INFORME AUDITORIA INTERNA

SEGURIDAD DE LA INFORMACIÓN

PROCESO AUDITADO:	**OFICINA DE PLANEACIÓN Y SISTEMAS**
LÍDER DEL PROCESO AUDITADO:	Dr. JUAN JOSÉ GÓMEZ VÉLEZ
LÍDER DE LA AUDITORÍA:	**Dra. LEYDY LUCÍA LARGO ALVARADO**
OBJETIVO DE LA AUDITORIA:	Conocer el nivel de exposición a un ataque externo e Identificar posibles vulnerabilidades de los sistemas de seguridad informática y de la información.
ALCANCE LA AUDITORIA:	Página web, planes y programas, mapas de riesgos, políticas internas y procesos y procedimientos.
EQUIPO AUDITOR:	Alvaro E. Ospina R. – Profesional Universitario Ricardo Alonso Torres Ramos – Contratista Blanca Cecilia Bardales Infante - Contratista Diego Sebastián Moreno Cruz - Contratista Wilson Estiven Gómez Rodríguez – Contratista Samir Alfredo Sebastián Corredor Espinoza – Contratista
FECHA DE INICIO:	06 DE OCTUBRE DE 2021
FECHA DE TERMINACIÓN:	16 DE DICIEMBRE DE 2021

I. INTRODUCCIÓN

La presente auditoria se adelantó en cumplimiento de las funciones legales de la Oficina Coordinadora del Control Interno más concretamente en cumplimiento del Programa Anual de Auditorías Internas – PAAI - 2021, la Ley 87 de 1993.

La auditoría de seguridad de caja negra tiene como finalidad conocer el nivel de exposición a un ataque externo a través de un test de intrusión. En el mismo sentido, esta auditoría se complementó con la revisión de diferentes actores que hacen parte de la seguridad e integridad de la información, tales como Planes y Programas, mapas de riesgos, políticas de seguridad, auditorías internas y externas anteriores.

II. METODOLOGÍA

La metodología utilizada en el proceso de esta auditoría se basa en la revisión documental, análisis de información, pruebas y consulta a través de los sistemas de información, así:

- Realización de test de intrusión con el software Nessus, programa de escaneo de vulnerabilidades.
- Revisión de auditorías internas y externas realizadas.
- Revisión de Mapas de Riesgos en seguridad informática y de la información.
- Revisión de Métricas de seguridad.
- Revisión de Proceso y Procedimientos.
- Revisión de Políticas de seguridad informática.
- Revisión de planes y programas.

III. RECURSOS

- Página web.
- Correo electrónico.
- Oficios de Requerimientos.
- Aplicaciones software libre – Nessus.
- Windows 10 32 Bits.
- Portátil Core i 5 8ª Generación.
- Guías de Seguridad y Privacidad de la Información – MINTIC.
- Meet de google.

IV. MARCO NORMATIVO

Ley 87 de 1993 *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"*
Ley 715 de 2001 *"Plan Nacional de Tecnologías de la Información y las Comunicaciones".*
Ley 790 de 2002, Artículo 14, *establece la obligatoriedad del gobierna nacional de promocionar el gobierna electrónico.*
Ley 1341 2009, *Promueve el acceso y usa de las TIC a través de su masificación, garantiza la libre competencia, el usa eficiente de la infraestructura y el espectro.*
Ley 1273 de 2009, *Por media de la cual se modifica el código penal, se crea un nueva bien jurídica tutelada - denominada "de la protección de la información y de las datas"*
Ley 1341 de 2009, *Par la cual se definen principias y conceptas sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones.*
Decreto 4485 de 2009, *"Par medio de la cual se adopto la actualización de la Norma Técnica de Calidad en la Gestión Pública."*
Decreto 235 de 2010, *"Por el cual se regula el intercambia de información entre entidades para el cumplimiento de funciones públicas."*
Ley 1581 de 2012, *Por la cual se dictan disposiciones generales para la protección de datos personoles.*
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."*
Decreto 1078 de 2015, *"Por medio del cual se expide el decreto única reglamentario del sector de tecnologías de la información y las comunicaciones."*
Resolución 3564 de 2015 Mintic, *"Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública."*
Ley 1955 de 2019, *"Corresponde al Plan Nacional de Desarrollo 2018- 2022 establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) artículos 147,148 y 230 ".*
Decreto 2106 de 2019, *"Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva."*
CONPES 3975 de 2019, *"Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital."*
Decreto 620 de 2020, *"Se establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, de acuerdo a las directrices que establezca el Ministerio de Tecnologías de la Información busca direccionar la relación entre la ciudadanía y la administración pública."*

Norma NTC-ISO 27001:2013. *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información.*

V. EJECUCIÓN

1. Realización de test de intrusión

Esta oficina realizó un test de intrusión a la página web de la entidad *"la dirección IP 23.96.32.104 https://www.camara.gov.co/"* con el aplicativo Nessus, finalizado el test de intrusión se obtuvieron los siguientes resultados:

1.1. Verificación del código de error 404 del servidor web (*El escaneo CGI se desactivará para este host porque el host responde a solicitudes de URL inexistentes con código HTTP 302 en lugar de 404.*).

Observación 1

El servidor web remoto está configurado de manera que no devuelve códigos de error '404 No encontrado' cuando se solicita un archivo inexistente, quizás devolviendo en su lugar un mapa del sitio, una página de búsqueda o una página de autenticación.

Si se produce una gran cantidad de agujeros de seguridad para este puerto, es posible que no todos sean precisos.

Recomendación

Crear la página de error 404 para la navegación.

1.2. Escáner Nessus SYN (*Se encontró que el puerto 22, 80 y 433 / tcp estaban abiertos*)

Observación 2

Este complemento es un escáner de puerto SYN 'medio abierto'. Deberá ser razonablemente rápido incluso contra un objetivo con cortafuegos.

Tenga en cuenta que los escaneos SYN son menos intrusivos que los escaneos TCP (conexión completa) contra servicios rotos, pero pueden causar problemas para firewalls menos robustos y también dejar conexiones sin cerrar en el destino remoto, si la red está cargada.

Recomendación

Que se proteja su objetivo con un filtro de IP.

1.3. Cifrados del modo CBC del servidor SSH habilitados

Observación 3

El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.

Recomendación

Deshabilitar el cifrado del modo de cifrado CBC y hobilitar el cifrado del modo de cifrado CTR o GCM.

1.4. Detección de protocolo TLS versión 1.0 y 1.1

Observación 4

TLS 1.0. TLS 1.0 tiene uno serie de defectos de diseño criptográfico, TLS 1.1 carece de soporte para los conjuntos de cifrados recomendados y actuales.

La habilitoción de estos protocolos no funcionorá correctomente con los principales navegadores web octuales y los principoles proveedores.

Recomendación

Habilite lo compotibilidad con TLS 1.2 y 1.3 y desoctive la compatibilidad con TLS 1.1 yTLS 1.1.

1.5. Compatibilidad con conjuntos de cifrado de intensidad media SSL.

Observación 5

El host remoto odmite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera lo potencia media como cuolquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES.

Tenga en cuenta que es considerablemente más fácil eludir el cifrado de nivel medio si el otocante se encuentra en lo mismo red físico.

Recomendación

Que se reconfigure lo oplicoción ofectodo si es posible pora evitar el uso de cifrados de fuerzo media.

1.6. No se puede confiar en el certificado SSL (*El siguiente certificado fue parte de la cadeno de certificados enviado por el host remoto, pero ha caducodo*).

Observación 6

- Primero, la porte superior de lo cadena de certificodos enviados por el servidor podría no ser descendiente de una autoridad de certificación público conocido. Esto puede ocurrir cuando la porte superior de la codena es un certificado autofirmodo no reconocido o cuondo falton certificados intermedios que conectarían la porte superior de la cadena de certificados con uno outoridad de certificación pública conocido.

- En segundo lugar, lo codena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el esconeo ocurre antes de una de las fechas 'notBefore' del certificodo, o después de uno de las fechos 'notAfter' del certificodo.

- En tercer lugar, la codena de certificados puede contener una firma que no coincide con la información del certificado o que no se puede verificar. Las firmos incorrectas se pueden solucionar hociendo que el emisor vuelva a firmar el

certificada con la firma incorrecta. Las firmas que no se pudieron verificar son el resultada de que el emisor del certificado utiliza un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier ruptura en la cadena dificulta que las usuarios verifiquen la autenticidad y la identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.

Recomendación

Que se adquiera a genere un certificado SSL adecuado pora este servicio.

1.7. Certificado SSL autofirmado (*El certificado que se encontró en la parte superior del certificado cadena enviada por el host remoto, pera está autofirmado y no se encuentran en la lista de autoridades de certificación conocidas*).

Observación 7

La cadena de certificados X.509 para este servicio no está firmado por una autoridad certificadora reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un otaque de intermediario contra el host remoto.

Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, pero está firmodo por una autoridad de certificación no reconocida.

Recomendación

Que se adquiera o genere un certificado SSL adecuado para este servicio.

2. Auditorias anteriores.

2.1. Auditorías Internas

En la revisión de auditorías anteriores se observó que no se abordaron temas relacionados con la seguridad de la información y las vulnerabilidades de los sistemas de información.

2.2. Auditorías Externas

En el 2015 se encontró un hallazgo por parte de la CGR relacionado con la Seguridad de la Información así, *"H6 Seguridad información. No se evidencia un plan de contingencia paro garantizar la continuidad de los servicios ante determinadas situaciones imprevistas o que alteren el normal funcionamiento del centro de cómputo. No se ho diseñado acciones que garanticen la custodia y restauración de la información en el momento que se requiera acceder a la dato"*, el cual fue subsanado y cerrado en la vigencia 2016.

En la auditoria adelantada por CGR a las vigencias 2018 y 2019 emite el siguiente hallazgo, *"H10-2018y2019 Seguridad de la Información (D) - Pérdida de Información de la Data: Seven y Kactus, afectando el praceso contable de PPE, Nómina y Personal y del Sistema de Gestión Documental ControlDoc. Así mismo, pérdida y disponibilidad de los servicios de telefonía, intranet, servidor de dominio. En resumen, se vio afectada lo mayoría de lo información de los aplicaciones de la CR. "*, La causa descrita por la CGR fue *"Carencia y debilidades en la aplicación de las controles, de acuerdo a las mejores prácticas expuestas en la Norma NTC-ISO 27001:2013.*

Ausencia de una solución de Backup que incluya todos los componentes de las sistemas: aplicaciones, data, servicios, entre otros y respaldo de la información fuera de las instalaciones del Datacenter." La entidad suscribe tres (3) acciones de mejora *"(1) Realizar capacitaciones al interior de la Entidad, sabre las políticas y procedimientos del Modelo de Seguridad de la Información. (2) Realizar y configurar las copias de seguridad semanalmente con su correspondiente registro en la Bitácora por aplicación. (3) Llevar registro de los Backup realizados en una Bitácora por aplicación.".* La Oficina Coordinadora del Control interno en cumplimiento a sus obligaciones cierra el 06 de diciembre de 2021 las acciones anteriores y reporta el cierre a la CGR.

3. Mapas de Riesgos.

Observación 8

Revisado los mapas riesgos se observó que no encuentran actualizados los riesgos relacionados con la seguridad informática y de la información. En reunión con las ingenieros Alvaro Carreña y Alejandro Muñoz, contratistas de la Oficina de Planeación y Sistemas confirman que los mapas de riesgos deben ser actualizados a la realidad actual de la entidad; esta oficina preguntó por el profesional responsable de esta trabajo, a lo cual responden que el profesional especializado que venía adelantando esta labor culminó su contrata. Que la falta de personal especializado de apoyo no ha permitido dar continuidad al proceso y debido a las múltiples actividades solo se cuenta para apoyar los dos ingenieros mencionados que son insuficientes.

La no actualización de los mapas de riesgos conlleva a que se materialicen nuevos riesgos, afectando la continuidad y seguridad de los activas de información de la entidad.

Recomendación

Que se dé continuidad al proceso de actualización de los riesgos mencionados con profesionales especializadas en materia de seguridad informática y de la información.

4. Métricas de Seguridad

Observación 9

La entidad no cuenta con métricas de seguridad. Las métricas permiten determinar si los procesos de seguridad implementadas cumplen con las políticas de seguridad adoptadas por la entidad, en el misma sentido, permiten identificar nuevos riesgos, puntos débiles y obtener información que permita la toma decisiones en los niveles estratégicos, técnicas y operativas de entidad.

Recomendación

Que se implementen métricas de seguridad con el fin llevar un monitoreo de las diferentes directrices establecidas en las Políticas de seguridad adoptadas por la entidad.

5. Proceso y Procedimientos

Observación 10

Revisada la página web se observa que en materia de seguridad informática y de la información se encuentra documentado y publicado el procedimiento de "GENERACIÓN DE COPIAS DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN – v1 del 2019", en el mismo sentido, no se encuentran procedimientos relacionados con la Seguridad de la información como son los de Recurso Humano (Capacitación y Sensibilización del Personal, Ingreso y Desvinculación del Personal), Gestión de Activos (Identificación y Clasificación de Activos) Control de Acceso y Procedimiento de Gestión de Incidentes de Seguridad de La Información entre otros.

La falta de procedimientos conlleva a la falta interpretación, errores y deficiencias en la ejecución de actividades o tareas, causanda posibles fallas de seguridad.

Recomendación

Que se definan e implementen los pracedimientos necesarias relacionados con la Seguridad informática y de la información en la Entidad, de conformidad con la norma ISO/IEC 27001.

6. Políticas de Seguridad

Observación 11

La entidad tiene implementado el "MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION DE LA CÁMARA DE REPRESENTANTES V2.0, JULIO DE 2020", documento que contiene los lineamientas y políticas administrativas que hacen parte de la seguridad de la información y que deben cumplir los funcionarios, contratistas y visitantes a terceros que tengan acceso a los servicios tecnológicos que les provea la entidad paro usa institucional. El manual de políticas de seguridad no cuenta con políticas para uso de dispositivos móviles, políticas de controles criptográficas y las políticas de seguridad de los recursos humanos entre otras.

De acuerdo a la bitácora de revisión y/o actualización, este documento no cuenta con una revisión o actualización reciente. La falto de actualización puede llevar a prácticas deficientes y fallas en la seguridad de los activos de información.

Recomendación

Que se actualicen las políticas de seguridad a la realidad actual de la entidad, teniendo en cuenta los lineamientos establecidos en la norma ISO/IEC 27001.

7. **Planes y Programas.**

Observación 12

La entidad actualmente se encuentra en proceso de implementación del Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI, dentro de los proyectos contenidos en este plan se encuentra el "Proyecto 29: Implementación de un Sistema de Gestión en Seguridad de la Información SGSI". Este proyecto se encuentra proceso de ser actualizado y aprobado por el Comité Institucional de Gestión y Desempeño, toda vez que revisado por los profesionales del área, estos encontraron unos errores que fueron corregidos.

La falta de implementación del SGSI expone a amenazas los activos de información de la entidad, aunque existan algunos herramientas implementadas podrían no ser suficientes para garantizar la seguridad y continuidad de los sistemas de información.

Recomendación

Se recomienda que se dé inicia la más pronto posible a la Implementación de un Sistema de Gestión en Seguridad de la Información SGSI con el fin de resguardar de manero más efectiva y organizada los activas de información de la entidad.

VI. CONCLUSIÓNES

La norma ISO/IEC 27000 define *"Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales."* Del mismo modo la ISO/IEC 27001 lo define; *"Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de lo información de una organización y lograr sus objetivos camerciales y/o de servicio."* El SGSI tiene como propósito principal preservar la protección de todos los activos de información de la entidad a través de la implementación de los distintos componentes que la conforman. Es así la oficina Coordinadora del Control Interno recomienda que se adelanten las acciones necesarias para implementar de manera inmediata el *"Sistema de Gestión en Seguridad de la Información SGSI"*, con el fin de brindar mayor seguridad a los activos de información frente a las diferentes amenazas.

En el mismo sentido, mientras se aprueba la actualización e implementa este proyecto, la entidad debe dar continuidad a los procesos que se venían actualizando como es el de los mapas de riesgos, capacitaciones en materia de seguridad de la información.

Cordialmente,

DRA. LEYDY LUCÍA LARGO ALVARADO
Coordinadora
Oficina Coordinadora del Control Interno

ING. ALVARO ERNESTO OSPINA RAMÍREZ
Profesional Universitario

ING. RICARDO ALONSO TORRES RAMOS
Contratista

Proyecto: Ing. Alvaro E. Ospina R. – Profesional Universitario