REFERENCIA	NOMBRE DE AUDITORIA	FECHA DE REALIZACIÓN		FECHA DEL INFORME
		INICIO	CIERRE	
A-P-GTI-01	Gestión de Tecnología de la Información	18/04/2016	28/06/2016	22/08/16

PROCESO /AREA AUDITADA	AUDITOR LIDER / AUDITOR
Tecnologías de Información	Milton Aristobulo Lopez
EQUIPO DE AUDITORES	**AUDITORES ACOMPAÑANTES**
--	--

1. CRITERIOS:

1.1 CALIDAD
No aplica
1.2 CONTROL INTERNO
Normatividad: - Decreto 1083 de 2015 (Función Pública) ARTÍCULO 2.2.21.5.2 LIBRO 2, PARTE 2, titulo 21, capitulo 5 - Decreto 3816 (Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública). - Decreto 2573 Lineamientos generales de la estrategia de gobierno en línea. - Ley 527 de 1999. Uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. - Ley 1712 de 2014 se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. - Políticas, Procedimientos, Planes de Mejora, Informes de Auditorias Anteriores, ISO 2700:20131, ITIL, COBIT. - CONPES 3854 del 11 de Abril de 2016 y 3292 del 28 de Junio de 2004.

2. OBJETIVOS:

2.1 CALIDAD
No aplica

2.2 CONTROL INTERNO
Evaluar el ambiente de control del proceso de Gestión de Tecnologías de Información, tomando como referencia los requerimientos mínimos de MECI, Políticas, Procedimientos de la Agencia, marco legal, normas internacionales como ISO 27001:2013, Marcos de referencia como ITIL y COBIT. Esto con el fin de mantener o mejorar los controles para minimizar los riesgos por la falta de confidencialidad, integridad y disponibilidad de la información.

3. ALCANCE:

En el presente informe, se presenta el diagnóstico de control realizado al proceso de Gestión de Tecnologías de Información de la Agencia, con el fin de Identificar Riesgos asociados a los Controles Generales implementados.

CONTROLES GENERALES EVALUADOS

TECNOLOGIAS DE INFORMACION – CONTROLES DE SEGURIDAD EN LAS OPERACIONES

- Políticas y Procedimientos
    - Sistema de Gestión de Servicios T.I; Registro de Solicitudes e Incidentes
    - Directorio Activo; Base de Datos del Dominio, presta servicios de Autenticación, Seguridad y Control de Objetos
    - Bases de datos y sistemas operativos
    - *System Center Configuration Manager*

- *Firewall*
- *VPN*
- Antivirus.
- Seguridad física de los centros de cómputo.

- POA - Indicadores de operación y/o Gestión

  - Proyectos de Tecnología 2016 (*IP* v4- *IP* v6).
  - Proyecto Seguridad de la Información

- Plan de continuidad

- Mapa de Riesgos

APLICACIONES DE INDUSTRIA - CONTROLES DEL MODULO DE ACCESO

Administración de usuarios y roles de los sistemas de información de Industria:

- SIIF - Sistema Integrado de Información Financiera
- SARA WEB – Nómina

En el alcance no se incluyó:

- ORFEO - Sistema de Gestión Documental (Esta aplicación se evaluará en la Auditoría al proceso de GESTIÓN DOCUMENTAL, que se iniciará el 11 de Julio de 2016).

- SIGI - Sistema Integrado de Gestión Institucional (Esta aplicación se evaluará en la Auditoría al proceso de GESTIÓN DOCUMENTAL, que se iniciará el 11 de Julio de 2016).

- eKOGUI - Sistema Litigioso del Estado (Esta aplicación se evaluará en la Auditoría al proceso de GESTIÓN DEL SISTEMA ÚNICO DE INFORMACIÓN LITIGIOSA DEL ESTADO, que se iniciará el 1 de Septiembre de 2016).

- Portal www.eKOGUI.gov.co - Sistema Litigioso del Estado - (Esta aplicación se evaluará en la Auditoría al proceso de GESTIÓN DEL SISTEMA ÚNICO DE INFORMACIÓN LITIGIOSA DEL ESTADO, que se iniciará el 1 de Septiembre de 2016).

4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

No hubo.

5. DOCUMENTOS EXAMINADOS:

Documentos publicados y consultados para la Auditoría:

- Caracterización del proceso de Gestión de Tecnologías de la Información
- Seis (6) formatos asociados al proceso.
- uno (1) guía asociada al proceso.
- Dos (2) políticas asociadas al proceso.
- Matriz de riesgos del proceso de Gestión De Tecnologías De La Información del aplicativo Sistema Integrado de Gestión Institucional (SIGI).
- POA

Documentos enviados a través de correo por el líder del proceso y evaluados para la Auditoría:

- Sistema de Gestión de Servicios T.I

  - Borrador Procedimiento para solicitud de servicios de TI
  - Portafolio de servicios de TI.doc (Borrador)
  - Perfiles_SoporteTIC_ServiciosTI.pdf

- ANS (No hay)

- Gestión de cambios
  - Procedimiento Gestión de Cambios.docx (Borrador)
- Nuevo desarrollo
  - Procedimiento para solicitud de servicios de ORFEO (Borrador)
- Solicitud y entrega de equipos
  - ACTA DE ENTREGA DE EQUIPO DE CÓMPUTOv2.docx –
  - Borrador Procedimiento para solicitud de servicios de TI V2.docx (Pendiente de Publicación SIGI)
- Asignación de licencias a usuarios
  - Guía de Control de Licencias.doc (Borrador)
- Monitoreo de eventos del sistema
  - Sistema de Monitoreo de Infraestructura IT -Eventos Infraestructura.pdf (Borrador)
- Administración y revisión de *logs*
  - *Event_Security_serverBD.evtx*
- Administración y revisión de antivirus
  - Política de protección contra código malicioso – SIGI
- Remediación de vulnerabilidades y actualización de parches
  - Instructivo para la distribución de actualizaciones – WSUS
- Ambientes de Desarrollo – Pruebas y Producción
  - Consultada en http//calidad.defensajuridica.gov.co/archivos/DE-M-02/DE-M-02- v-2 -Manual de políticas Institucionales y de Desarrollo Administrativo Ítem 6.4.11.
- Administración de Centros de Datos
  - Borrador Instructivo de Control de accesos a centro de datos
- Administración de usuarios y roles especiales
  - Borrador Política Administración por Sistema Operativo.docx
- Administración de copias de seguridad (*Backups*)
  - Guía de gestión de respaldo y restauración de copias de seguridad.docx (Borrador)
  - Política de *backup* http://calidad.defensajuridica.gov.co/archivos/DE-M-02/DE-M-02- v-2 -Manual de políticas Institucionales y de Desarrollo Administrativo.pdf
  - Soporte de *backups* realizados.xlsx
  - Entrega Cintas 2015.pdf
- Gestión de usuarios
  - Borrador Procedimiento para solicitud de servicios de TI V2.docx- Formato para solicitud de servicios de TI.docx - Grupos de internet creados.txt

- Guía para la estandarización de cuentas de usuario.doc
- Listado de usuarios del directorio Activo.
- Políticas de contraseñas aplicadas en el D.A

- Gestión de Políticas en el *F.W.*

  - Listado de políticas o reglas aplicadas actualmente en el *firewall*.txt

- Gestión Infraestructura de Comunicaciones

  - Manual de herramienta de monitoreo de infraestructura tecnológica
  - Inventario de infraestructura comunicaciones

- Gestión de *VPN Client to Site*

  - Listado de usuarios que utilizan VPN Client to Site.txt - Listado de VPN activas site to site.txt.

- Mapa de riesgos

  - Publicado en SIGI

- Plan de Continuidad

  - DRP estrategia DC; Estrategia DRP Directorio Activo (Documento de julio de 2015)
  - DRP estrategia eKOGUI; Estrategia 1 DRP Plataforma eKOGUI – Recuperación a partir de los servidores replicados en la ANDJE (Documento de julio de 2015)
  - DRP estrategia eKOGUI *Netvault*; Estrategia 1 DRP Plataforma – Recuperación a partir de los *BackUp* Alojados En *Dell-Netvault* (ANDJE) (Documento de julio de 2015)
  - DRP estrategia eKOGUI Replicación; Estrategia 1 DRP Plataforma eKOGUI – Recuperación a partir de los servidores replicados en la ANDJE (Documento de julio de 2015)
  - Pruebas DRP_Estrategia_1_eKOGUI_Replicación; estrategia 1 DRP plataforma eKOGUI recuperación a partir de los servidores replicados en la ANDJE (Documento de julio de 2015)
  - Estrategia DRP comunicaciones unificadas *Lync server*
  - Estrategia 1 DRP plataforma ORFEO
  - Estrategia 1 DRP portal web www.defensajuridica.gov.co

- Indicadores de operación y/o Gestión – POA

  - POA 04-SG-16 Desarrollar requerimientos para fortalecer el Sistema de Gestión Documental ORFEO: Desarrollar los 5 requerimientos más demandados por la entidad. Corte a Mayo el 20% - Junio el 40%
  - POA 07-SG-16 Realizar informes trimestrales de implementación del Plan y Estrategia de Transición de IPv4 a IPv6. (Realizar informes trimestrales de avance en la implementación del plan y la estrategia de transición de IPv4 a IPv6. Informe en Marzo). Se valida informe de Marzo en carpeta 07-SG-16 del mes de marzo.
  - 04-DGI-1-2-16 Soporte y Mantenimiento de la versión en operación eKOGUI: Se valida cumplimiento de cumplimiento del 85% de incidencias reportadas. Se validó, Se validan \\Srvstorage\ANDJE\Planeacion\Carpeta OAP\Soportes Indicadores POA y PAA 2016\Indicadores POA y PAA DGI 2016

- Aplicaciones de industria

  - SARA WEB. De acuerdo con la validación realizada, se observó que parámetros del módulo no se encuentran activos ejemplo: claves_letras, claves_números, número_intentos, clave_longitud, clave repetir, clave_cambiooobligatorio, configuración de ruta de LOG (ver soporte en papeles de trabajo)
  - Para la aplicación SIIF, se apoyó en el la evaluación realizada y cuyo soporte se encuentra en el informe de referencia GF SIC-CIC-02-03 de fecha de cierre 06/05/2016

6. PLAN DE MUESTREO

N/A

7. RESUMEN DEL INFORME:

7.1 Elementos de la Norma de Calidad	Numeral de la Norma	Número de no Conformidades
No Aplica		
Total de no conformidades	No aplica	No aplica

7.2 Normas de Control Interno	Criterio	Número de Hallazgos
No hubo hallazgos		
Total de hallazgos	**----------**	**0**

8. INFORME

8.1 FORTALEZAS

El desarrollo de la Auditoría permitió identificar que existen controles generales al proceso de Gestión de Tecnologías de Información que a la fecha han minimizado la materialización de riesgos tecnológicos.

Cumplimiento de los compromisos adquiridos en el POA, al corte de la Auditoría, y que aunque existe un plan de continuidad para los procesos misionales, también está contemplado un plan de continuidad para todos los procesos de la ANDJE en Plan estratégico de tecnología 2017 – 2020.

Con el fin de implementar controles adicionales y minimizar los riesgos referentes a la norma ISO 27002 y a Decreto 1083 de 2015 Artículo 2.2.21.5.2 Libro 2, Parte 2, Titulo 21, Capitulo 5, el líder del proceso estableció un plan de compromisos de entrega de Documentos y guías de T.I. referentes a controles de seguridad en las operaciones.

8.2 CUMPLIMIENTO DE PRINCIPIOS

Los Criterios tomados como marco de referencia, para la evaluación de Controles Generales de Tecnología, corresponden a los establecidos por COBIT 5.

CRITERIOS DE INFORMACIÓN COBIT 5

- Eficacia. Con base en la Auditoría realizada se observó que la Agencia cuenta con aplicaciones donde se almacena la información que soporta las actividades para cada proceso. A la fecha del informe se estaban adelantando requerimientos para que la información generada por las aplicaciones satisficiera las necesidades de los usuarios.

- Eficiencia. Se observó que el proceso de Gestión de Tecnologías de Información estaba adelantando planes de trabajo con el fin de definir Procedimientos, Guías y Políticas para ofrecer un mejor servicio a los usuarios y en guiarlos en la solicitud y obtención de herramientas o soluciones para el uso de la información como un servicio (Si la información que satisface las necesidades de los usuarios se obtiene y utiliza de una manera fácil «es decir consume pocos recursos, esfuerzo físico, esfuerzo cognitivo, tiempo y dinero» es eficiente).

- Integridad. Durante el período evaluado no se observaron inconsistencias en la integridad de la información (entendida la integridad como completitud y precisión).

- Disponibilidad. Se observó que el proceso de Gestión de Tecnologías de Información contaba con planes para el respaldo de la información y para mantenerla disponible a los usuarios de los servicios misionales de la Agencia. Dentro del Plan estratégico de Tecnologías de Información 2017-2020 se incluyen actividades para garantizar en un 100% la disponibilidad de la información.

- Confidencialidad: Se observó que el proceso de Gestión de Tecnologías de Información estaba adelantando planes y proyectos para clasificar y asegurar el acceso a la información sólo por los usuarios autorizados.

8.3 CONTENIDO

De acuerdo con el plan de Auditoría para el año 2016, se realizó la evaluación de los Controles Generales al proceso de Gestión de Tecnologías de Información.

La evaluación fue realizada según el alcance definido y de acuerdo con el siguiente con el siguiente sistema de valoración:

	Control Satisfactorio	Cuando se cumplen con las disposiciones establecidas en el marco regulatorio y procedimental, se considera que los controles son apropiados.
	Control Aceptable	Cuando las deficiencias encontradas en el control no son de impacto grave y de fácil solución. Hasta el momento no han impactado en los principios de la Agencia.
	Control Deficiente	Cuando ahí violación de Principios de Legalidad, de control y procedimientos. Afecta los principios de la Agencia.

1 CONTROLES DE SEGURIDAD EN LAS OPERACIONES

1.1 Políticas y Procedimientos

1.1.1 Gestión de Servicios T.I

Observación – Riesgo

Aunque la Agencia Nacional de Defensa Jurídica del Estado a la fecha de la auditoría contaba con procedimiento para solicitud de servicios T.I, portafolio, catálogo de servicios de tecnología y contaba con un canal de comunicación a través del cual los usuarios puedan solicitar y recibir servicios estándar con una aprobación previa "Sistema de Gestión de Servicios de T.I.". Estos procedimientos no están oficializados ni publicados lo cual puede generar falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información.

Recomendación

Proporcionar procedimientos o guías para oficiales para que los usuarios puedan:

- Diferenciar la Gestión de Incidencias de la Gestión de Requerimientos.
- Proporcionar información a los usuarios y clientes sobre la disponibilidad de los servicios y el procedimiento para obtenerlos.
- Establecer Acuerdos de Niveles de Servicio (ANS) con los clientes o usuarios.

Con lo anterior se logra:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio acordados en los ANS.
- Mayor control de los procesos y monitorización del servicio:
    - Optimización de los recursos disponibles.
    - Número total de solicitudes de servicio.
    - Tiempo medio que dura la gestión de cada tipo de solicitud de servicio.
    - Número y porcentaje de solicitudes de servicio completadas en los tiempos acordados (ANS).
    - Coste medio de cada tipo de solicitud de servicio.
    - Nivel de satisfacción del cliente con la gestión de las solicitudes de servicio.
- Mejora la satisfacción general de clientes y usuarios.

1.1.2 Gestión de Cambios

Observación – Riesgo

El proceso de Gestión de Tecnologías de Información elaboró un procedimiento "Borrador" para la Gestión. Este procedimiento no está oficializado ni publicado lo cual puede generar falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información.

Los sistemas de gestión de la información son muy susceptibles a los cambios de configuración por las sofisticadas interrelaciones entre todos los elementos de configuración involucrados. Un cambio aparentemente menor puede provocar una reacción en cadena con resultados catastróficos que afecte la operación normal de la Agencia.

El control inadecuado de los cambios en las instalaciones y sistemas de procesamiento de la información es una causa común de fallas en el sistema o en la seguridad. Los cambios en el entorno operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la operacional puede tener impacto sobre la confiabilidad de las aplicaciones

Recomendación

Todo procedimiento o guía de operación debe ser oficial con el fin de que todo cambio sea autorizado por el responsable de la información.

En particular, se deberían considerar los siguientes asuntos:

- Identificación y registro de cambios significativos
- Planificar la puesta a prueba de los cambios
- Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información
- Procedimiento de aprobación formal para los cambios propuestos
- Verificar de que se han cumplido los requisitos de seguridad de la información
- Comunicación de todos los detalles de los cambios a todas las personas pertinentes;
- Procedimientos de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos
- Suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente urgente que esté afectando la operación.
- Responsabilidades y procedimientos de gestión formales para asegurar el control satisfactorio de todos los cambios. Cuando se hacen los cambios, se debería conservar un registro de auditoría que contenga toda la información pertinente.

1.1.3 Nuevos Desarrollos

Observación – Riesgo

En el proceso de Gestión de Tecnologías de Información de la Agencia Nacional de Defensa Jurídica del Estado se administran los requerimientos o nuevos desarrollos del Proceso de gestión documental "ORFEO". Estos se solicitan a través de requerimientos y cuentan con un formato de solicitud, el cual no se encuentra oficializado ni publicado. No se observaron reglas para el desarrollo de software.

Lo anterior puede ocasionar impacto en el ambiente operacional o programación no segura tanto para los nuevos desarrollos como para escenarios de reúso de códigos.

Recomendación

Los procedimientos o actividades de operación tecnológica se deben documentar y poner a disposición de todos los usuarios que los necesiten, ya que estos permiten generar directrices para administrar y asegurar las correctas operaciones de los procesos tecnológicos.

Es importante establecer reglas donde se incluyan pruebas de software en un ambiente separado tanto de los ambientes de producción como de desarrollo por parte de los usuarios, esto permite tener control sobre el software nuevo y tener protección adicional de la información operacional que se usa para propósitos de pruebas.

Para el caso de ORFEO, donde el desarrollo es contratado, se deberían considerar:

- Los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
- Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
- Pruebas de aceptación para determinar la calidad y exactitud de los entregables.
- Soportes de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- Documentación del desarrollo para crear entregables.

1.1.4 Solicitud Y Entrega De Equipos 

Observación – Riesgo

El Manual de políticas institucionales cuenta con políticas para la ubicación y protección de los equipos, seguridad de los equipos fuera de las instalaciones, reutilización y/o eliminación de equipos y retiro de estos, igualmente cuentan con las actas de entrega.

1.1.5 Asignación de Licencias a Usuarios 

Observación – Riesgo

Para la administración de licenciamiento se basan en la guía de control de licencias de software. Esta guía no está oficializada ni publicada. Es necesario oficializar estos instrumentos de administración con el fin de minimizar riesgos en falta de aseguramiento en el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

Recomendación

Se debe implementar procedimientos y/o guías apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados, para lo anterior es importante tener en cuenta dentro de la guía a aprobar:

- Adquirir software sólo a través de fuentes conocidas y confiables para asegurar que no se violan los derechos de autor.
- Mantener los registros de activos apropiados e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.
- Llevar a cabo revisiones acerca de que solo hay instalados software autorizado y productos con licencia.
- Establecer responsables a través de medios oficiales la revisión periódica de la asignación y estado del licenciamiento a través de la herramienta de la Agencia (*System Center*).

1.1.6 Monitoreo de Eventos del sistema 

Observación – Riesgo

La Agencia cuenta con la herramienta NAGIOS CORE, para monitorear los eventos de los servicios informáticos, la cual está soportada por el Manual de Herramienta de Monitoreo de Infraestructura Tecnología. Esta guía no está oficializada ni publicada. Sin un adecuado monitoreo y control de la infraestructura Tecnológica se pueden presentar escenarios de indisponibilidad que afectarían los servicios y la operación de la Agencia.

Recomendación

Se debe oficializar los procedimientos de operación para monitorea y revisar los registros acerca de las excepciones, fallas y eventos que presenta los servicios de tecnología que soportan la plataforma de la Agencia. Se debe tener en cuenta al menos: Fechas, horas y detalles de los eventos; identificación del dispositivo; e identificación del sistema o aplicación afectada.

1.1.7 Administración y revisión de *logs*

Observación – Riesgo

En la validación realizada de la Auditoría se observó que existen *logs* activos (*event_security_serverBD*). Si los *logs* no estuvieran activos no sería posible realizar los seguimientos a cambios significativos de información y así minimizar la falta de integridad en la información. Se observó que no existían guías, manuales o directrices para la gestión de *logs.*

Recomendación

Establecer procedimientos o guías oficiales y políticas para la administración y seguimiento de *logs* de los sistemas de información e infraestructura tecnología, definiendo responsables, con directrices para que los *logs* solo puedan ser accedidos por los usuarios autorizados.

1.1.8 Administración y revisión de antivirus

Observación – Riesgo

La ANDJE cuenta con una herramienta antivirus con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Igualmente en el Manual de Políticas Institucionales y de Desarrollo Administrativo se plantea que "Todos los Colaboradores y terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de la ANDJE son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales. En el desarrollo de la Auditoría no se evidenció procedimientos oficializados para el seguimiento o gestión del antivirus así como el procedimiento que se debe realizar en caso de presentarse uno.

La activación o contagio de un virus informático en la Agencia puede traer perdida de información y por lo tanto impacto en las operaciones normales.

Recomendación

Establecer guías o procedimientos para la administración del antivirus, este debe contener la periodicidad de la actualización, análisis de los virus detectados y las actividades o pasos a seguir en caso que se llegase a presentar uno.

1.1.9 Remediación de vulnerabilidades y actualización de parches

Observación – Riesgo

En la evaluación al proceso de Gestión de Tecnologías de Información se observó que existía en el inventario de activos de infraestructura un documento o guía "NORMAS DE CONTROL AL SOFTWARE OPERATIVO". Este documento no se encontraba oficializado ni publicado. Esto puede generar falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información.

Recomendación

Se debe implementar y oficializar un documento o guía que contemple las acciones y responsables para la identificación de vulnerabilidades técnicas potenciales, tales como:

- Definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
- Definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente.
- Identificar los riesgos asociados y las acciones a seguir como la aplicación de parches de sistemas vulnerables o la aplicación de otros controles
- Los parches se deberían probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se deberían considerar otros controles como:
  - Dejar de operar los servicios o capacidades relacionados con la vulnerabilidad
  - Incrementar el seguimiento para detectar ataques reales
  - Llevar un log de auditoría para todos los procedimientos realizados
  - Seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia
  - Abordar primero los sistemas que están en alto riesgo
  - La vulnerabilidad técnica debería estar alineado con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente.

1.1.10 Ambientes de Desarrollo – Pruebas y Producción 

Observación – Riesgo

De acuerdo con el MANUAL DE POLITICAS INSTITUCIONALES Y DE DESARROLLO ADMINISTRATIVO y en el proceso de la Auditoría se observó que se contaba con la "POLÍTICA DE SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN" igualmente se validó el inventario de los ambientes de producción, pruebas y desarrollo.

1.1.11 Administración de Centros de Datos 

Observación – Riesgo

La ANDJE, cuenta con dos centros de datos: Propio (donde reposan las aplicaciones misionales) y Alterno (donde reposan las demás Aplicaciones). En el "MANUAL DE POLITICAS INSTITUCIONALES Y DE DESARROLLO ADMINISTRATIVO" publicado en SIGI existe la política para el acceso físico, la cual contempla el acceso a los centros de datos.

Se realizó visita al centro de datos propio el cual cumple con los mínimos estándares de control como etiquetado de cables, piso falso, aire acondicionado, Bitácora de Ingreso al Centro de Datos; igualmente se contaba con Instructivo de Control de Accesos a Centro de datos. Los Documentos mencionados no se encuentran aprobados ni publicados, lo cual genera falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información y prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Agencia.

Recomendación

Oficializar los procedimientos, guías y/o formatos.

1.1.12 Administración de usuarios y roles especiales 

Observación – Riesgo

De acuerdo con la evaluación, se observó que no se contaba con guías y /o procedimientos para la gestión y aseguramiento de usuario y roles privilegiados. Lo anterior puede generar riesgos en falta de confidencialidad e integridad de la información, pues estos usuarios y roles podrían ser utilizados para fines diferentes a los de la operación normal.

Los titulares de cuenta de usuario privilegiado pueden estar en capacidad de manipular los *logs* e información sensible en instalaciones de procesamiento de información bajo su control directo.

Recomendación

Establecer políticas, guías y/o procedimientos con el fin de asegurar los usuarios y roles privilegiados. Procedimental el aseguramiento y uso de estos en caso que se requiera.

1.1.13 Administración de *Backups*

Observación – Riesgo

Con base en los soportes entregados se observa que realizan copias de respaldo, de acuerdo "GUIA DE GESTIÓN DE RESPALDO Y RESTAURACIÓN DE COPIAS DE SEGURIDAD". Esta Guía no estaba oficializada ni publicada lo que puede generar falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información.

Las copias de respaldo se distribuyen en dos grupos: A nivel de estaciones de trabajo (incluyendo portátiles), y servidores. La herramienta utilizada es *NetVault Backup*. Para servidores se generan *jobs*.

Los procedimientos operaciones documentados para las copias de respaldo protegen a la Agencia contra la pérdida de datos.

Recomendación

Se debe documentar y oficializar los procedimientos de operación para las copias de respaldo de: Información, software e imágenes de los sistemas. Realizar pruebas de respaldo de acuerdo a la política de copias de respaldo. A los procedimientos operacionales se les debe hacer seguimiento a la ejecución de las copias de respaldo y tener en cuenta las fallas de las copias de respaldo programadas para asegurar la integridad de las copias de respaldo.

Los procedimientos de operación deben incluir al menos:

- Copias completas de respaldo, y procedimientos de restauración documentados.
- Definir el alcance: copias de respaldo completas o diferenciales y frecuencia con que se hagan las copias de respaldo.
- Las copias de respaldo se deberían almacenar en un lugar remoto, Con el fin de mitigar daños que pueda ocurrir en el sitio principal.
- Los soportes de las copias de respaldo deben gozar de protección física.
- Se deben realizar pruebas de respaldo
- En situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deberían estar protegidas por medio de encriptación.

1.1.14 Gestión de usuarios

Observación – Riesgo

Los usuarios se encuentran creados a nivel del Directorio Activo (D.A.). Se validan los parámetros de contraseñas implementados en las directivas del D.A. los cuales corresponde a las políticas definidas en él MANUAL DE POLITICAS INSTITUCIONALES Y DE DESARROLLO ADMINISTRATIVO. Los usuarios son creados de acuerdo con el estándar definido en el Guía para la creación de cuentas de usuario de directorio. Cuando se crea el usuario a nivel del D.A. no se está almacenado el número de cedula ni tipo de contrato (planta, prestación de servicios). Para la inhabilitación o eliminación de un usuario a nivel del D.A. se realiza a través de la solicitud del supervisor del contrato o del Jefe de área al responsable de Sistemas de Gestión de Tecnologías.

Para los usuarios privilegiados a nivel de base de datos y sistemas operativos no existía un control ni procedimiento de aseguramiento de estos. No existía un procedimiento guía lo cual genera falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información.

Aunque se tienen definidos seis (6) grupos de acceso a internet no se observó la definición o política y/o directriz de la asignación del usuario al grupo de acuerdo con el cargo funciones.

La utilización de usuarios privilegiados a nivel de aplicación, bases de datos y sistemas operativos genera riesgos de falta de confidencialidad e integridad en la información. Por ser usuarios privilegiados están en capacidad de manipular los *logs* e información sensible en las instalaciones de procesamiento de información por lo tanto de podrían modificar los datos de la Agencia o podrían ser utilizados para fines diferentes a los de la operación normal.

Recomendación

Tener en cuenta la inclusión del número de cedula y tipo de contrato de los usuarios a nivel de D.A. esto facilita futuras integraciones entre los sistemas de información de la Agencia (Ejemplo D.A. - SARA WEB), facilitando la utilización del mismo usuario y/o la misma clave para los diferentes aplicativos que maneja un mismo usuario; esto minimiza utilizar diferentes usuarios y diferentes claves de un mismo usuario para cada aplicación. Documentar y oficializar el procedimiento o guía de operación para el aseguramiento de usuarios y perfiles privilegiados así como la utilización en casos requeridos (Aplicación de una actualización). Definir lineamientos para la asignación de usuarios a los grupos de internet así como documentar y oficializar los accesos definidos por cada grupo o las restricciones que presente dicho grupo.

1.1.15 Gestión de Políticas en el *F.W.*

Observación – Riesgo

La Agencia cuenta con un *Firewall FortiGate 200B* el cual protege de ataques externos a la red LAN. La administración y la protección se realizan a través de reglas que se encuentran configuradas y administradas por la Agencia. Al momento de la auditoria no existía un procedimiento guía lo cual puede genera falta de aseguramiento de las operaciones correctas y seguras en los procesamientos de la información. Una mala asignación o modificación a una regla sin la autorización necesaria podría generar una vulnerabilidad para que un atacante vulnere nuestros sistemas.

Recomendación

Documentar y oficializar el procedimiento o guía de operación para la modificación, creación o eliminación de reglas en el *firewall* de la Agencia. Adicional a la información técnica, de puerto y/o servicio, la guía debería contemplar sustentar la necesidad la necesidad de la creación, modificación o eliminación de la regla y la autorización del líder del proceso.

1.1.16 Gestión Infraestructura de Comunicaciones

Observación – Riesgo

La Agencia cuenta con la herramienta *Nagios Core* para monitorear los eventos de los servicios informáticos, la cual está soportada por el Manual de Herramienta de Monitoreo de Infraestructura Tecnología. Esta guía no estaba oficializada ni publicada. Se llevaba un inventario manual de los dispositivos o elementos que componen la infraestructura técnica de la Agencia. Para la administración de estos dispositivos no se observó procedimientos o guías, lo cual puede generar riesgos en la falta de continuidad del negocio.

La Agencia debe mantener un inventario de los activos involucrados en el ciclo de vida de la información, y documentar su importancia. La documentación se debería mantener en inventarios dedicados o existentes, según sea apropiado. La no gestión de los dispositivos o elementos de infraestructura puede causar falta de continuidad en las operaciones de la Agencia.

Recomendación

Documentar y oficializar el procedimiento o guía de operación para la Administración de la infraestructura tecnológica. Se debe asegurar que todos los elementos, estén inventariados, clasificados y protegidos de acuerdo al riesgo que se expongan.

1.1.17 Gestión de *VPN Client to Site*

Observación – Riesgo

La Agencia cuenta con una *VPN Client to Site* de FORTINET para el acceso remoto que requieren los usuarios de la Agencia (ejemplo teletrabajo). No estaba definido el protocolo, guía o directriz que defina que usuarios que de acuerdo con sus funciones deben tener asignada una *VPN* o el procedimiento oficial para su asignación.

Una asignación no autorizada a una *VPN* puede ocasionar riesgos en falta de confidencialidad de la información; un usuario puede consultar y al almacenar información desde sitios fuera de la Agencia.

Recomendación

Definir y oficializar políticas o directrices, así como guías para la asignación de VPN.

1.2 Mapa de Riesgos

Observación – Riesgo

Se observó en SIGI un solo riesgo para el proceso de GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN, el cual se identifica como: "ERRORES EN LA IDENTIFICACIÓN, CLASIFICACIÓN Y PRIORIZACIÓN DE LAS NECESIDADES DE SOLUCIONES DE TIC". Los riesgos son dinámicos, la no identificación oportuna de estos genera vulnerabilidades que no detectadas a tiempo son una amenaza potencial de explotación.

Recomendación

Existen Riesgos en los procesos de sistemas de información como Falta de integridad, confidencialidad y/o disponibilidad de la información. Validar el riesgo definido en la matriz de riesgos de acuerdo con la metodología de riesgos con el fin de identificar riesgos adicionales al proceso y revisarlos periódicamente.

1.3 Plan de Continuidad

Observación – Riesgo

Se observó que existía un Plan de continuidad para los aplicativos misionales y la realización de pruebas de funcionalidad del mismo. Igualmente se observó en el Plan Estratégico de Tecnología (2017-2020) la inclusión de un plan de continuidad con mayor cobertura al vigente al momento de la auditoria.

1.4 Indicadores de Gestión – POA

1.4.1 Secretaría General POA 04-SG-16 Desarrollar requerimientos para fortalecer el Sistema de Gestión Documental ORFEO

Observación – Riesgo

Se validaron los compromisos adquiridos de Acuerdo con el POA (desarrollar los cinco (5) requerimientos más demandados por la Entidad) los cuales se cumplieron de acuerdo con lo observado.

1.4.2 Secretaría General POA 07-SG-16 Realizar informes trimestrales de implementación del Plan y Estrategia de Transición de IPv4 a IPv6

Observación – Riesgo

Se validaron los compromisos adquiridos de Acuerdo con el POA los cuales cumplen de acuerdo con lo observado. Se verificó que se cumplió con "Realizar informes trimestrales de avance en la implementación del plan y la estrategia de transición de IPv4 a IPv6" con corte al informe de Marzo/2016.

1.4.3 Dirección de Gestión de Información POA 04-DGI-1-2-16
Soporte y mantenimiento de la versión en operación eKOGUI

Observación – Riesgo

Se validaron lo compromisos adquiridos de Acuerdo con el POA a nivel de la operación actual (no se incluyó proyecto ya que forma parte de la Auditoría Gestión del Sistema Único de Actividad Litigiosa) los cuales cumplen de acuerdo con lo observado. Cumplimiento del 85% de incidencias reportadas.

2 Aplicaciones De Industria

2.1.1 SARA WEB

Observación – Riesgo

La ANDJE cuenta con el software de SARA WEB. De acuerdo con la validación realizada se observó que la aplicación SARA WEB no tenía implementados los controles de gestión de contraseñas ej: claves_letras, claves_números, número_intentos, clave_longitud, clave repetir, clave_cambioobligatorio, configuración de ruta de LOG (ver soporte en papeles de trabajo).

Recomendación

Validar con el proveedor de SARA WEB, el estado de la parametrización del módulo de seguridad y solicitar los ajustes necesarios en módulo de acuerdo con las políticas definidas en la Agencia.

2.1.2 SIIF

Observación – Riesgo

Para la aplicación SIIF, se apoyó en el la evaluación realizada y cuyo soporte se encuentra en el informe de referencia GF SIC-CIC-02-03 de fecha de cierre 06/05/2016.

9. DESCRIPCIÓN DE LA (S) NO CONFORMIDAD (ES) Y/O HALLAZGO (S)

9.1. NO CONFORMIDADES EN EL SISTEMA DE CALIDAD

REQUISITO DE LA NORMA	NO CONFORMIDAD	OBSERVACIONES
No Aplica	No Aplica	No Aplica

9.2. HALLAZGOS EN EL SISTEMA DE CONTROL INTERNO

REQUISITO DE LA NORMA	HALLAZGOS	OBSERVACIONES
Ninguno		

10. RECOMENDACIONES:

Referidas dentro del texto del informe para cada control analizado.

Firma Auditor Designado y Equipo Auditor	Firma Jefe de Control Interno ANDJE
Informe firmado Electrónicamente en Orfeo Rad. 20161020011113	Informe firmado Electrónicamente en Orfeo Rad. 20161020011113