PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

TABLA DE CONTENIDO

INTRODUCCION 4

1.1 OBJETIVO GENERAL 5

1.2 OBJETIVOS ESPECIFICOS 5

2. GLOSARIO 6

3. ANALISIS DE LA SITUACION ACTUAL DE LA ENTIDAD. 8

3.1 MISIÓN 8

3.2 VISION 8

3.3 OBJETIVOS INSTITUCIONALES 8

3.4 PRINCIPIOS 9

3.5. VALORES 10

3.6. ORGANIGRAMA 11

3.7 MAPA DE PROCESOS 12

3.8 POLITICA DE SEGURIDAD DE LA INFORMACIÓN 13

3.9 INFRAESTUCTURA TECNOLÓGICA DE LA ENTIDAD 13

3.9 ROLES, FUNCIONES 13

3. PRUEBAS DE EFECTIVIDAD 15

3.1 CONTEXTO DE ANALISIS 15

3.2 RECONOCIMIENTO DEL OBJETIVO 16

3.3 MODELADO DE AMENAZAS.....17

3.4 ANÁLISIS DE VULNERABILIDADES EN LA PRUEBAS.....17

3.4 TIPO DE PRUEBA EJECUTADAS.....18

4. PLANEACIÓN DE TI.....60

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....63

INTRODUCCION

El presente documento expone los resultados de los ejercicios de Pruebas de efectividad en los componentes tecnológicos y físicos de la contraloría general de Santander que trabajen con información privilegiada de la entidad.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

1.1 OBJETIVO GENERAL

Estructurar un documento que logre lineamientos y las buenas prácticas de Seguridad de la Información en la Contraloría General de Santander.

1.2 OBJETIVOS ESPECIFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la Contraloría General de Santander.
- Contribuir a mejorar los procesos de intercambio de información pública en la Contraloría General de Santander.
- Optimizar la gestión de la seguridad de la información al interior de la Contraloría General de Santander.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

2. GLOSARIO

- **Activo:** recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

- **Amenaza:** cualquier agente, condición o circunstancia que podría causar daño, pérdida, o podría comprometer un activo de información.

- **Ataque Informático:** evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

- **Denegación de servicio (DoS):** ataque informático a un sistema o a una red que causa que un servicio o un recurso sea inaccesible por sus usuarios legítimos. Normalmente se ejecuta sobrecargando los recursos computacionales o el canal de comunicaciones utilizado por los usuarios para acceder al servicio.

- **Enumeración:** listado de diferente tipo de información sobre un dispositivo digital; dentro de la información que puede ser enumerada se tienen cuentas de usuarios, tipos de servicios habilitados, etc.

- **Impacto:** consecuencia de la materialización de una amenaza.

- **Intruso informático:** persona que logra acceso a un sistema sin autorización.

- **Riesgo:** exposición o la posibilidad de pérdida o daño de los activos de TI dentro de esa infraestructura de TI.

- **Vulnerabilidad:** existencia de una falla de software, diseño de la lógica, o error en la aplicación que puede conducir a un acontecimiento inesperado y no deseable para el sistema.

- **MITRE CVE List:** (Common Vulnerabilities and Exposures): Lista de vulnerabilidades definidas y mantenidas por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

3. ANALISIS DE LA SITUACION ACTUAL DE LA ENTIDAD.

3.1 MISIÓN

“Ejercer vigilancia y control participativo a la gestión fiscal en el Departamento de Santander, buscando determinar si cumple con a los principios, políticas, planes, programas, proyectos, presupuestos y normatividad aplicables y sus resultados aportan al desarrollo sostenible y a los fines esenciales del Estado.”

3.2 VISION

“En el 2025, la Contraloría General de Santander será reconocida como un órgano de control y vigilancia moderno, oportuno y efectivo, líder del mejoramiento de la gestión fiscal y aliado estratégico del control social, político e interno de sus entidades vigiladas.”

3.3 OBJETIVOS INSTITUCIONALES

- Mejorar la cobertura, oportunidad y efectividad del control fiscal, mediante las auditorías enfocadas en los riesgos fiscales de los sujetos, puntos de control, operaciones, procesos y recursos objeto de control fiscal e implementar controles en las etapas claves del proceso auditor para mejorar su oportunidad y calidad.

- Mejorar los tiempos y la calidad de las actuaciones procesales y de los fallos de responsabilidad fiscal para obtener el resarcimiento de los daños ocasionados al patrimonio público como consecuencia de la conducta dolosa o gravemente culposa de quienes realizan gestión fiscal o de servidores públicos o particulares que participen, concurran, incidan o contribuyan directa o indirectamente en la producción de los mismos.

- Los controles, social, político e interno son complementos indispensables del control fiscal, por ello desde la Contraloría GENERAL DE SANTANDER serán promovidos y gestionados de manera prioritaria.

- Obtener y utilizar eficientemente recursos económicos que permitan disponer de talento humano, y elementos físicos y tecnológicos necesarios para el logro de los objetivos y las funciones misionales de la Contraloría General De Santander.

- Articular con organismos de control, investigación y vigilancia, para la defensa del patrimonio público.

3.4 PRINCIPIOS

- La Contraloría General de Santander identifica y ejerce las labores bajo los siguientes principios éticos:

- **TRANSPARENCIA:** La Contraloría General de Santander desarrolla su misión de cara a la comunidad.

- **EQUIDAD:** En el cumplimento de los fines misionales, los empleados públicos y contratistas de la Contraloría General de Santander propenderán por lograr el equilibrio en la aplicación de los diferentes sistemas de auditoría y cobertura que atienda los riesgos en el manejo de los fondos públicos y las necesidades de las poblaciones vulnerables.

- **EFICIENCIA:** La excelente gestión de los empleados públicos, contratistas y demás personas vinculadas con los fines misionales de la Contraloría General de Santander se observa en el cumplimiento de sus funciones y responsabilidades desarrolladas con agilidad y profesionalismo.

- **ECONOMÍA:** Se tendrá en cuenta que las normas de procedimiento se utilicen para agilizar las decisiones, que los procesos se adelanten en el menor tiempo y con la menor cantidad de gastos de quienes interviene en ellos.

- **IMPARCIALIDAD:** La Contraloría general de Santander deberá actuar teniendo en cuenta que la finalidad de los procedimientos consisten en asegurar y garantizar los derechos de todas las personas sin discriminación alguna.

- **CUMPLIMIENTO:** La realización de las responsabilidades de los empleados públicos, contratistas y demás personas vinculadas con los fines misionales de la Entidad, teniendo como meta clara las necesidades de la comunidad y sus compromisos con la ley.

- **IGUALDAD:** Todos los ciudadanos y los entes sujetos de control son iguales frente al ejercicio del control fiscal.

- **INTEGRIDAD:** El ejercicio de las funciones se realizan de manera intachable y actuando con rectitud.

- **EFICACIA:** Los procedimientos deben lograr su finalidad removiendo de oficio los obstáculos formales y evitando decisiones inhibitorias.

- **CELERIDAD:** Se dará el impulso oficioso de los procedimientos y se suprimirán los trámites innecesarios.

- **PUBLICIDAD:** La Contraloría dará a conocer sus decisiones mediante comunicaciones, notificaciones o publicaciones.

- **CONTRADICCION:** La comunidad y los interesados tendrán oportunidad de conocer y controvertir las decisiones por los medios legales.

3.5. VALORES

Son características morales positivas que toda persona posee, como atributos o cualidades nuestras y de los demás, estos constituyen un ambiente de armonía gratificante en las relaciones interpersonales.

La Contraloría General de Santander reconoce y actúa bajo los siguientes valores éticos:

- **HONESTIDAD**: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés de la comunidad sobre cualquier tipo de interés particular.

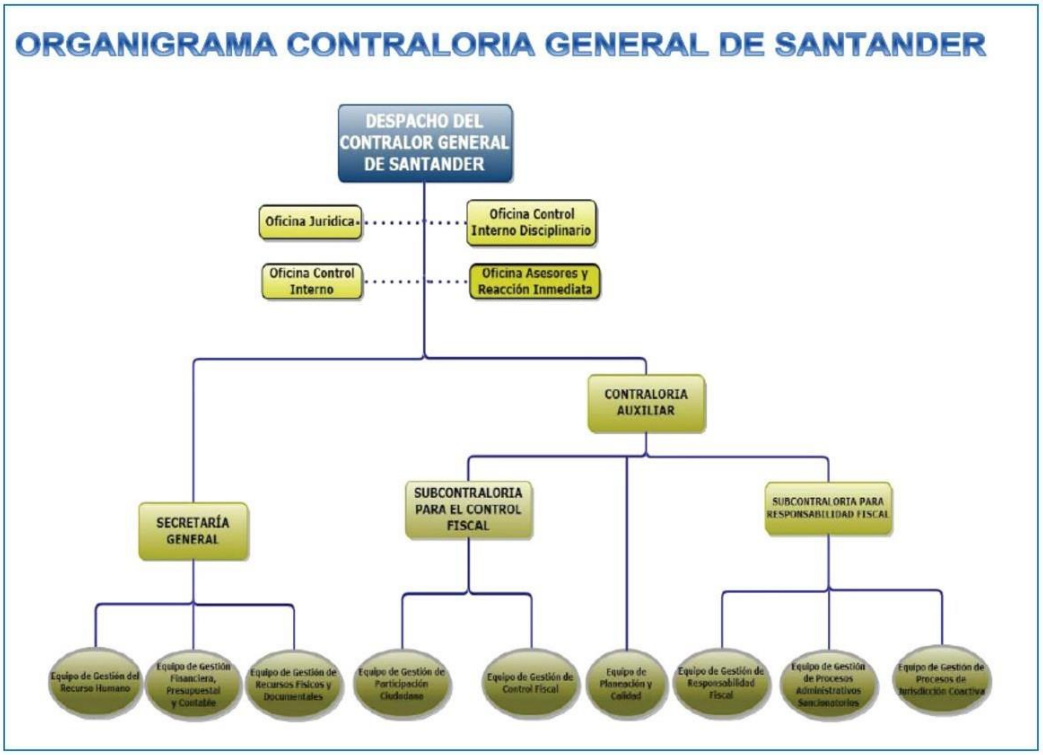
- **RESPETO**: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

- **COMPROMISO**: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar y con trabajo y dedicación garantizo el cumplimiento de la labor fiscalizadora en pro del mejoramiento continuo.

- **DILIGENCIA**: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención prontitud, destreza y eficiencia, para de esta manera optimizar el uso de los recursos del estado.

- **JUSTICIA**: Actuó con imparcialidad, garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

3.6. ORGANIGRAMA

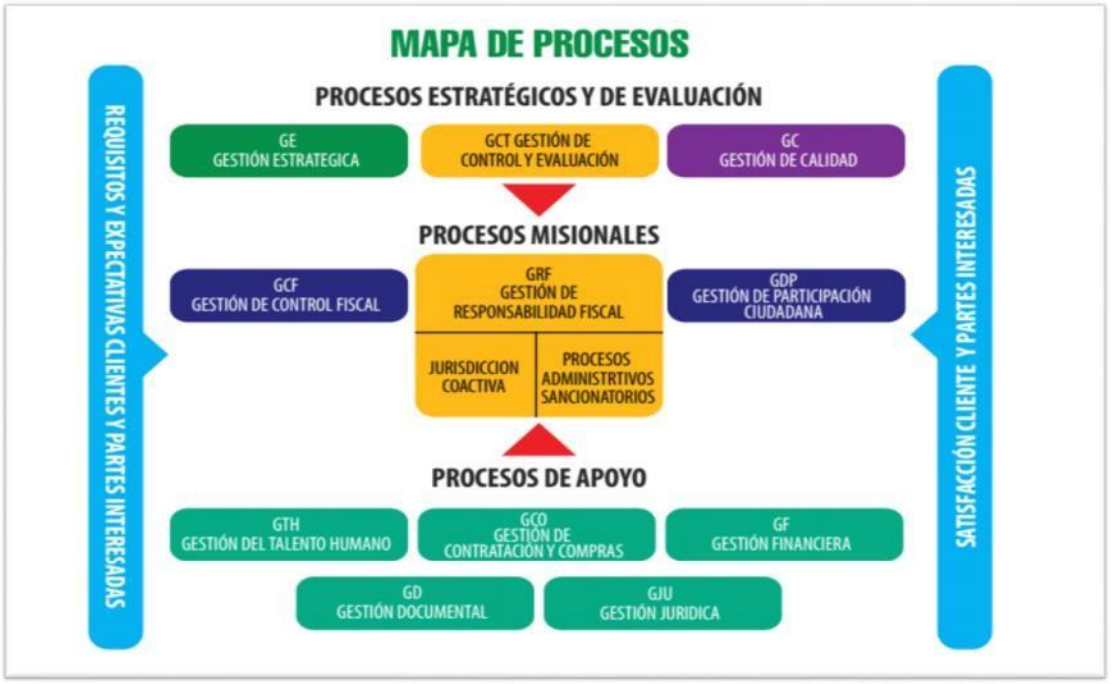


Análisis: Se identifica por en el organigrama que la entidad no tiene definido un responsable directo de seguridad de la información o una dependencia que ejecute dichas actividades.

Definir esta jerarquía en un organigrama es fundamental para agilizar los procesos y flujos de trabajo buscando garantizar la integridad, confidencialidad y disponibilidad de la Información de la contraloría general de Santander.

Cabe resaltar que dichas funciones podría asumirla un área u oficina de las existentes actualmente pero habría que actualizar las funciones y responsabilidades pertinentes.

3.7 MAPA DE PROCESOS



Análisis: Se identificó en el mapa de procesos recibido, que se tienen dimensionados los procesos estratégicos, misionales y de apoyo.

No se evidencia un proceso de gestión de TI que podría estar ubicado como proceso de apoyo en la ejecución de los procesos estratégicos y misionales de la Contraloría General de Santander.

La gestión de seguridad de la información puede estar catalogada como un proceso adicional de apoyo pero puede ser delegado a otro proceso de control que garantice un adecuado manejo de la Información.

3.8 POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Análisis: La entidad **NO** cuenta actualmente con una política de seguridad que aporte lineamientos para la seguridad de la información.

3.9 INFRAESTUCTURA TECNOLÓGICA DE LA ENTIDAD

La entidad **NO** cuenta actualmente con la identificación y clasificación de los activos de información que poseen por lo tanto no se han identificado, clasificado y etiquetado los activos de Información con los que cuenta la entidad en la ejecución de sus actividades diarias.

La entidad **NO** cuenta actualmente con el diagrama de la infraestructura de la red cableada e inalámbrica que posee actualmente.

La entidad **NO** cuenta actualmente con servidores de red que presten servicios propios tanto para usuarios internos o externos.

Los servicios que se prestan para usuarios externos están dados por un convenio interadministrativo de cooperación para el uso de la herramienta SIA que es de propiedad de la Auditoría General de la República.

3.9 ROLES, FUNCIONES

La Contraloría General de Santander dentro de sus manuales de funciones de los cargos así:

- Nivel directivo
- Nivel Asesor
- Nivel Profesional
- Nivel Técnico
- Nivel Asistencial

A revisar en los manuales de funciones que la entidad tenga activos actualmente con el objetivo de identificar lo comprendido y designado en materia de seguridad de la información para los servidores públicos, lo realizado en seguridad en los procesos y el estado de las políticas de la entidad. Se evidenció lo siguiente:

Los cargos a los cuales se les analizaron sus funciones referentes a seguridad de la información fueron para los niveles Profesional, Técnico y Asistencial ya que son los que manipulan directamente la información y hacen parte del alcance de este informe.

Se evidencio al revisar los manuales de funciones para los cargos de Nivel Profesional, Nivel Técnico y Nivel Asistencial de la Contraloría General de Santander que se cuenta a manera global las siguientes funciones específicas que podrían dar a entender responsabilidades de los funcionarios a nivel de seguridad de la información y son:

- Responder por la seguridad y conservación de los documentos que reciba o le sean entregados en el examen de cuentas por revisar o en las Auditorías en que participe como comisionado.
- Mantener absoluta reserva de la información pertinente al proceso fiscal, jurisdicción coactiva y administrativo sancionatorio.
- Mantener absoluta reserva de la información pertinente al proceso administrativo sancionatorio

Adicionalmente no se encontraron funciones específicas en los cargos revisados que involucren la integridad, confidencialidad y disponibilidad de la información manejada y administrada en diferentes medios (magnéticos, físicos etc.) sobre las labores realizadas

3. PRUEBAS DE EFECTIVIDAD

3.1 CONTEXTO DE ANALISIS

El contexto es la ejecución de Pruebas de efectividad de los controles implementados en la infraestructura tecnológica de la contraloría general de Santander.

Escenario	Canal	Descripción / Vectores de acceso
Externo – Red de Internet	Internet	Pruebas de efectividad y vulnerabilidades a la página web de la entidad http://www.contraloriasantander.gov.co realizado desde internet
Interno- Red Lan	Red Local	• Red de datos de la contraloría general de Santander • Equipos conectados a la red inalámbrica y cableada de la contraloría general de Santander. • Procedimientos y practicas usadas actualmente que tengan que ver con información de la entidad.

Tabla 5. Vectores de acceso para evaluación de dispositivos de red

Es importante tener en cuenta que estas pruebas no tuvieron como objetivo identificar solamente una vulnerabilidad sobre un sistema específico o algún sistema desactualizado, sino que la meta principal fue identificar los riesgos de seguridad de la información existente en los controles de toda índole y que fueron evaluados a través de las pruebas, para que la entidad tome las medidas proactivas/preventivas para que se mitiguen los riesgos encontrados.

La ejecución de estas pruebas de efectividad buscan que la entidad alcance específicamente un nivel de protección inicial para que implemente posteriormente un modelo de seguridad y privacidad de la información bajo un modelo de mejoramiento continuo y a su vez sirva como insumo de controles necesarios de dicho modelo.

Las pruebas se realizaron en horarios laborales ya que los dispositivos objetivos fueron los equipos de cómputo de los funcionarios de la entidad.

Debido a las limitaciones de equipos e infraestructura tecnológica en seguridad de la información y de los servicios propios que presta la entidad en la red de internet, las direcciones IP objetivo de estas pruebas de efectividad, son las direcciones IP internas que se descubrieron en las pruebas.

Como no se cuenta con ningún servicio en la red ni con equipos de hardware tipo servidor. Las vulnerabilidades encontradas no fueron explotadas ya que su corrección depende de actualizaciones del sistema operativo de los equipos analizados y vulnerarlos afectaría la disponibilidad del equipo analizado; mas su corrección debe darse por una política de actualización que se debe crear en la entidad.
Dichas explotaciones de vulnerabilidades deben ser aplicadas por la entidad posterior a la corrección de las mismas en cada máquina comprometida e identificada en las pruebas ejecutadas.

3.2 RECONOCIMIENTO DEL OBJETIVO

Según la propuesta ofertada, se obtuvo información a través de las etapas de levantamiento de la misma aplicando el método **ACTIVO y SEMI-PASIVO** según la guía metodológica número 01 de pruebas de efectividad del componente 4 (seguridad y privacidad de la información) del manual de gobierno en línea para entidades públicas con las siguientes actividades:

- Escaneo de puertos.
- Análisis de vulnerabilidad a puertos abiertos
- Búsqueda de directorios, archivos que no están públicamente disponibles.
- Organigrama de la entidad.
- Bloques de direccionamiento IP adquirido.
- Identificación de las instalaciones físicas.
- Escaneo a la página web

3.3 MODELADO DE AMENAZAS

Debido a lo identificado inicialmente el etapa de levantamiento de información donde la entidad no cuenta con servicios propios en equipos dedicados exclusivamente a la prestación de servicios (servidores) y no se tienen una identificación de los activos de información ni del proceso de sistemas de información en su mapa de procesos actuales, las pruebas no se orientaron hacia la relación de que beneficio podría obtener un atacante si logra el objetivo de penetrar el sistema debido a que no hay claridad en los activos clasificados y etiquetados a proteger por parte de la entidad.

Es por esto que las pruebas se orientaron al análisis de vulnerabilidades expuestas por los sistemas operativos, dispositivos de hardware, de enrutamiento y conocimiento del personal en la protección de la información personal y de trabajo diario.

3.4 ANÁLISIS DE VULNERABILIDADES EN LA PRUEBAS

Según el modelado de amenazas definido para estas pruebas de efectividad se trató de descubrir falencias en los sistemas y aplicaciones nivel del host específico a un inventario de máquinas descubiertas en las pruebas.

Se ejecutaron de dos maneras:

- Con una análisis ACTIVO donde se tuvo contacto directo con los objetivos (equipos de computo) a probar de manera automática a través de software especializado en escaneo de puertos, escaneo basado en servicios, escaneo específico para servicios web y escaneo de red.

- Con una análisis PASIVO a través del uso de metadatos en archivos publicados en internet, que pueden contener información sobre el tipo de servidor, nombres de dominio, direccionamiento IP, etc.

Una vez se realizó la verificación de las vulnerabilidades con base a los métodos anteriores, se investigó en las diferentes bases de datos para comprobar la veracidad de lo que se ha encontrado y las posibles maneras de apalancar o aprovechar las fallas identificadas basados en las siguientes fuentes de información:

Bases de datos de vulnerabilidades (CVE)
Alertas o publicaciones de proveedores de plataformas. Bases de datos de exploits.

Estas investigaciones y sus resultados son dados en las recomendaciones del presente informe para su posterior aplicación por parte de la entidad.

Sin embargo como las vulnerabilidades encontradas fueron corroboradas con las Bases de datos de vulnerabilidades (CVE), en los resultados se menciona el impacto al que se encuentra expuesta el equipo o dispositivo en el cual fue encontrado.

3.4 TIPO DE PRUEBA EJECUTADAS

Se ejecutaron pruebas de efectividad denominadas “Pruebas Con Conocimiento Completo Del Entorno” basados en la toda la información recopilada relacionada al sistema objetivo con acompañamiento del personal responsable de los sistemas informáticos de las entidad

9.2 ALCANCE DE LAS PRUEBAS EJECUTADAS

A continuación se describen los alcances de las pruebas ejecutadas con las modificaciones hechas debido a la limitante encontrada en la falencia de recursos informáticos en seguridad de la información por parte de la entidad así:

Nombre de la Prueba: Sondeo de red
Descripción: Recolección de datos, obtención de información y política de control para encontrar el número de sistemas alcanzables que deben ser analizados en las pruebas de efectividad

Resultado Esperado: Nombres de Dominio Nombres de Servidores Direcciones IP Mapa de Red Información ISP / ASP Propietarios del Sistema y del Servicio Posibles limitaciones del test
Insumos: Acceso a la red de la contraloría general de Santander
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Identificación de los Servicios de Sistemas
Descripción: Validación de la recepción del sistema a protocolos tunelizados, encapsulados o de enrutamiento en los equipos de cómputo de la entidad
Resultado Esperado: Puertos abiertos, cerrados y filtrados Lista de los protocolos descubiertos Servicios activos Tipos de Servicios Tipo de Sistema Lista de sistemas activos
Insumos: Acceso a la red de la contraloría general de Santander
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Revisión de Privacidad
Descripción: Evidenciar cómo se encuentra configurada la privacidad en posibles vulnerabilidades que impliquen el almacenamiento, transmisión y control de datos en la página web de la entidad.
Resultado Esperado: Posibles vulnerabilidades en la página web de la entidad.
Insumos: Acceso al dominio web de la entidad
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Búsqueda y Verificación de Vulnerabilidades
Descripción: Identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en los equipos de los funcionarios de la entidad.
Resultado Esperado: Listado de posibles vulnerabilidades de denegación de servicio Listado de áreas securizadas a través de ocultación o acceso visible Listado de vulnerabilidades actuales eliminando falsos positivos Listado de convenciones para direcciones de e-mail, nombres de servidores, etc..
Insumos: Acceso a la red de la contraloría general de Santander
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Testeo de Aplicaciones de Internet
Prueba **NO EJECUTADA** por estar fuera del alcance ya que la entidad no cuenta con aplicaciones funcionales en internet que sean de propiedad de la contraloría general de Santander.

Nombre de la Prueba: Enrutamiento
Descripción: Evaluar los dispositivos de enrutamiento de la entidad para obtener:
Resultado Esperado: Se trató de Tipo de Router y Propiedades implementadas Información del Router como servicio y como sistema
Insumos: Acceso a la red de la contraloría general de Santander Acceso a la configuración del Router de la entidad
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Testeo de Control de Acceso
Descripción: La prueba inicialmente buscaba revisar las reglas de control de acceso (ACL) configuradas en dispositivos de hardware o software que tuviese la entidad para la gestión y filtro de la totalidad de tráfico entrante y saliente de los computadores de la red interna. Como se aclaró que la entidad no cuenta con este tipo de dispositivos de seguridad debido a la infraestructura tecnológica con la que se cuenta; La prueba se basó en la revisión de las configuraciones que se tenga para controlar el acceso a dispositivitos tanto de red cableada como red inalámbrica. Dicha revisión se hizo a través de una lista de chequeo de configuración mínima de seguridad
Resultado Esperado: Verificación de las configuraciones actuales configuradas como control de acceso en el dispositivo para identificar que exista una configuración mínima de seguridad
Insumos: Acceso a la red de la contraloría general de Santander Acceso a la configuración del dispositivo enrutador

Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Testeo de Sistema de Detección de Intrusos
Descripción: Prueba NO EJECUTADA por estar fuera del alcance ya que la entidad no cuenta con un sistema de detección de intrusos (IDS)

Nombre de la Prueba: Verificación de Redes Inalámbricas [802.11]
Descripción: verificación del acceso a redes WLAN 802.11
Resultado Esperado: Verificación de las políticas para redes inalámbricas WLAN 802.11 para obtener las configuraciones o políticas definidas para el acceso a redes inalámbricas.
Insumos: Acceso a la red de la contraloría general de Santander Acceso a los Routers inalámbricos de la entidad
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Verificación de Dispositivos de Entrada Inalámbricos
Descripción: Verificar los dispositivos de entrada inalámbricos tales como ratones y teclados. Estos dispositivos se están popularizando aunque presentan profundas vulnerabilidades y compromisos en privacidad y seguridad
Resultado Esperado: Verificar los dispositivos de entrada inalámbricos tales como ratones y teclados conectados o usados en la red de la entidad para obtener si la entidad esta vulnerables a un conjunto de debilidades que han logrado explotar los atacantes con un sistema llamado 'mousejacking'.
Insumos: Acceso a la red de la contraloría general de Santander

Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Revisión de Privacidad de dispositivos inalámbricos
Descripción: Identificar que privacidad se tiene definida para los dispositivos de comunicación inalámbricos que pueden sobrepasar los límites físicos y monitorizados de la entidad
Resultado Esperado:

Configuraciones de privacidad existente o usadas actualmente
Insumos: Acceso a la red de la contraloría general de Santander
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Evaluación de Controles de Acceso físico
Descripción: Evaluar los privilegios de acceso de la entidad a sus bienes a través de puntos de acceso físicos
Resultado Esperado: Tipos de autenticación Tipos de sistemas de alarmas Lista de disparadores de alarmas
Insumos: Acceso a la red de la contraloría general de Santander
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nombre de la Prueba: Encuesta de Percepción de Seguridad de la información en funcionarios de la entidad (Valor Agregado a la propuesta inicial)

Descripción: Realizar una encuesta de precepción y conocimientos básicos de seguridad de la información en una muestra de 31 funcionarios de la contraloría general de Santander que servirá para futuras tomas de decisiones en capacitaciones adicionales que al entidad requiera impartir con el fin de fortalecer la seguridad de la información en la entidad a través de la aplicación de un total de 16 preguntas de respuesta cerrada con opción múltiple.
Resultado Esperado: Percepción de la seguridad de la Información en los funcionarios de la entidad
Insumos: Acceso a la red de la contraloría general de Santander
Responsables: Profesional Especializado en Seguridad de la información más un ingeniero de sistemas de apoyo asignados el contratista

Nota: Los alcances de las pruebas inicialmente ofertadas se modificaron según las limitaciones encontradas en la falta de dispositivos de seguridad y procedimientos que fueron identificados en la etapa de levantamiento de información.

9.3 RESULTADOS DE LAS PRUEBAS EJECUTADAS

10.8.1 Prueba denominada: Sondeo de red

Herramienta Usada:

- Netdiscover
- Zenmap

Resultados:

Con Netdiscover se obtuvo el rango utilizado y la clasificación de la red cableada 192.168.20.0/24

Con Netdiscover se obtuvo el rango utilizado y la clasificación de la red inalámbrica 192.168.88.0/24

Con Zenmap se obtuvo el mapa de red de los equipos conectados actualmente, direcciones IP, identificación de equipos y dispositivos periféricos (impresoras y escáner).

Se ejecutó el comando **#nmap -T4 -A -v 192.168.20.0/24**

- -T4 : Temporizador nivel 4
- -A : Habilitar traceroute y detección de Sistema operativo
- -v : Nivel de salida (los datos que se proporcionan de resultado)

El resultado de la ejecución de este comando en Zenmap es un listado de objetivos analizados de la red 192.168.20.0/24 que es el rango de IP que se utiliza actualmente en la contraloría general de Santander. La información primordial es la "tabla de puertos interesantes". Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado por cada máquina encontrada conectada a la red en ese momento y que nos da el estado de cada una.

Se detectaron en el momento de la ejecución 67 máquinas o pc conectados a la red y de la cual se obtuvo el siguiente mapa de red.

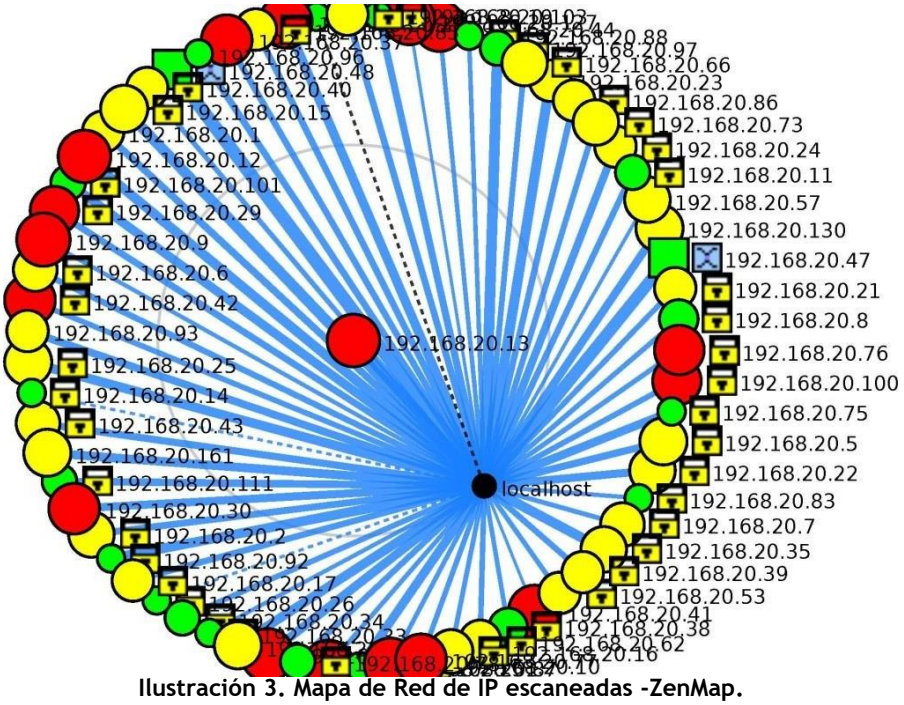


Ilustración 3. Mapa de Red de IP escaneadas -ZenMap.

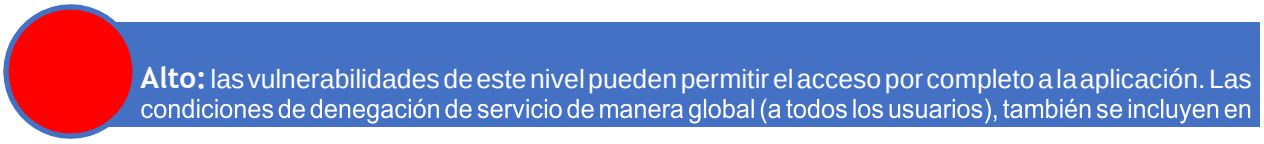
Los colores están dados en baso al criterio de evaluación del riesgo dada en el numeral 2.2.3 del presente informe

Las IP descubiertas en el escaneo fueron:192.168.20.1 192.168.20.2 192.168.20.5 192.168.20.6 192.168.20.7 192.168.20.8 192.168.20.9 192.168.20.10 192.168.20.11 192.168.20.12 192.168.20.13	192.168.20.14 192.168.20.15 192.168.20.16 192.168.20.17 192.168.20.19 192.168.20.21 192.168.20.22 192.168.20.23 192.168.20.24 192.168.20.25 192.168.20.26	192.168.20.28 192.168.20.29 192.168.20.30 192.168.20.31 192.168.20.33 192.168.20.34 192.168.20.35 192.168.20.37 192.168.20.38 192.168.20.39 192.168.20.40	192.168.20.41 192.168.20.42 192.168.20.43 192.168.20.44 192.168.20.47 192.168.20.48 192.168.20.49 192.168.20.51 192.168.20.53 192.168.20.57 192.168.20.60	192.168.20.62 192.168.20.66 192.168.20.73 192.168.20.75 192.168.20.76 192.168.20.77 192.168.20.78 192.168.20.83 192.168.20.85 192.168.20.86 192.168.20.87	192.168.20.88 192.168.20.92 192.168.20.93 192.168.20.96 192.168.20.97 192.168.20.100 192.168.20.101 192.168.20.103 192.168.20.111 192.168.20.127 192.168.20.130 192.168.20.161

No se identificaron Nombres de Dominio

No se identificaron Nombres de Servidores (equipos con Funciones de red específicos)

Las limitación al test se dan por la no tenencia en la entidad de servidores propios ya que es escaneo y pruebas de efectividad van más dirijas a este tipo de servicios, sin embargo se realiza el resto de las pruebas planificadas con el objetivo de evaluar las vulnerabilidades de la maquinas encontradas con clasificación de riesgo alto o High. (Color rojo según el mapa de red obtenido)



Dichas IP son:

192.168.20.9 , 192.168.20.10 , 192.168.20.12 , 192.168.20.13 , 192.168.20.28 , 192.168.20.29 , 192.168.20.30 , 192.168.20.31 , 192.168.20.37 , 192.168.20.42 , 192.168.20.44 , 192.168.20.76 , 192.168.20.77 , 192.168.20.100 , 192.168.20.127

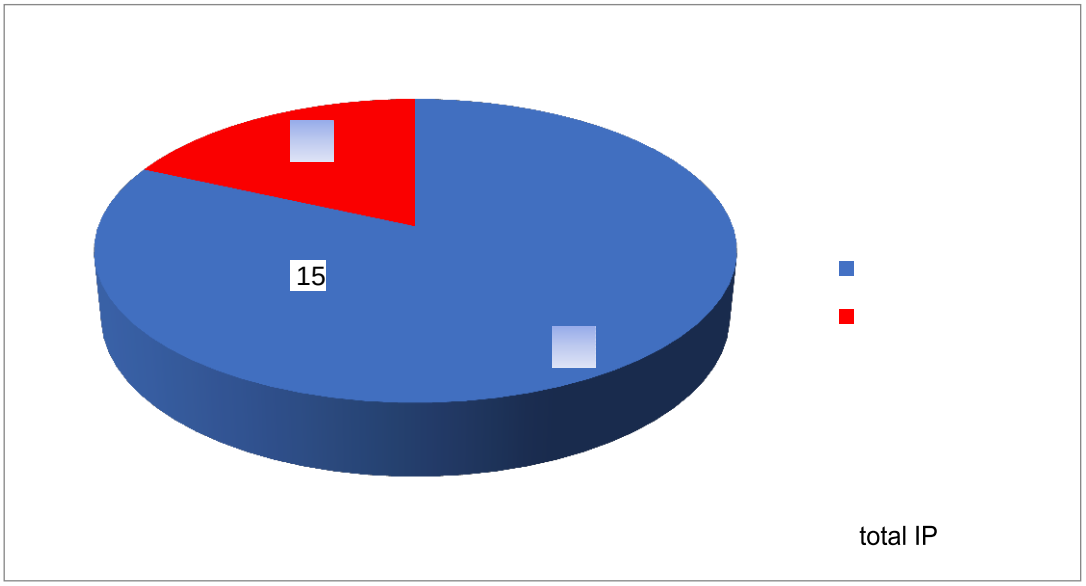


Ilustración 4. IP con Riesgo Alto por Puertos Abiertos.

Se obtuvo que el ISP contratado para la entidad, es la empresa Telebucaramanga

Nota. El reporte completo del resultado arrojado por la herramienta Zenmap para la red cableada se adjunta en el CD anexo a este informe.

10.8.2 Prueba denominada: Identificación de vulnerabilidades sobre los Servicios de Sistemas

Herramienta Usada:

- Zenmap

Resultados:

Se realiza el análisis de puertos a las maquinas descubiertas con riesgo alto clasificado en el numeral 2.2.3 del presente informe para identificar las posibles vulnerabilidades y servicios disponibles en cada una.

Los estados de los puertos encontrados son:

- *open* (abierto): significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en esepuerto.
- *filtered* (filtrado): indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a esepuerto.
- *closed* (cerrado): Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento.
- *unfiltered* (no filtrado): son aquellos que responden a los sondeos pero no puede determinar si se encuentran abiertos ocerrados.

A continuación se muestran las IP que se encontraron con puertos en estado *open*:

Dirección IP	Puerto	Estado	Servicio	tipo de Dispositivo
	135/tcp	open	msrpc	
	139/tcp	open	netbios-ssn	
	445/tcp	open	microsoft-ds	
	5357/tcp	open	http	
	5432/tcp	open	postgresql	

192.168.20.9	7070/tcp	open	ssl/realserver?	computador
	49152/tcp	open	msrpc	
	49153/tcp	open	msrpc	
	49154/tcp	open	msrpc	
	49159/tcp	open	msrpc	
	49160/tcp	open	msrpc	
	49161/tcp	open	msrpc	
192.168.20.10	135/tcp	open	msrpc	computador
	139/tcp	open	netbios-ssn	

	445/tcp	open	microsoft-ds	
	1110/tcp	filtered	nfsd-status	
	5800/tcp	open	vnc-http	
	5900/tcp	open	vnc	
	49152/tcp	open	msrpc	
	49153/tcp	open	msrpc	
	49154/tcp	open	msrpc	
	49155/tcp	open	msrpc	
	49156/tcp	open	msrpc	
	49157/tcp	open	msrpc	
192.168.20.12	21/tcp	open	ftp	impresora
	80/tcp	open	http	
	139/tcp	open	netbios-ssn	
	445/tcp	open	routersetup	
	515/tcp	open	printer	
	631/tcp	open	http	
	9090/tcp	open	soap	
	9100/tcp	open	jetdirect?	
	9101/tcp	open	jetdirect?	
	9102/tcp	open	jetdirect?	
	9103/tcp	open	jetdirect?	
192.168.20.13	21/tcp	open	ftp	impresora
	80/tcp	open	http	
	139/tcp	open	netbios-ssn	
	445/tcp	open	routersetup	
	515/tcp	open	printer	
	631/tcp	open	http	
	9090/tcp	open	soap	
	9100/tcp	open	jetdirect?	
	9101/tcp	open	jetdirect?	
	9102/tcp	open	jetdirect?	
	9103/tcp	open	jetdirect?	
	21/tcp	open	ftp	
	80/tcp	open	http	
	139/tcp	open	netbios-ssn	

192.168.20.28	445/tcp	open	routersetup	impresora
	515/tcp	open	printer	
	631/tcp	open	http	
	9090/tcp	open	soap	
	9100/tcp	open	jetdirect?	
	9101/tcp	open	jetdirect?	
	9102/tcp	open	jetdirect?	
	9103/tcp	open	jetdirect?	
192.168.20.29	135/tcp	open	msrpc	computador
	139/tcp	open	netbios-ssn	
	445/tcp	open	microsoft-ds	
	1801/tcp	open	msmq?	
	2103/tcp	open	msrpc	
	2105/tcp	open	msrpc	
	2107/tcp	open	msrpc	
192.168.20.30	21/tcp	open	ftp	impresora
	80/tcp	open	http	
	139/tcp	open	netbios-ssn	
	445/tcp	open	routersetup	
	515/tcp	open	printer	
	631/tcp	open	http	
	9100/tcp	open	jetdirect?	
	9101/tcp	open	jetdirect?	
	9102/tcp	open	jetdirect?	
192.168.20.31	21/tcp	open	ftp	impresora
	80/tcp	open	http	
	139/tcp	open	netbios-ssn	
	445/tcp	open	routersetup	
	515/tcp	open	printer	
	631/tcp	open	http	
	9090/tcp	open	soap	
	9100/tcp	open	jetdirect?	
	9101/tcp	open	jetdirect?	
	9102/tcp	open	jetdirect?	
	9103/tcp	open	jetdirect?	
	21/tcp	open	ftp	

192.168.20.37	23/tcp	open	telnet	impresora
	80/tcp	open	http	
	280/tcp	open	http	
	443/tcp	open	ssl/https?	
	515/tcp	open	printer	
	631/tcp	open	http	
	7627/tcp	open	ssl/soap-http?	
	9100/tcp	open	jetdirect?	
192.168.20.42	135/tcp	open	msrpc	computador
	139/tcp	open	netbios-ssn	
	445/tcp	open	microsoft-ds	
	554/tcp	open	rtsp?	
	2869/tcp	open	http	
	5800/tcp	open	http-proxy	
	5900/tcp	open	vnc	
	10243/tcp	open	http	
	49158/tcp	open	msrpc	
192.168.20.44	21/tcp	open	ftp	impresora
	23/tcp	open	telnet	
	80/tcp	open	http	
	280/tcp	open	http	
	443/tcp	open	ssl/https?	
	515/tcp	open	printer	
	631/tcp	open	http	
	7627/tcp	open	ssl/soap-http?	
	9100/tcp	open	jetdirect?	
192.168.20.76	135/tcp	open	msrpc	computador
	139/tcp	open	netbios-ssn	
	445/tcp	open	microsoft-ds	
	2869/tcp	open	http	
	2968/tcp	open	enpp?	
	5357/tcp	open	http	
	6543/tcp	open	mythtv?	
	49157/tcp	open	msrpc	
	21/tcp	open	ftp	
	23/tcp	open	telnet	

192.168.20.77	80/tcp	open	http	impresora
	280/tcp	open	http	
	443/tcp	open	ssl/https?	
	515/tcp	open	printer	
	631/tcp	open	http	
	7627/tcp	open	ssl/soap-http?	
	9100/tcp	open	jetdirect?	
192.168.20.100	135/tcp	open	msrpc	computador
	139/tcp	open	netbios-ssn	
	445/tcp	open	microsoft-ds	
	5357/tcp	open	http	
	5800/tcp	open	http-proxy	
	5900/tcp	open	vnc	
	49155/tcp	open	msrpc	
192.168.20.127	21/tcp	open	ftp	impresora
	23/tcp	open	telnet	
	80/tcp	open	http	
	280/tcp	open	http	
	443/tcp	open	ssl/https?	
	515/tcp	open	printer	
	631/tcp	open	http	
	7627/tcp	open	ssl/soap-http?	
	9100/tcp	open	jetdirect?	

Puertos en estado *open* que se encuentran presentes en la IP escaneadas con clasificación de riesgo Alto con el servicio prestado.

Nro Puerto	Protocolo	servicio	Nro Puerto	Protocolo	servicio
21	tcp	ftp	6543	tcp	mythtv?
23	tcp	telnet	7070	tcp	ssl/realserver?
80	tcp	http	9090	tcp	soap
135	tcp	msrpc	9100	tcp	jetdirect?
139	tcp	netbios-ssn	9101	tcp	jetdirect?

280	tcp	http	9102	tcp	jetdirect?
515	tcp	printer	9103	tcp	jetdirect?
554	tcp	rtsp?	10243	tcp	http
631	tcp	http	49152	tcp	msrpc
1110	tcp	nfsd-status	49153	tcp	msrpc
1801	tcp	msmq?	49154	tcp	msrpc
2103	tcp	msrpc	49155	tcp	msrpc
2105	tcp	msrpc	49156	tcp	msrpc
2107	tcp	msrpc	49157	tcp	msrpc
2869	tcp	http	49158	tcp	msrpc
5357	tcp	http	49159	tcp	msrpc
5432	tcp	postgresql	49160	tcp	msrpc

Las posibles vulnerabilidades que se pueden explotar por los servicios en estado *open* descritos anteriormente se describen a continuación basados en el **CVE (Common Vulnerabilities and Exposures)** que lo reporta como vulnerable.

Nro	Servicio	Definición	Vulnerabilidad Por estar en estado *open*	Nro CVE	IP Expuesta/Puerto
1	ftp	protocolo de transferencia de archivos	La función plupload_action del archivo /wp-content/plugins/updraftplus/admin.php es afectada por esta vulnerabilidad. A través de la manipulación del parámetro name como parte de Parameter se causa una vulnerabilidad de clase escalada de privilegios. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-16871	192.168.20.12 21/tcp 192.168.20.13 21/tcp 192.168.20.28 21/tcp 192.168.20.30 21/tcp 192.168.20.31 21/tcp 192.168.20.3721/tcp 192.168.20.4421/tcp 192.168.20.7721/tcp 192.168.20.127 21/tcp
2	telnet	Protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.	Una función desconocida del componente Telnet Service es afectada por esta vulnerabilidad. Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-15376	192.168.20.3723/tcp 192.168.20.4123/tcp 192.168.20.4423/tcp 192.168.20.7723/tcp 192.168.20.127 23/tcp

3	msrpc	Es una tecnología propietaria de Microsoft para desarrollar componentes de software distribuidos sobre varias computadoras y que se comunican entre sí.	Una función desconocida del componente Flow Daemon es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase denegación de servicio. Esto tiene repercusión sobre la la disponibilidad.	CVE-2013-4688	192.168.20.9 135/tcp 192.168.20.9 49152/tcp 192.168.20.9 49153/tcp 192.168.20.9 49154/tcp 192.168.20.9 49159/tcp 192.168.20.9 49160/tcp 192.168.20.9 49161/tcp 192.168.20.10 135/tcp 192.168.20.10 49152/tcp 192.168.20.10 49153/tcp 192.168.20.10 49154/tcp 192.168.20.10 49155/tcp 192.168.20.10 49156/tcp 192.168.20.10 49157/tcp 192.168.20.29 135/tcp 192.168.20.29 2103/tcp 192.168.20.29 2105/tcp 192.168.20.29 2107/tcp 192.168.20.42 135/tcp 192.168.20.42 49158/tcp 192.168.20.76 135/tcp 192.168.20.76 49157/tcp 192.168.20.100 135/tcp 192.168.20.100 49155/tcp
4	netbios-ssn	Servicios de red sobre capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.	Una función desconocida del componente Windows NetBT Session Services es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-0161	192.168.20.9 139/tcp 192.168.20.10 139/tcp 192.168.20.12 139/tcp 192.168.20.13 139/tcp 192.168.20.28 139/tcp 192.168.20.29 139/tcp 192.168.20.30 139/tcp 192.168.20.31 139/tcp 192.168.20.42 139/tcp 192.168.20.76 139/tcp 192.168.20.100 139/tcp

5	http	Protocolo de comunicación que permite las transferencias de información en la World Wide Web.	Una función desconocida del archivo net/xfrm/xfrm_user.c del componente XFRM Dump Policy es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-16939	192.168.20.9 5357/tcp 192.168.20.12 631/tcp 192.168.20.13 631/tcp 192.168.20.28 631/tcp 192.168.20.30 631/tcp 192.168.20.31 631/tcp 192.168.20.37 280/tcp 192.168.20.37 631/tcp 192.168.20.42 2869/tcp 192.168.20.42 10243/tcp 192.168.20.44 280/tcp 192.168.20.44 631/tcp 192.168.20.76 2869/tcp 192.168.20.76 5357/tcp 192.168.20.77 280/tcp 192.168.20.77 631/tcp 192.168.20.100 5357/tcp 192.168.20.127 280/tcp 192.168.20.127 631/tcp
6	printer	Servicio de impresión que usa una secuencia de comandos de PCL proviene del driver de la impresora y éstos son necesarios para realizar una cierta impresión	La función printDirect en la biblioteca lib/printer.js es afectada por esta vulnerabilidad. Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2014-3741	192.168.20.12 515/tcp 192.168.20.13 515/tcp 192.168.20.28 515/tcp 192.168.20.30 515/tcp 192.168.20.31 515/tcp 192.168.20.37 515/tcp 192.168.20.44 515/tcp 192.168.20.77 515/tcp 192.168.20.127 515/tcp

7	rtsp	Protocolo de transmisión en tiempo real (del inglés Real Time Streaming Protocol) establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de video. El RTSP actúa como un	Una función desconocida del componente URL Handler es afectada por esta vulnerabilidad. Mediante la manipulación con el valor del input rtsp://admin@yourip:554/h264_hd.sdp se causa una vulnerabilidad de clase autenticación débil. Esto tiene repercusión sobre la la confidencialidad.	CVE-2017-10796	192.168.20.42 554/tcp
		mando a distancia mediante la red para servidores multimedia.			
8	nfsd-status	servicio de Linux Kernel	Una función desconocida del archivo fs/nfsd/nfs3xdr.c del componente NFSv2/NFSv3 es afectada por esta vulnerabilidad. Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-7895	192.168.20.10 1110/tcp

9	msmq	Servicio (Microsoft Message Queuing o MSMQ) es una implementación de cola de mensajes desarrollada por Microsoft e implementada en sus sistemas operativos Windows Server desde Windows NT 4 y Windows 95. Windows Server 2016 y Windows 10 también incluye este componente. Además de su compatibilidad con la plataforma de servidor	Una función desconocida del componente Message Queuing Service es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase designfehler. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2009-1922	192.168.20.29 1801/tcp
		convencional, MSMQ se ha incorporado a las plataformas Microsoft Embedded desde 1999 y al lanzamiento de Windows CE			

10	msrpc	Servicio de Llamada a procedimiento remoto de Microsoft. (Microsoft RPC)	Una función desconocida del componente FlowDaemon es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase denegación de servicio. Esto tiene repercusión sobre la la disponibilidad.	CVE-2013-4688	192.168.20.9 135/tcp 192.168.20.9 49152/tcp 192.168.20.9 49153/tcp 192.168.20.9 49154/tcp 192.168.20.9 49159/tcp 192.168.20.9 49160/tcp 192.168.20.9 49161/tcp 192.168.20.10 135/tcp 192.168.20.10 49152/tcp 192.168.20.10 49153/tcp 192.168.20.10 49154/tcp 192.168.20.10 49155/tcp 192.168.20.10 49156/tcp 192.168.20.10 49157/tcp 192.168.20.29 135/tcp 192.168.20.29 2103/tcp 192.168.20.29 2105/tcp 192.168.20.29 2107/tcp 192.168.20.42 135/tcp 192.168.20.42 49158/tcp 192.168.20.76 135/tcp 192.168.20.76 49157/tcp 192.168.20.100 135/tcp 192.168.20.100 49155/tcp
11	postgresql	Servicio de gestión de bases de datos relacionales de objetos (ORDBMS) con énfasis en la extensibilidad y el cumplimiento de estándares.	La función jsonb_populate_recordset/jsonb_populate_recordset es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios. Esto tiene repercusión sobre la confidencialidad y disponibilidad.	CVE-2017-15098	192.168.20.9 5432/tcp

12	vnc	Servicio gráfico de uso compartido de escritorio que utiliza el protocolo de Frame Buffer Remoto (RFB) para controlar remotamente otra computadora. Transmite los eventos de teclado y mouse de una computadora a otra, retransmitiendo las actualizaciones de la pantalla gráfica en la otra dirección, a través de una red.	Una función desconocida del archivo hw/display/cirrus_vga.c del componente Cirrus CLGD 54xx VGA Emulator es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-7980	192.168.20.10 5800/tcp 192.168.20.10 5900/tcp 192.168.20.42 5900/tcp 192.168.20.100 5900/tcp
13	mythtv	MythTV es una aplicación de entretenimiento, Convierte una computadora con el hardware necesario en un grabador de video digital de transmisión en red	La función sendtomythtv del archivo mythcontrolserver.c es afectada por esta vulnerabilidad. Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2006-6860	192.168.20.76 6543/tcp
14	ssl/realserver	servicio usado para la reproducción y transmisión de audio de la empresa RealNetworks	Una función desconocida del componente Request Handler es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase denegación de servicio. Esto tiene repercusión sobre la la disponibilidad.	CVE-2004-0389	192.168.20.9 7070/tcp

15	soap	SOAP (Simple Object Access Protocol) es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.	Mediante la manipulación de un input del componente XML Document Handler se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.	CVE-2017-9765	192.168.20.12 9090/tcp 192.168.20.13 9090/tcp 192.168.20.28 9090/tcp 192.168.20.31 9090/tcp
16	jetdirect	Servicio de servidor de impresión	Una función desconocida del componente Web Administration Interface es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase directory traversal. Esto tiene repercusión sobre la la confidencialidad.	CVE-2008-4419	192.168.20.12 9100/tcp 192.168.20.12 9101/tcp 192.168.20.12 9102/tcp 192.168.20.12 9103/tcp 192.168.20.13 9100/tcp 192.168.20.13 9101/tcp 192.168.20.13 9102/tcp 192.168.20.13 9103/tcp 192.168.20.28 9100/tcp 192.168.20.28 9101/tcp 192.168.20.28 9102/tcp 192.168.20.28 9103/tcp 192.168.20.30 9100/tcp 192.168.20.30 9101/tcp 192.168.20.30 9102/tcp 192.168.20.31 9100/tcp 192.168.20.31 9101/tcp 192.168.20.31 9102/tcp 192.168.20.31 9103/tcp 192.168.20.37 9100/tcp 192.168.20.44 9100/tcp 192.168.20.77 9100/tcp 192.168.20.127 9100/tcp

10.8.3 Prueba denominada: Revisión de privacidad en el dominio web www.contraloriasantander.gov.co

Herramienta Usada:

Vega: Plataforma de prueba y escáner de código abierto para probar la seguridad de las aplicaciones web. Trabaja con soporte para encontrar y validar Inyección SQL, Cross-Site Scripting (XSS), divulgación de información confidencial inadvertidamente y otras vulnerabilidades. Está escrito en Java, basado en GUI, y se ejecuta en Linux, OS X y Windows.

Resultados:

La herramienta VEGA maneja módulos de detección bajo 4 conceptos:

- High (según nuestra clasificación de la tabla 2 sería el equivalente a Alto)
- Medium (según nuestra clasificación de la tabla 2 sería el equivalente a Medio)
- Low (según nuestra clasificación de la tabla 2 sería el equivalente a Bajo)
- Info (si clasificar en nuestro informe pero de muy poca relevancia).

Para este análisis de toman los riesgos clasificados con High (alto) y Medium (medio) debido a la relevancia e importancia de las vulnerabilidades encontradas.

El resultado fue el siguiente:

Numero de vulnerabilidad : 1
Clasificación del Riesgo: `Alto`
Nombre de la Vulnerabilidad: `"ShellShock" Injection`

Recursos Afectados:
 	
`/http:/contraloriasantander.gov.co/wp-login.php`
 	
`/publicaciones/informe-ambiental/()%20{%20:%3B}%3B%20/bin/sleep%2031`
 	
`/wp-admin`
 	
`/wp-content/()%20{%20:%3B}%3B%20/bin/sleep%2031`

Descripción: El problema se debe a una vulnerabilidad en el shell Bash. Esta vulnerabilidad puede manifestarse remotamente en aplicaciones web si la entrada suministrada por el usuario se pasa al entorno de shell Bash, lo que puede ocurrir si los valores de encabezado o parámetro se convierten en variables de entorno local. Si se explota con éxito, esta vulnerabilidad puede llevar a la ejecución del comando en el host subyacente.
Impacto:
Posible vulnerabilidad de inyección de comandos. Los atacantes pueden ejecutar comandos en el servidor. La explotación puede conducir a un acceso remoto no autorizado.
Reporte CVE (Common Vulnerabilities and Exposures) que soporta la Vulnerabilidad: CVE-2014-6271 CVE-2014-6278 CVE-2014-7169
Numero de vulnerabilidad : 2
Clasificación del Riesgo: Alto
Nombre de la Vulnerabilidad: Session Cookie Without HttpOnly Flag
Recurso Afectado: / "la raíz completa"
Descripción: Se ha detectado que una cookie de sesión puede haberse configurado sin el indicador HttpOnly. Cuando este indicador no está presente, es posible acceder a la cookie a través del código de script del lado del cliente. El indicador HttpOnly es una medida de seguridad que puede ayudar a mitigar el riesgo de ataques de secuencias de comandos entre sitios que se dirigen a las cookies de sesión de la víctima. Si se establece el indicador HttpOnly y el navegador admite esta función, el código de script proporcionado por el atacante no podrá acceder a la cookie.
Impacto: Acceso a una cookie que puede repercutir en diferentes acciones a favor de un atacante
Numero de vulnerabilidad : 3
Clasificación del Riesgo: Alto
Nombre de la Vulnerabilidad: Session Cookie Without Secure Flag
Recurso Afectado: /wp-admin
Descripción: Se ha detectado que una cookie de sesión conocida puede haber sido configurada sin el indicador de seguridad.
Impacto: Las cookies pueden exponerse a los espías de la red. Las cookies de sesión son credenciales de autenticación; los atacantes que los obtienen pueden obtener acceso no autorizado a las aplicaciones web afectadas.
Numero de vulnerabilidad : 4
Clasificación del Riesgo: Alto

Nombre de la Vulnerabilidad: Shell Injection
Recursos Afectados: /http:/contraloriasantander.gov.co/wp-login.php /inicio-de-sesion/ /wp-admin/
Descripción: Las vulnerabilidades de inyección de comandos a menudo ocurren cuando los datos suministrados externamente no son adecuadamente saneados como parte de un
comando del sistema ejecutado a través de un intérprete de comandos o shell. Vulnerabilidades como estas pueden explotarse utilizando metacaracteres del intérprete de comandos para ejecutar comandos adicionales que no estaban destinados a ser ejecutados por el desarrollador de la aplicación. La función del sistema () y los derivados son a menudo responsables, ya que estas funciones son muy simples de usar. Estas vulnerabilidades pueden otorgar acceso remoto a los atacantes, si se explotan con éxito.
Impacto: Posible vulnerabilidad de inyección de comandos. Los atacantes pueden ejecutar comandos en el servidor. La explotación puede conducir a un acceso remoto no autorizado.
Numero de vulnerabilidad : 5
Clasificación del Riesgo: Alto
Nombre de la Vulnerabilidad: SQL Injection
Descripción: Se ha detectado una posible ruta absoluta del sistema de archivos (es decir, una que no está relacionada con la raíz web). Esta información es confidencial, ya que puede revelar cosas sobre el entorno del servidor a un atacante. Conocer el diseño del sistema de archivos puede aumentar las posibilidades de éxito de los ataques a ciegas. Las rutas completas del sistema se encuentran a menudo en la salida de error. Esta salida nunca se debe enviar a clientes en sistemas de producción. Se debe redirigir a otro canal de salida (como un registro de errores) para que lo analicen los desarrolladores y los administradores del sistema.
Impacto: La divulgación de estas rutas revela información sobre el diseño del sistema de archivos. Esta información puede ser delicada, su divulgación puede aumentar las posibilidades de éxito para otros ataques.
Numero de vulnerabilidad : 7
Clasificación del Riesgo: Medio
Nombre de la Vulnerabilidad: Possible XML Injection

Recurso Afectado: /http:/contraloriasantander.gov.co/wp-login.php Parámetro: rememberme /wp-admin/admin.php?page=vega>'>"><vega></vega> Parámetro: method /wp-login.php?redirect_to=http://contraloriasantander.gov.co/wp-admin/admin.php%3Fpage=wpfd%200%200%20-%20-&reauth=vega>'>"><vega></vega> Parámetro: reauth /wp-login.php?redirect_to=vega>'>"><vega></vega>&action=wpfd&task=file.download&wpfd_category_id=348&wpfd_file_id=7544&token=623dd279dd5ced3f4224edcc969da4be&preview=1&reauth=1 Parámetro: redirect_to
Descripción: Se ha detectado una posible vulnerabilidad de inyección XML. La inyección de XML puede ocurrir cuando se utilizan datos suministrados externamente que no se han validado lo suficiente para crear un documento XML. Es posible que estos datos corrompan la estructura de los documentos. Las posibles consecuencias dependen del documento XML y para qué se utiliza.
Impacto: Esto podría afectar la lógica de la aplicación, dependiendo de cómo se use el documento XML. Una vulnerabilidad de inyección XML puede conducir a una pérdida de integridad de los datos utilizados o almacenados por la aplicación. XML puede ser un vector de inyección que omite los filtros de contenido (por ejemplo, incluye javascript en una sección CDATA).

10.8.4 Prueba denominada: Búsqueda y Verificación de Vulnerabilidades sobre sistemas operativos

Herramienta Usada:

OpenVas - Conjunto de herramientas para explotar las vulnerabilidades disponibles en los puertos y direcciones encontradas por las herramientas anteriores.

Bajo esta plataforma se utiliza toda la salida recopilada y se selecciona las vulnerabilidades en la base de datos para poder explotar cada uno de los puertos y servicios que se detectaron abiertos con rutinas y plugins que se tienen ya definidos por la aplicación.

Resultados:

Con la herramienta OpenVas se obtuvo un escaneo de los equipos para identificar vulnerabilidades en sus sistemas operativos, arrojando un resultado de 7 direcciones IP con 9 riesgos de alta de explotación en su sistema operativo o kernel así:

192.168.20.7
192.168.20.9
192.168.20.15
192.168.20.32
192.168.20.59
192.168.20.65
192.168.20.79

A continuación se muestran los resultados obtenidos con la vulnerabilidad identificada:

Vulnerabilidad en sistema operativo Nro. 1
IP afectada: 192.168.20.7 192.168.20.9 192.168.20.15 192.168.20.32 192.168.20.65 192.168.20.79
Severidad : 7.5% - Alto
Vulnerabilidad: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
Descripción: Los host ejecutan SMB / NETBIOS y es propenso a la vulnerabilidad de omisión de autenticación
Impacto: La explotación exitosa podría permitir a los atacantes usar acciones para hacer que el sistema se bloquee. Nivel de impacto: sistema
Reporte CVE (Common Vulnerabilities and Exposures) que soporta la Vulnerabilidad: CVE-1999-0519
Vulnerabilidad en sistema operativo Nro. 2
IP afectada:

192.168.20.15 192.168.20.39 192.168.20.52
Severidad : 9.3% - Alto
Vulnerabilidad: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
Descripción: Estos host no cuentan con una actualización de seguridad crítica de acuerdo con el boletín de Microsoft MS17-010.
Impacto: La explotación exitosa permitirá a los atacantes remotos obtener la capacidad de ejecutar código en el servidor de destino, también podría llevar a la divulgación de información del servidor. Nivel de impacto: sistema
Reporte CVE (Common Vulnerabilities and Exposures) que soporta la Vulnerabilidad: CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148

10.8.5 Prueba denominada: Enrutamiento

Herramienta Usada:

- OpenVas

Resultados:

La herramienta nos permitió encontrar la siguiente vulnerabilidad (1) sobre el dispositivo que enruta el tráfico en la entidad así:

Vulnerabilidad de Router : 8
Clasificación del Riesgo: Alto
Nombre de la Vulnerabilidad: MikroTik RouterOS WPA2 Key Reinstallation Vulnerabilities - KRACK
Severidad o Riesgo: 8.3% (Alto) Host : 192.168.20.1
Descripción: El dispositivo MikroTik RouterOS usa WPA2 y esta propenso a múltiples debilidades de seguridad, también conocidos como Ataques de Reinstalación de Claves (KRACK).

Impacto: La explotación de estos problemas puede permitir que un usuario no autorizado

intercepte y manipule datos o divulgue información sensible. Esto puede ayudar en futuros ataques
Reporte CVE (Common Vulnerabilities and Exposures) que soporta la Vulnerabilidad: CVE-2017-13077 CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081 CVE-2017-13082 CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088

Tabla 10. Vulnerabilidad dispositivo de Enrutamiento de la Entidad

10.8.6 Prueba denominada: Testeo de Control de Acceso

Actividad Realizada:

- Chequeo de configuración Mínima

Resultados:

Actualmente la red cableada de la entidad cuenta con identificación punto a punto. Es decir existe numeración en el lugar de trabajo y en el Switch, labor que ayuda a solventar situaciones a la hora de presentarse problemas.

Existe un adecuado control de acceso físico a las instalaciones en cuanto a lo que respecta a la conexión cableada de un dispositivo ajeno a la entidad.

Se evidencia la existencia de una Routerboard mikrotik. Esta recibe la fibra y la distribuye a otra mikrotik de 5 puertos. así mismo cuenta con dos switch administrables marca cisco. Se desconoce si actualmente están siendo administrados. El personal actual no conoce dicha información.

Se evidencio la utilización de Switch 5 puertos marca Tplink. Esto debido a la instalación de dispositivos o periféricos compartidos en la red, tales como impresoras y escáneres.

La entidad actualmente usa el direccionamiento IP de manera dinámica a través de un servicio DCHP en el dispositivo de enrutamiento tanto para la red cableada como para la red inalámbrica, debido a que la mayoría de equipos son portátiles y estos son los usados por los funcionarios para realizar las auditorias en los diferentes municipios del departamento.

La red inalámbrica o Wifi cuenta con hotspot (zonas de alta demanda de tráfico) para el acceso al servicio por parte de los funcionarios. Actualmente se cuenta con la creación de 40 usuarios en el dispositivo; de estos usuarios se tiene destinado el uso de 30 únicamente para funcionarios y los 10 restantes para visitantes. En este momento al intentar conectar se debe probar todas las posibles contraseñas y usuarios para poder realizar la conexión debido a que estas están de manera compartida por algunos de los funcionarios y personal adscrito a la entidad.
Esto sucede debido a que la contraloría general de Santander no cuenta con un SSID para el uso propio de funcionarios y personal.

10.8.7 Prueba denominada: Verificación de Redes Inalámbricas [802.11]

Herramienta Usada:

- Zenmap

Resultados:

Se ejecutó el comando **#nmap -T4 -A -v 192.168.88.0/24**

- -T4 : Temporizador nivel 4
- -A : Habilitar tracerooute y detección de Sistema operativo
- -v : Nivel de salida (los datos que se proporcionan de resultado) Se

identifican las siguientes IP en la red inalámbrica

192.168.88.1
192.168.88.2
192.168.88.3
192.168.88.6
192.168.88.13
192.168.88.14

192.168.88.16

Se realiza el análisis de puertos a las maquinas descubiertas en la red inalámbrica con riesgo alto clasificado en el numeral 2.2.3 del presente informe para identificar las posibles vulnerabilidades y servicios disponibles en cada una.

Los estados de los puertos encontrados en estado *open* (abierto) significan que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto.

A continuación se muestran las IP que se encontraron con puertos en estado *open*:

Dirección IP	Puerto	Estado	Servicio	tipo de Dispositivo
192.168.88.1	23/tcp	open	tcpwrapped	router
	53/tcp	open	tcpwrapped	
	80/tcp	open	tcpwrapped	
	443/tcp	open	tcpwrapped	
	1987/tcp	open	tcpwrapped	
	2000/tcp	open	tcpwrapped	
	64872/tcp	open	tcpwrapped	
	64873/tcp	open	tcpwrapped	
	64874/tcp	open	tcpwrapped	
	64875/tcp	open	tcpwrapped	
192.168.88.2	5357/tcp	open	tcpwrapped	teléfono
192.168.88.3	135/tcp	open	tcpwrapped	no identificado
	139/tcp	open	tcpwrapped	
	445/tcp	open	tcpwrapped	
	554/tcp	open	tcpwrapped	
	1688/tcp	open	tcpwrapped	
	2869/tcp	open	tcpwrapped	
	10243/tcp	open	tcpwrapped	
	17500/tcp	open	tcpwrapped	
	49152/tcp	open	tcpwrapped	
	49153/tcp	open	tcpwrapped	
	49154/tcp	open	tcpwrapped	
	49156/tcp	open	tcpwrapped	
	49160/tcp	open	tcpwrapped	
	49161/tcp	open	tcpwrapped	

	49162/tcp	open	tcpwrapped	
192.168.88.6	135/tcp 139/tcp 445/tcp 554/tcp 10243/tcp 17500/tcp 49155/tcp 49156/tcp	open open open open open open open open	tcpwrapped tcpwrapped tcpwrapped tcpwrapped tcpwrapped tcpwrapped tcpwrapped tcpwrapped	no identificado
192.168.88.13	135/tcp 139/tcp	open open	tcpwrapped tcpwrapped	no identificado

	445/tcp	open	tcpwrapped	
	1110/tcp	open	tcpwrapped	
	1688/tcp	open	tcpwrapped	
	17500/tcp	open	tcpwrapped	
	49152/tcp	open	tcpwrapped	
	49153/tcp	open	tcpwrapped	
	49154/tcp	open	tcpwrapped	
	49156/tcp	open	tcpwrapped	
	49157/tcp	open	tcpwrapped	
	49158/tcp	open	tcpwrapped	
192.168.88.14	135/tcp	open	tcpwrapped	teléfono
	139/tcp	open	tcpwrapped	
	445/tcp	open	tcpwrapped	
	2968/tcp	open	tcpwrapped	
	49668/tcp	open	tcpwrapped	
192.168.88.16	135/tcp	open	tcpwrapped	teléfono
	139/tcp	open	tcpwrapped	
	445/tcp	open	tcpwrapped	
	5357/tcp	open	tcpwrapped	
	6646/tcp	open	tcpwrapped	
	49667/tcp	open	tcpwrapped	

Puertos en estado *open* que se encuentran presentes en la IP escaneadas con clasificación de riesgo Alto con el servicio prestado.

Nro Puerto	Protocolo	servicio	Nro Puerto	Protocolo	servicio
23	tcp	Tcp wrapped	17500	tcp	Tcp wrapped
53	tcp	Tcp wrapped	49152	tcp	Tcp wrapped
80	tcp	Tcp wrapped	49153	tcp	Tcp wrapped
135	tcp	Tcp wrapped	49154	tcp	Tcp wrapped
139	tcp	Tcp wrapped	49155	tcp	Tcp wrapped
443	tcp	Tcp wrapped	49156	tcp	Tcp wrapped
445	tcp	Tcp wrapped	49157	tcp	Tcp wrapped
554	tcp	Tcp wrapped	49158	tcp	Tcp wrapped

1110	tcp	Tcp wrapped	49160	tcp	Tcp wrapped
1688	tcp	Tcp wrapped	49161	tcp	Tcp wrapped
1987	tcp	Tcp wrapped	49162	tcp	Tcp wrapped
2000	tcp	Tcp wrapped	49667	tcp	Tcp wrapped
2869	tcp	Tcp wrapped	49668	tcp	Tcp wrapped
2968	tcp	Tcp wrapped	64872	tcp	Tcp wrapped
5357	tcp	Tcp wrapped	64873	tcp	Tcp wrapped
6646	tcp	Tcp wrapped	64874	tcp	Tcp wrapped
10243	tcp	Tcp wrapped	64875	tcp	Tcp wrapped

Las posibles vulnerabilidades que se pueden explotar por los servicios en estado *open* descritos anteriormente se describen a continuación basados en el **CVE (Common Vulnerabilities and Exposures)** que lo reporta como vulnerable.

Nro	Servicio	Definición	Vulnerabilidad Por estar en estado *open*	Nro CVE	IP Expuesta
1	Tcp wrapped	es un sistema de red ACL que trabaja en terminales y que se usa para filtrar el acceso de red a servicios de protocolos de Internet que corren en sistemas operativos	Una función desconocida del componente TCP Timestamp Handler es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase designfehler. Esto tiene repercusión sobre la la disponibilidad.	CVE-2005-0356	192.168.88.1 192.168.88.2 192.168.88.3 192.168.88.6 192.168.88.13 192.168.88.14 192.168.88.16

Tabla 12. Vulnerabilidades expuestas por IP inalámbricas bajo el criterio CVE (Common Vulnerabilities and Exposures)

NOTA ACLARATORIA: Como este servicio se presenta en los dispositivos móviles y al red inalámbrica es compartida para funcionarios y visitantes. No se realizara ninguna observación que conlleve a la mitigación de esta vulnerabilidad pues se realiza otra recomendación de segmentación de red nombrada en el numeral 11.2 del presente documento que soluciona la vulnerabilidad actual de tener dispositivos de visitantes en la red de los funcionarios.

Nota. El reporte completo del resultado arrojado por la herramienta Zenmap para la red inalámbrica se adjunta en el CD anexo a este informe.

10.8.8 Prueba denominada: Verificación de Dispositivos de Entrada Inalámbricos

Actividad Ejecutada:

- Verificación con Inspección Ocular

Resultados:

En el trabajo de campo realizado en la entidad se puedo evidenciar el uso de algunos dispositivos inalámbricos como mouse y teclados.

Las instalaciones en el área de auditores están retiradas de oficinas y acceso público. Lo que dificulta la posibilidad de conexión.

Con el uso de estos dispositivos de entrada inalámbricos se presenta la vulnerabilidad clasificada como riesgo medio, que podría ser aprovechada para que el atacante descargase malware en el computador de la víctima y a partir de ahí tomar control de ese equipo. Varios de los fabricantes aseguran tener ya un parche para el problema mientras que otras como Lenovo admiten que tendrán que reemplazar este tipo de soluciones porque no ofrecen actualizaciones para dichos periféricos.

10.8.9 Prueba denominada: Revisión de Privacidad de dispositivos inalámbricos

Actividad Ejecutada:

- Revisión de configuración existente

Resultados:

Como la entidad cuenta con un hotspot para brindar acceso tanto a funcionarios como visitantes, se tiene la mala práctica de permitir que sean usados dispositivos personales tales como portátiles, miniportátiles, Smartphone y tablets para actividades relacionadas con el trabajo. Por lo tanto el resultado dado por el alto riesgo que existe al permitir este tipo de prácticas que atentan directamente contra la privacidad de todos los dispositivos que se encuentren conectados a la red ; es por esto que en la sección 4.2 del presente documento se hace la respectiva recomendación para que se segmente la red de manera que no se

continúe con esta configuración que afecta la disponibilidad, integridad y confidencialidad de la información que viaja pro al red inalámbrica.

10.8.10 Prueba denominada: Evaluación de Controles de Acceso físico

Actividad ejecutada:

- Chequeo visual

Resultados:

La entidad cuenta con los controles físicos brindados por la gobernación de Santander debido a su ubicación dentro del edificio público.
Al ingreso toda persona que ingrese debe registrarse, al igual que el destino al cual se dirige y los dispositivos tecnológicos con los que ingresa.

La contraloría general de Santander, no cuenta con ningún control de acceso físico a sus instalaciones y/o a sus Centrales de información (Rack, dispositivos de red, archivo).

Se observó que no se cuenta con un sitio de almacenamiento documental que brinde seguridad de acceso y trazabilidad.

10.8.11 Prueba Adicional - Encuesta de Percepción para Funcionarios (Valor Agregado)

A continuación se muestran los resultados por cada pregunta junto con su análisis de la respuesta recibida por parte de los funcionarios.

Nro. pregunta	Indicador de Desconocimiento del Riesgo
Pregunta 1 ¿Los Smartphone y tabletas no se infectan con virus?	29.03%
Pregunta 2 Recibes este correo de tu banco en el que te solicita confirmar tus datos personales y bancarios de manera urgente, supuestamente por motivos de seguridad	22.58%

Pregunta 3 ¿Qué protocolo de seguridad debe tener configurado el Router WiFi de tu casa?	54.88%
Pregunta 4 ¿Crees que son seguras las siguientes contraseñas?	16.12%
Pregunta 5 Un virus informático es capaz de borrar las fotos almacenadas en un ordenador	19.35%
Pregunta 6 ¿Es necesario que compruebes los ficheros que descargas a través de redes P2P?	12.90%
Pregunta 7 En Internet, cuando hablamos de cookies, ¿a qué nos referimos?	19.35%
Pregunta 8 ¿Qué debes hacer si Windows te muestra una ventana diciéndote que hay actualizaciones pendientes de instalar en el equipo?	80.64%
Pregunta 9 ¿Qué debes hacer si la policía "bloquea" tu ordenador por haber accedido a contenidos ilegales de Internet y te pide 100€ para solucionarlo?	12.90%
Pregunta 10 ¿Sabes que es un hacker?	35.48%
Pregunta 11 ¿Estás informado acerca de las prevenciones que hay que tener para evitar el acceso de un hacker u otra amenaza a tu computador o portátil?	74.19%
Pregunta 12 ¿Qué prevenciones toma en el momento de darle seguridad a tu computador o portátil?	3.22%
Pregunta 13 ¿Qué amenazas informáticas conoces?	0.00%
Pregunta 14 ¿Sabes lo que debes hacer en caso de la entrada de una amenaza a tu equipo?	77.41%
Pregunta 15 ¿Conoces algún caso de hackeo a algún equipo o página web?	54.88%
Pregunta 16 ¿Qué redes ocupa generalmente para conectarse a internet desde su computador o portátil?	41.93%
Promedio indicador	
34.67%	

Este porcentaje obtenido indica que el existe un **34.67%** de probabilidad en incurrir en prácticas que pueden vulnerar la seguridad de la entidad.

El indicador es bajo lo que significa que existe un 66% de conocimiento ante situaciones que impliquen seguridad de la información.

Los detalles de cada pregunta se encuentran en el informe técnico que hace parte integral de las pruebas de efectividad.

10.9 PRUEBAS NO SATISFACTORIAS

Es importante aclarar que las pruebas realizadas abarcaron las capas de aplicación, sistema operativo, web y red. En la siguiente tabla se presentan las pruebas realizadas por el consultor, concerniente a lo identificado las cuales no fueron satisfactorias y su descripción.

Categoría	Nombre de la prueba	Observaciones
Pruebas de Efectividad	Testeo de Aplicaciones de Internet	La entidad no cuenta con aplicaciones propias en internet para servicios a usuarios internos y externos por lo tanto la prueba no se pudo ejecutar
	Testeo de Sistema de Detección de Intrusos	La entidad no cuenta con un sistemas detección de intrusos por lo tanto la prueba no se pudo ejecutar

4. PLANEACIÓN DE TI

Objetivo Estratégico de TI	**Optimizar la Planificación Estratégica de TI en la Contraloría General de Santander**				
Dominio	**Planeación Estratégica**		**Indicadores**		
Metas	**Productos**	**Actividades**	**Formula**	**Fecha de Inicio**	**Fecha Final**
Realizar seguimiento al Plan Estratégico de TI en la entidad	Plan Estratégico de TI PETI	Actualización del PETI: a. El portafolio o mapa de ruta de los proyectos b. La proyección del presupuesto, d. El plan de comunicaciones del PETI	% de seguimiento del plan estratégico de TI	Enero 2022	Diciembre 2022
Objetivo Estratégico de TI	**Implementar esquemas de gobernabilidad de TI dentro de la Contraloría General de Santander**				
Dominio	**Gobierno de TI**		**Indicadores**		
Metas	**Productos**	**Actividades**	**Formula**	**Fecha de Inicio**	**Fecha Final**
Formular el proceso de Gestión Tecnológica en la entidad	Proceso de Contratación utilizando las diferentes plataformas que propone Colombia Compra Eficiente para este proceso	Utilizando las directrices de Colombia Compra eficiente viabilizar la adquisición de productos y servicios tecnológicos	% de formulación Gestión Tecnológica de la Entidad	Marzo de 2022	Noviembre de 2022
	Proceso de TI dentro de la entidad.	Incluir dentro del Sistema de Gestión de Calidad la entidad el proceso de TI			
	Metodología para transferencia de tecnología de proveedores hacia la entidad	Continuar un proceso de transferencia de tecnología de otras entidades o apoyo del sector privado hacia la Contraloría de Santander, para la apropiación de TIC			

Objetivo Estratégico de TI	**Optimizar las capacidades para el uso estratégico de la información dentro de la Contraloría General de Santander**				
Dominio	**Información**		**Indicadores**		
Metas	**Productos**	**Actividades**	**Formula**	**Fecha de Inicio**	**Fecha Final**
Formular Componente de Planeación y Gestión de Información en la Entidad	Documentación de Planeación y Gestión de Información	a Indice de información clasificada y reservada b Esquema de Publicación c. Registro de Activos de Información.	% de formulación Gestión Componente de Gestión de Información de la Entidad	Julio de 2022	Diciembre de 2022
	Formular un estándar de calidad de los componentes de información	Generar indicadores para medir el flujo de información en la entidad			
Objetivo Estratégico de TI	**Optimizar las capacidades para el uso estratégico de la información dentro de la Contraloría General de Santander**				
Dominio	**Sistemas de Información**		**Indicadores**		
Metas	**Productos**	**Actividades**	**Formula**	**Fecha de Inicio**	**Fecha Final**
Realizar políticas de trazabilidad de la información en la entidad	Catálogo de sistemas de información	Formular Catálogo de sistemas de información	% de realización de las políticas de trazabilidad de la información	Febrero de 2022	Diciembre de 2022
Objetivo Estratégico de TI	**Optimizar las capacidades para el uso estratégico de la información dentro de la Contraloría General de Santander**				
Dominio	**Servicios Tecnológicos**		**Indicadores**		
Metas	**Productos**	**Actividades**	**Formula**	**Fecha de Inicio**	**Fecha Final**

Aumentar la disponibilidad de los recursos tecnológicos	Ampliación de la capacidad de los recursos tecnológicos	Realizar la proyección de la capacidad de los recursos tecnológicos. Realizar adquisición e instalación de los recursos tecnológicos requeridos. Poner en funcionamiento la infraestructura tecnológica requerida.	% de Disponibilidad de los recursos tecnológicos de la entidad	Enero de 2022	Diciembre de 2022
Objetivo Estratégico de TI	Definir la estrategia para apoyar el uso y apropiación de las TIC en la entidad				
Dominio	Uso y apropiación		**Indicadores**		
Metas	**Productos**	**Actividades**	**Formula**	**Fecha de Inicio**	**Fecha Final**
Definir prácticas concretas para el uso y apropiación de las TIC en la entidad	Plan de uso y apropiación de TIC en la entidad.	Definir estrategia de uso y apropiación en el Plan de Capacitaciones de la Entidad. Ejecutar actividades de uso y apropiación en la entidad.	% de ejecución de las prácticas concretas de uso y apropiación en TIC en la entidad	Febrero de 2022	Diciembre de 2022

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Metas	Productos	Actividades	Formula	Fecha de Inicio	Fecha Final
Definir Políticas de Seguridad y Privacidad de la Información en la entidad	Documento de Políticas de Seguridad y Privacidad de la Información en la entidad.	Formular Políticas de Seguridad de la Información. Definir acto administrativo de adopción de las políticas. Socialización de dichas políticas con los funcionarios de la entidad.	% de formulación del Políticas de Seguridad de la Información	Febrero de 2022	Diciembre de 2022
Formalizar el área de TI en la Contraloría General de Santander	Acto administrativo o documento de actualización de mapa de procesos de la entidad.	Crear proceso de TI en la entidad. Definir el acto administrativo o documento de formalización del proceso. Socialización de dicho proceso con los funcionarios de la entidad.	% de formalización de proceso de TI en la entidad	Febrero de 2023	Diciembre de 2023

Ejecutar la mitigación de riesgos de seguridad y privacidad de la información.	Ejecución Plan de Riesgos de Seguridad y privacidad de la Información	Actualizar el plan de Riesgos de Seguridad y Privacidad de la Información. Ejecutar Plan de Riesgos SPI	% de Ejecución del Plan de Riesgos de Seguridad y Privacidad de la Información.	Enero de 2022	Diciembre de 2022
Definir Lineamientos Técnicos para la protección de la información en la entidad.	Actualización de la página web de la entidad	Minimizar las vulnerabilidades de la página web de la entidad.	% de actualización de la página web de la entidad	Marzo de 2022	Octubre de 2022
Definir Lineamientos Técnicos para la protección de la información en la entidad.	Adquisición de Software antivirus	Minimizar las pérdidas de información por software antivirus de la entidad.	% de actualización de la página web de la entidad	Febrero de 2022	Octubre de 2022

FREDY ANTONIO ANAYA MARTINEZ
Contralor General de Santander

Proyectó: Carlos Alberto Mendoza Saad – Profesional EspecializadoG-03