la Especialización en Auditoría Informática que cursa en la Universidad Nacional Abierta y a Distancia (UNAD), me permito informarle que ha sido autorizada su realización.

Atentamente,

Gerson Orlando Bermont Galavis
Director General
Dirección Territorial de Salud de Caldas

SGS SGS

Sede Principal
Teléfonos: +57 (6) 8783096 - 8783097 - Fax: +57 (6) 8783171 / Dirección: Cl. 49 No. 26 - 46
Manizales, Caldas
e-mail: informacion@saluddecaldas.gov.co / www.saluddecaldas.gov.co

F002-P05-GAF V03 Página 1 de 1

Fuente: El autor.

Anexo 2. Acuerdo de Confidencialidad

DIRECCIÓN TERRITORIAL Salud de Caldas	DIRECCION TERRITORIAL DE SALUD DE CALDAS SISTEMA DE GESTION DE CALIDAD Proceso Gestión de la Calidad Acuerdo de Confidencialidad y Protección de la Información	Versión: 03 Código: F009-P01-GC Fecha: 27/05/2015

ACUERDO DE CONFIDENCIALIDAD Y PROTECCIÓN DE LA INFORMACIÓN
ENTRE LA DIRECCION TERRITORIAL DE SALUD DE CALDAS Y (_____).

Este acuerdo de confidencialidad realizado y suscrito entre La Dirección Territorial de Salud de Caldas, **EL PROVEEDOR** (en adelante **EL PROVEEDOR** y (_____), en adelante **EL CLIENTE**, representada por _____ identificado con cédula de ciudadanía N° _____ de _____, en su calidad de Representante Legal, tiene como finalidad establecer los términos que rigen el uso y la protección de la información que recíprocamente se intercambiarán las partes, previas las siguientes:

CONSIDERACIONES

Que la Ley Estatutaria 1581 de octubre 17 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, constituye el marco general de la protección de los datos personales en Colombia, establece normas para la certificación de buenas prácticas en la protección de datos, tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

Que el Decreto 1377 de junio 27 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012, formula los aspectos relacionados con la autorización del titular de información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al tratamiento de datos personales.

Que **EL PROVEEDOR** y **EL CLIENTE** en beneficio mutuo desean revelarse determinada información verbal o escrita, en general de carácter no mercantil que puede incluir entre otros planes de proyectos, inversión y desarrollo, información técnica, información sobre determinantes sociales, software, bases de datos, y otras informaciones que se refieran al uso de la plataforma Web del sistema "Gestión Integrada de Bienestar Social" que se encuentra en el portal de la Dirección Territorial de Salud de Caldas www.saluddecaldas.gov.co en la pestaña Observatorio Social de Caldas -Atención Primaria Social-.

Que el presente acuerdo de confidencialidad tiene como finalidad establecer el uso y la protección de la información que se han entregado y se entregarán entre **EL CLIENTE** y **EL PROVEEDOR** mutuamente.

ESTIPULACIONES

Las partes del acuerdo se someterán a las siguientes estipulaciones:

1- POLITICA DE PROTECCIÓN DE DATOS. El responsable del tratamiento de datos debe contar con una política de tratamiento de la información, la cual obliga al responsable y encargado de la misma. Su incumplimiento acarreara las sanciones correspondientes. Art 21 L 1581/12. Cualquier cambio de política que afecte el contenido de la autorización, se debe comunicar al titular a más tardar al momento de implementar las nuevas políticas y obtener nueva autorización si el cambio se refiere a la finalidad del tratamiento. Debe nombrarse un responsable de la protección de datos personales y de trámite a las solicitudes de los titulares.

2- PROCEDIMIENTOS. Se debe tener una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de la información, como también la descripción de la finalidad para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.

Fuente: Dirección Territorial de Salud de Caldas

Anexo 3. Informe vulnerabilidades

Manizales – Caldas, diciembre de 2016

Doctor **Gerson Orlando Bermont Galavis,** Ingeniero **Sebastián Martínez**
Dirección Territorial de Salud de Caldas
La Ciudad.

Ref. Entrega Informe Final

Respetado Doctor,

Con la presente realizo entrega del informe final de hallazgos encontrados en la auditoria al sistema de seguridad sistema "Gestión Integrada de Bienestar Familiar". Realizada en su totalidad en las instalaciones del observatorio social de salud pública de la dirección territorial de salud de caldas.

De igual manera se realiza entrega del plan de mejoramiento propuesto para rectificar los hallazgos de vulnerabilidades.

Anexo encontrara el documento donde se evidencia todos los objetivos propuestos en el desarrollo de la auditoria, su procedimiento para detectarla y los planes de mejoramientos propuestos a implementar y corregir las vulnerabilidades halladas. De igual forma les comunico que el presente proyecto está incluido en el repositorio de la Universidad Nacional Abierta y a Distancia UNAD.

Gracias por la colaboración prestada por usted y su grupo de trabajo

Cordialmente

Jaime Alberto Pineda Ramirez
Estudiante Especialización Seguridad Informática
UNAD La Dorada

Fuente: El autor.

Anexo 4. Lista de chequeo políticas de seguridad – acceso físico

Empresa: Dirección Territorial de Salud de Caldas		
Dominio: Auditoria Interna		
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"		
Auditor: Ing. Jaime Alberto Pineda Ramirez		
Entrevistado: Ing. Alonso Jimenez - Director de Sistemas DTSC		
Cargo: Profesional Universitario Grado 1		
Política	***Se cumple***	
	Si	***No***
Acceso Físico		
La entidad dispone de un área exclusiva para el centro de cómputo y comunicaciones, donde se ubicarán los sistemas de telecomunicaciones y servidores	X	
Los sistemas de comunicaciones están protegidos de tal forma que no se tenga acceso físico fácilmente.	X	
El acceso de terceras personas debe ser registrado, debidamente identificado y vigilado, portara un carnet que le es asignado por el área de seguridad de las instalaciones.		X
Las visitas de personas internas o externas de la institución, a las áreas seguras de los centros de cómputo procesamiento y comunicaciones, serán supervisadas por un empleado de la dependencia de sistemas.		X
Las visitas a los centros de cómputo, procesamiento y comunicaciones se realizaran en un horario establecido por la dirección de sistemas.		X
El personal responsable y autorizado de mover, cambiar, extrae cualquier elemento de computo será únicamente empleados del área de sistemas.	X	
Data Center		
Tener una puerta de acceso de vidrio templado transparente.	X	
Ser un área restringida, con control de acceso, el acceso será solo del personal autorizado.	X	
Mantener libre de polvo.	X	
Poseer elementos para medir temperatura.	X	
Mantener temperatura a 21 grados centígrados.	X	
Respaldo de energía redúndate.	X	
Estándares de protección eléctrica vigente.	X	
Sistema de tierra y protección e instalaciones eléctricas.	X	
Control de humedad		X
Prevención y protección de incendios.	X	
Sistema de Extinción.	X	
Infraestructura		
Cableado estructurado con estándares vigentes		X
Resguardo de equipos de cómputo bajo supervisión del área de sistemas.	X	

Fecha: Octubre 31 de 2016

Auditor — **Entrevistado**

Fuente: El autor.

Anexo 5. Lista de chequeo políticas de seguridad - respaldo

Empresa: Dirección Territorial de Salud de Caldas		
Dominio: Auditoria Interna		
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"		
Auditor: Ing. Jaime Alberto Pineda Ramirez		
Entrevistado: Ing. Alonso Jimenez - Director de Sistemas DTSC		
Cargo: Profesional Universitario Grado 1		
Política	***Se cumple***	
	Si	***No***
Instalaciones de equipos de cómputo		
Contar con planos actualizados de las instalaciones eléctricas y de comunicaciones de la red.	X	
Las instalaciones eléctricas y de comunicaciones están resguardadas del paso de personas y libres de interferencias electromagnéticas.	X	
Control		
Se lleva un control total y sistematizado de los recursos de cómputo y licenciamiento.	X	
Cuando ingresa o se retira un empleado a la estructura orgánica de la institución el área de talento humano le avisa al área de sistemas para activar o desactivar el respectivo usuario.		X
Respaldos		
Las Bases de Datos serán respaldadas según plan de respaldos implementado por la entidad. Contemplando copias completas e incrementales.	X	
Las Bases de Datos deberán de tener una réplica en uno o más equipos remotos en lugares seguros.	X	
Copias de los respaldos deberán estar almacenados en un lugar seguro y distante a la institución.	X	
Los usuarios tendrán un árbol de directorios configurado para realizar respaldo de forma automática, debidamente configurado por el área de sistemas.		X
Los usuarios deberán solicitar al área de sistemas realizar respaldo de información que este por fuera de las anteriores proposiciones.		X
Uso		
Los usuarios deberán hacer uso adecuado de los recursos tecnológicos de cómputo y de red que la institución ha puesto a su disposición y de los demás empleados.	X	
Los usuarios solo solicitaran apoyo en problemas tecnológicos al personal autorizado del área de sistemas.	X	
El correo electrónico institucional será de uso exclusivo para las actividades		X

Fecha: octubre 31 de 2016

Auditor

Alonso Jimenez

Entrevistado

Fuente: El autor.

Anexo 6. Lista de chequeo políticas derecho de autor

Empresa: Dirección Territorial de Salud de Caldas		
Dominio: Auditoria Interna		
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"		
Auditor: Ing. Jaime Alberto Pineda Ramirez		
Entrevistado: Ing. Alonso Jimenez - Director de Sistemas DTSC		
Cargo: Profesional Universitario Grado 1		
Política	***Se cumple***	
	Si	***No***
Derechos de Autor		
Se establece como prohibición la inspección, copia y almacenamiento de programas, software o fuentes que vayan contra las leyes de derecho de autor.	X	
Se establece como prohibición realizar copias de los programas propios o utilitarios instalados en la institución.	X	
Se prohíbe instalar programas o software, solo el personal autorizado del área de sistemas lo puede realzar.	X	
Si se va a utilizar software libre, solo el personal del área de sistemas tendrá la faculta de instalarlo, y con previa solicitud para verificar el sistema de licenciamiento.		X
Se prohíbe descargar música y videos de internet.		X
Se prohíbe utilizar el interne de la entidad para escuchar música, ver videos o TV en línea.		X
Si se descubre a algún empleado realizando copias del software de la institución se procede a iniciar un proceso disciplinario.	X	
El personal del área de sistemas realizara periódicamente una revisión a los equipos de cómputo de los usuarios para verificar el inventario del software instalado.		X
Se establece desde la configuración del usuario que no pueda instalar ningún software.	X	
Si por algún motivo se encuentra software que no cumpla con los requisitos de licenciamiento, se procede a desinstalar e iniciar proceso de control interno contra el usuario.	X	
Lo usuarios NO utilizan la intranet para compartir música, videos o información personal		X
Lo usuarios que se enteren que alguno de sus compañeros está realizando actos que van en contra de los políticas aquí estipuladas deberán notificar al superior o al área de sistemas directamente.		X
Los usuarios que no apliquen las anteriores políticas anteriormente estipuladas serán sujetos a sanciones disciplinarias de la oficina de control interno.		

Fecha: octubre 31 de 2016

Auditor **Entrevistado**

Fuente: El autor.

Anexo 7. Lista de chequeo políticas de seguridad – Red de datos

Empresa: Dirección Territorial de Salud de Caldas
Dominio: Auditoria Interna
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"
Auditor: Ing. Jaime Alberto Pineda Ramirez
Entrevistado: Ing. Alonso Jimenez - Director de Sistemas DTSC
Cargo: Profesional Universitario Grado 1

Política	*Se cumple*	
	Si	*No*
Red		
La responsabilidad de los datos que se transmitan por la red, y emitidos desde un equipo de cómputo será únicamente responsabilidad del usuario	X	
No se puede destruir, eliminar o barrar información de los equipos de cómputo, sin la debida autorización del usuario propietario de los datos.		X
La red de datos será exclusivamente para las actividades laborales.		X
Las cuentas de usuarios serán controladas y configuradas únicamente por el área de sistemas.	X	
Software para realizar análisis del comportamiento de la red, será una actividad solo del área de sistemas.	X	
El mantenimiento preventivo y correctivo de la red de datos será realizado únicamente por el personal de sistemas.	X	
Todos los equipos portátiles y dispositivos móviles que se conecten al wifi, deben hacer la respectiva solicitud al área de sistemas.	X	
Los equipos conectados a los wifi de la institución están debidamente registrados en la bitácora de la oficina de sistemas.		X
Para los empleados se utilizar la red de wifi de PC-DTSC		X
Para los visitantes se utilizara la red de wifi PC-Visitantes		X
Correo electrónico		
Solo se utilizaran correos electrónicos institucionales		X
La creación de correos institucionales solo se realizara por parte del personal del área de sistemas.	X	
Para crear una cuenta de correo institucional a un empleado de la institución, la oficina de talento humano deberá expedir al área de sistemas una certificación de la vinculación laboral.	X	
Al ingresar a la cuenta de correo electrónico por primera vez, se le solicitara al usuario cambiar la contraseña.		X
La longitud de las contraseñas será igual o superior a ocho caracteres influyendo alfanuméricos y caracteres especiales.		X
La información enviada desde la institución a correos electrónicos será de cuentas oficiales.		X

Fecha: Noviembre 02 de 2016

Auditor **Entrevistado**

Fuente: El autor.

Anexo 8. Lista de chequeo políticas de seguridad – Sistema “Gestión Integrada de Bienestar Social”

Empresa: Dirección Territorial de Salud de Caldas
Dominio: Auditoria Interna
Procesos: Auditoria al Sistema de Seguridad del Sistema “Gestión Integrada de Bienestar Social”
Auditor: Ing. Jaime Alberto Pineda Ramirez
Entrevistado: Ing. Sebastian Martinez - Administrador Sistema “Gestión Integrada de Bienestar Social”
Cargo: Contratista

Política	***Se cumple***	
	Si	***No***
Gerencias		
No se darán usuarios, ni contraseñas a quienes estén desarrollando pasantías de universidades.	X	
Revisar logs constantemente		X
Monitoria los recursos de red		X
Identificación de usuarios y contraseñas		
Todos y cada uno de los usuarios de la red o sistemas de información tendrán un solo acceso con información de nombre de usuario y contraseña	X	
Ningún empleado recibirá usuarios o contraseñas sin que la oficina de talento humano expida la respectiva certificación de que existe una relación contractual.	X	
El empleado deberá aceptar y conocer las políticas de seguridad establecidas por la entidad, hasta ese momento se le configurara usuario y contraseña.		X
La oficina de sistemas le definirá el nombre de usuario.	X	
El usuario definirá su propia contraseña de acuerdo al estándar de longitud y caracteres especiales.	X	
Se configuraran los usuarios de tal forma que cuando ingresen por primera vez al sistema, se le solicite cambiar la contraseña que le fue asignada	X	
Los usuarios solo podrán ingresar a los datos que se le parametrizen con el usuario, de acuerdo al rol.	X	
Se configuraran los usuarios para que cada dos meses se les solicite cambio de contraseña		X
Al usuario ingresar por primera vez al sistema, tendra la opción de aceptar el acuerdo de confidencialidad de la información de acuerdo a lo establecido por las politicas y tratamientos de datos		X
Los usuarios no podran ser multilogin.	X	

Fecha: octubre 07 de 2016

Auditor

Sebastian Martinez

Entrevistado

Fuente: El autor.

Anexo 9. Lista de chequeo directivas de control

Empresa: Dirección Territorial de Salud de Caldas
Dominio: Auditoria Interna
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"
Auditor: Ing. Jaime Alberto Pineda Ramirez
Entrevistado: Ing. Alonso Jimenez - Director de Sistemas DTSC
Cargo: Profesional Universitario Grado 1

Directivas de Control	*Se cumple*	
	Si	*No*
Una sola cuenta por cada usuario	X	
Contraseñas con longitud y caracteres especiales de acuerdo al estándar solicitado		X
Bloqueo de lectura de medios de almacenamiento removibles.	X	
Bloque de página de Facebook	X	
Bloque de página de YouTube		X
Bloqueo de páginas para adultos	X	
Bloqueo de páginas de no interés.	X	
Bloqueo de descarga de música y videos		X
Cambio de contraseña obligatorio cada dos mese	X	
Límite de usuarios del sistema.		X
Límite de usuarios para ingreso a la plataforma "Gestión Integrada de Bienestar Social"		X
Configuración de respaldos en sitio	X	
Configuración de respaldos remotos	X	
Perfiles de usuarios según requerimientos		X
Perfiles con privilegios según requerimientos		X

Fecha: Octubre 25 de 2016

Auditor

Alonso Jimenez
Entrevistado

Fuente: El autor.

Anexo 10. Lista de chequeo directivas usuario final

Empresa: Dirección Territorial de Salud de Caldas
Dominio: Auditoria Interna
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"
Auditor: Ing. Jaime Alberto Pineda Ramirez
Entrevistado: Dra. Carmenza Osorio - Profesional de Vigilancia Salud Publica
Cargo: Contratista

Directivas Usuario Final	***Se cumple***	
	Si	***No***
Posee usuario al Sistema "Gestión Integrada de Bienestar Social"	X	
Accede constantemente al Sistema "Gestión Integrada de Bienestar Social"	X	
Conoce que tipo de usuario posee en el sistema		X
El sistema le ha solicitado realizar cambio de contraseña		X
Su perfil de usuario le permite exportar información	X	
El aplicativo le permite verificar información personal de los habitantes del departamento	X	
La información que exporta la ha enviado por correo electronico a otras personas e instituciones	X	
Cando deja de usuar el aplicativo por semanas, este se bloquea o inactiva		X
Ha recibido capacitación en uso del Sistema "Gestión Integrada de Bienestar Social"	X	
Ha recibido capacitación o información sobre las politicas de seguridad del aplicativo Sistema "Gestión Integrada de Bienestar Social"		X

Fecha: octubre 20 de 2016

Auditor **Entrevistado**

Fuente: El autor.

Anexo 11. Cuestionario director sistemas TIC

Empresa: Dirección Territorial de Salud de Caldas
Dominio: Auditoria Interna
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"
Auditor: Ing. Jaime Alberto Pineda Ramirez
Entrevistado: Ing. Alonso Jimenez - Director de Sistemas DTSC
Cargo: Profesional Universitario Grado 1
Cuestionario
* Como director de TIC de la dirección Territorial de Salud de Caldas, considera que la institución cuenta con un esquema de seguridad con politicas y controles acorde a los requisitos establecidos en las directivas de seguridad informatica?
Rta: SI. Pienso que por se la entidad del area de la salud, donde se trabaja con información de mucha importancia tanto de población, como de entidades prestadoras de salud (hospitales, clinicas, centros de salud), siempre se debe estar con altos niveles de seguridad informatica, que permita proteger esa información de posibles ataques. Por otro lado la entidad esta certificada en calidad, lo que nos obilga tambien a tener ciertos controles establecidos.
* Considera que se puede mejorar el esquema de seguridad informatica de la Dirección Territorial de Salud de Caldas?
Rta: SI. Desde el punto de vistas de los sistemas, siempre se debe estar en continua actualización, ya que los ciberdelincuentes nunca descansan y siempre van a estar queriendo sabotear a las entidades y mas a estas que poseen información sensible. Y para evitarlo tiene que estar mejorando cada dia.
* Apoya usted la iniciativa de realizar una auditoría interna a uno de los sistemas de información de la entidad?
Rta: SI. Claro que si, apoyo la iniciativa de realizar esta auditoría al sistema de información Gestión Integrada de Bienestar Social, ya que los resultados que arroge sera de gran importancia para nosotros como area y como institución.
* Como rutina laboral, revisan constantemente que se este cumpliendo con las politicas y controles de seguridad establecidos?
Rta: SI. Esta establecido que cada 6 meses se realice una revisión a estas politicas y controles. Pero hay que dejar en claro que si se presenta algun intento de sabotaje o ataque, la politica establece que se debe proceder inmediatamente a verificar el check list.

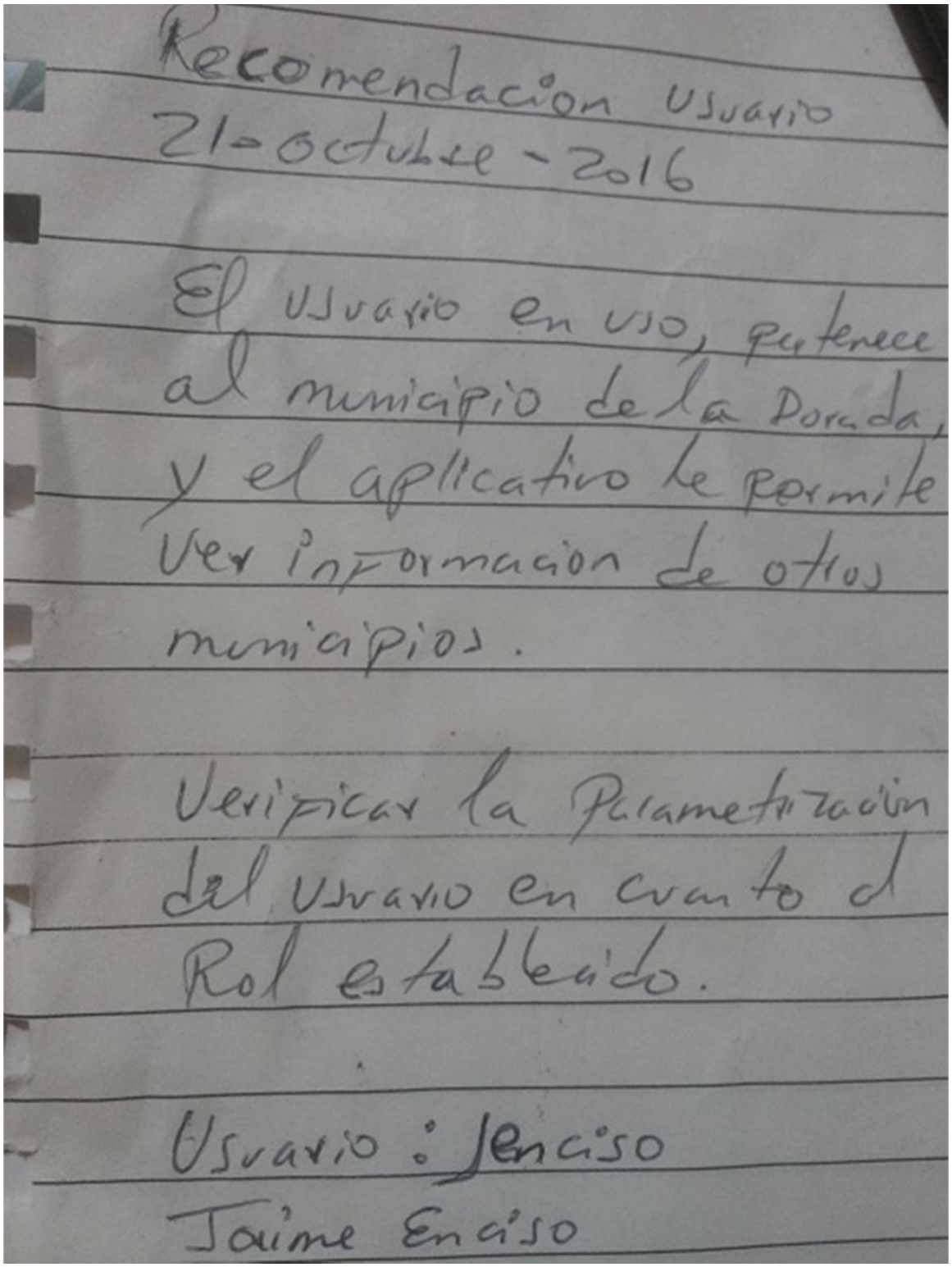
Fuente: El autor.

Anexo 12. Cuestionario administrador sistemas

Empresa: Dirección Territorial de Salud de Caldas
Dominio: Auditoria Interna
Procesos: Auditoria al Sistema de Seguridad del Sistema "Gestión Integrada de Bienestar Social"
Auditor: Ing. Jaime Alberto Pineda Ramirez
Entrevistado: Ing. Sebastian Martinez - Administrador Sistema "Gestión Integrada de Bienestar Social"
Cargo: Contratista
Cuestionario
* Como administrador del Sistema "Gestión Integrada de Bienestar Social", considera que se estba aplicando la politicas y controles de seguridad de acuerdo a lo establecido por las directivas de seguridad?
Rta: SI. Es importante resaltar que muchas de las politicas y controles de seguridad del aplicativo estan bajo el esquema de seguridad de la entidad, ya que el aplicativo esta alojado en el servidor de la DTSC. Pero de igualmanera el sistema aplica directivas propias de control y roles de usuario desde el modulo de configuración y parametrización.
* Considera que se puede mejorar el esquema de seguridad del Sistema "Gestión Integrada de Bienestar Social" ?
Rta: Si. En especial lo que tiene que ver con los usuarios y configuración y parametrización, debido a que no siempre se cumple con las condiciones de seguridad al momento de crear usuarios y contraseñas.
* Apoya usted la iniciativa de realizar una auditoría interna al sistemas de información "Gestión Integrada de Bienestar Social" de la Dirección Territorial de Salud de Caldas?
Rta: SI. Por supuesto y bien sea por que es una directriz de la dirección general y por iniciativa propia, me gustaria que se realice esta auditoría, ya que me brindaria mayor seguridad y confiabilidad sobre la información que se procesa en dicho aplicativo.
* Se presentan continuamente problemas con la seguridad del sistema "Gestión Integrada de Bienestar Social" ?
Rta: No. Hasta el momento no se ha presentado ningun intento de sabotaje por parte de algun intruso, pero Si se han presentado problemas con los usuarios que la contraseña es muy debil en su nivel de seguridad.

Fuente: El autor.

Anexo 13. Recomendación usuario



Fuente: El autor.