AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

INFORME FINAL DE AUDITORÍA AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficina de Control Interno
Elaborado Por: Jorge Hernando Torres Ribero
Aprobado por: Adriana Milena Herrera Abril

A. Introducción

La Oficina de Control Interno de la Agencia Nacional de Defensa Jurídica del Estado, en el desarrollo de su Plan Anual de Auditorías 2024 – 2025, practicó la auditoría al Plan de Seguridad y Privacidad de la Información, con el objetivo de verificar la información, procedimientos, procesos y manuales que comprenden y hacen parte del Modelo de Seguridad y Privacidad de la Información (MSPI) y su implementación hasta mayo de 2024 como mínimo.

En el marco de la auditoría se verificó:

1) Control de Acceso y Gestión de Usuarios
2) Gestión de Activos de Información y Clasificación de la Información
3) Seguridad Operativa y Gestión de Incidentes
4) Gestión de Cambios y Desarrollo de Software Seguro
5) Respaldo y Restauración de Datos
6) Plan de Sensibilización y Comunicación de Seguridad de la Información
7) Contratos
8) FURAG

Dicha auditoría se efectuó del 02 de junio al 16 de julio de 2024, con envío de informe final del 12 de agosto de 2024, y sus resultados se presentan a continuación.

B. Desarrollo de la Auditoría

El análisis realizado por parte de la Oficina de Control Interno al Modelo de Seguridad y Privacidad de la Información (MSPI), se realizó tomando como base la normatividad expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones en el *"Documento Maestro del Modelo de Seguridad y Privacidad de la información"* de Octubre de 2021, el cual tiene como fin identificar los requerimientos de seguridad y privacidad de la información en las entidades del estado, permitiendo así establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las mismas. Igualmente se revisaron los proceso y procedimientos relevantes internos de la entidad (ver anexo 2).

Sobre el particular se aclara que se evaluaron las temáticas 1 a 8 de la sección anterior cubriendo los requerimientos de la norma.

1. CONTROL DE ACCESO Y GESTIÓN DE USUARIOS

En esta sección se detalla el análisis de los controles de acceso y gestión de usuarios implementados en la organización, basado en la revisión de documentos y evidencias presentadas. A continuación, se presenta un resumen de la evaluación realizada.

1.1. Existencia de políticas y procedimientos de control de acceso documentados:

- **Evidencias:** Procedimiento GTI P01 pasos de creación de usuarios y accesos realizados por talento humano. El procedimiento GTI P01 está vigente y se encuentra en actualización al igual que la Guía de gestión de usuarios GTI-G10. Se expidió Circular y se verifican casos con mesa de servicio, sin embargo, las evidencias aportadas son de 2023.
- **Criterio de Auditoría:** Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.2: Política de Gestión de Acceso Numeral: 6.4.2. Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Gestión de Acceso Numeral: 5.4.2.
- **Evaluación:** Se evidenció el cumplimiento, sin embargo, en el informe preliminar se recomendó mantener los registros actualizados.

  Sobre el particular la OASTI en su respuesta al informe preliminar No aceptó la recomendación , en razón a que indicó que el área si cuenta con los Registros correspondientes a lo cursado en el año 2024, los cuales se podían consultar en el siguiente enlace al archivo CASOS CREACION INACTIVACION 2024.xlsx.

  Por lo anterior la OCI procedió a revisar de nuevo la información y conforme a lo encontrado se retira la recomendación.

1.2. Implementación de doble factor de autenticación

- **Evidencias:** Logs de autenticación y configuración de doble factor (Log de accesos Pantalla y a nivel de aplicativo)
- **Criterio de Auditoría**: Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.3: Política de Autenticación Numeral: 6.4.3. Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Autenticación Numeral: 5.4.3.
- **Evaluación:** Se verificó el cumplimiento y la implementación completa y operativa. Se evidencian Logs de autenticación y configuración de doble factor disponibles. Actualmente se está revisando para el correo; en el nuevo plan se están implementando controles de doble factor de autenticación y se están estableciendo nuevas propuestas de capa de seguridad adicional a los correos de la Agencia. Se **recomienda** priorizar los sistemas que manejen activos de Información Críticos para la Entidad.

La OASTI aceptó la Recomendación, e indicó que propondrá las acciones de mejora correspondientes para los sistemas referidos. En virtud de lo anterior, la recomendación será la siguiente:

- Se evidenció cumplimiento a través de las políticas en los sistemas Ekogui, Daruma, Orfeo y Mercurio. Sin embargo, los criterios de la Política de Seguridad y Privacidad de la Información (Sección 5.4) sugieren la implementación de controles adicionales de autenticación. La falta de estos controles adicionales se debe presuntamente a la priorización de otras medidas de seguridad. Mejorar estos controles podría incrementar la seguridad de las cuentas de usuario y reducir el riesgo de accesos no autorizados.

1.3. Gestión de derechos de acceso privilegiado

- **Evidencias:** Gestión de Usuarios (CORREOS_ELCTRONICOS_2023 Gestión de Usuarios.docx1.1 USUARIOS D.A. ACTIVOS-INACTIVOS 2024.xlsx, CASOS CREACION INACTIVACION 2024.xlsx).

- **Criterio de Auditoría:** Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.4: Política de Gestión de Acceso Privilegiado Numeral: 6.4.4. Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Gestión de Acceso Numeral: 5.4.4.
- Evaluación: Se corroboró el cumplimiento a través de comunicaciones con GTH, Contratos y BID. Se presentó la evidencia de los correos enviados en 2023 y 2024.

1.4. Revisión periódica de derechos de acceso

- **Evidencias:** CORREOS_ELCTRONICOS_2023, Gestión de Usuarios (CORREOS_ELCTRONICOS_2023, CASOS CREACION INACTIVACION 2024.xlsx).
- **Criterio de Auditoría:** Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.5: Política de Revisión de Accesos Numeral: 6.4.5. Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Revisión de Accesos Numeral: 5.4.5.
- **Evaluación:** Se evidenció el cumplimiento cada vez que aplican novedades de personal y a través de solicitud en correos desde GTI solicitando novedades al GTH, Grupo de contratos y al BID, los soportes presentados son de 2023, por lo tanto, se **recomienda** mantener actualizada la información a 2024 y establecer una periodicidad adecuada de solicitud. 1.3. y 1.4

En respuesta al informe preliminar la OASTI, no aceptó la recomendación, indicando que cuenta con los registros correspondientes de 2024, los cuales se pueden consultar en el enlace puesto a disposición de la auditoría: CASOS CREACION INACTIVACION 2024.xlsx.

De conformidad con lo anterior, se revisó la información entregada, y se retira la recomendación de mantener actualizada la información.

1.5. Políticas de gestión de cuentas de usuario

- **Evidencias:** A nivel aplicativo Gestión Usuarios Ekogui (A nivel aplicativo GEst...).
- **Criterio de Auditoría:** Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.6: Política de Gestión de Cuentas de Usuario Numeral: 6.4.6. Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Gestión de Cuentas de Usuario Numeral: 5.4.6.
- **Evaluación:** Se evidenció cumplimiento a través de las políticas en los sistemas Ekogui, Daruma, Orfeo Mercurio, y se encuentran definidos en la guía GTI-G10 y el procedimiento GTI-P01.

1.6. Monitoreo y registro de accesos

- **Evidencias:** Log de accesos Pantallazo de configuración ekogui (Log de accesos Pantalla).
- **Criterio de Auditoría**: Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.7: Política de Monitoreo y Registro de Accesos Numeral: 6.4.7. Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Monitoreo y Registro de Accesos Numeral: 5.4.7.
- **Evaluación:** Se evidencio la realización del monitoreo y registros implementados, efectivamente existen Logs de acceso y auditorías disponibles. Se registra la traza en los sistemas de directorio activo. Otros sistemas mantienen logs por defecto, por ejemplo, Ekogui. Dichos logs se utilizan si suceden eventos de seguridad en tiempo real.

1.7. Procedimientos para la detección y respuesta a accesos no autorizados

- **Evidencias:** Procedimientos de respuesta a incidentes (A nivel aplicativo GEst...).
- **Criterio de Auditoría**: Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.5: Política de Detección y Respuesta a Accesos No Autorizados Numeral: 6.4.5. Política de Seguridad y Privacidad de la Información, Sección 5.5: Detección y Respuesta a Accesos No Autorizados Numeral: 5.5.1.
- **Evaluación:** Se encontraron disponibles los procedimientos de detección y respuesta documentados y operativos, igualmente los procedimientos y reportes disponibles. Procedimiento de Incidentes de seguridad GTI-P05.

1.8. Evaluación de cumplimiento de políticas de acceso

- **Evidencias:** CREACION USUARIOS GLPI – Mesa de Servicio (CORREOS_ELCTRONICOS_202...).
- **Criterio de Auditoría:** Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.6: Política de Evaluación de Cumplimiento de Acceso Numeral: 6.4.6. Política de Seguridad y Privacidad de la Información Sección 5.6: Evaluación de Cumplimiento de Políticas de Acceso Numeral: 5.6.1.
- **Evaluación**: Se evalúo el uso del formato F04 del cual se evidenció su utilización, además está incluido en el sistema GLP Mesa de ayuda, también se encuentra en Daruma y en los correos de accesos.

2. GESTIÓN DE ACTIVOS DE INFORMACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

En esta sección se detalla el análisis de la gestión de activos de información y su clasificación, basado en la revisión de documentos y evidencias presentadas. A continuación, se presenta un resumen de la evaluación.

2.1. Inventario de Activos de Información

- **Criterio de Auditoría:**

  Política de Seguridad y Privacidad de la Información, Sección 6.1: Inventario de Activos de Información, Numeral: 6.1.1. Documento, Numeral 11 del Anexo del Modelo de Seguridad y Privacidad de la Información MSPI Documento Maestro, numerales **A.6.1.1, A.6.1.2, A.6.2, A.7, A.8.2, A.9, A.9.2, A.10, A.12, A.13**
- **Evidencia Presentada:** GTI-F-05 Matriz de Inventario Clasificación y Publicación de Información. Sin embargo, el Sistema Daruma no visualiza los riesgos a menos que tengan un plan de mejoramiento, lo cual es incorrecto.
- **Evaluación**: Se presentó evidencia del inventario de activos de información actualizado en agosto de 2023, operación que se efectúo de manera anual según GTI-G-01 Guía de Inventario de Activos, Clasificación y Publicación de Información. Se solicitó por correo electrónico, reunión con líderes de proceso para revisión de activos de información. Se actualizó realizando solicitud por correo electrónico.

2.2. Clasificación de la Información según su Criticidad

- **Criterio de Auditoría**:

  Política de Seguridad y Privacidad de la Información, Sección 6.2: Clasificación de Información, Numeral: 6.2.1.

- **Evidencia Presentada**:
  - Guía de inventario de activos, clasificación y publicación de información gti-g-01
  - Activos_información__2023.xls
  - Indice_información_clasificada_reservada_2023_7122023.xls
  - Documento de uso aceptable de activos de información.
- **Evaluación:**

  En la evaluación realizada, se observó que la clasificación y gestión de la **información** contenida en el "**Módulo de Comités de Conciliación**", corresponde a datos de carácter reservado, de acuerdo con lo previsto en los artículos 18 y 19 con su parágrafo de la Ley 1712 de 2014 (actas de comité de conciliación y fichas de conciliación) hasta de 275 Entidades Públicas del Orden Nacional (EPON) y 108 territoriales, cuya custodia está bajo la Agencia Nacional de Defensa Jurídica del Estado.

  El Decreto 103 de 2015 al tratar la Gestión de la **Información** Clasificada y Reservada, en su artículo 30 indica que las Entidades que tengan la "*custodia*" de la información debe identificar las disposiciones de Ley para asignarle el carácter de clasificado o reservado. Adicionalmente, el artículo 32 precisa que la obligación de clasificar la información reservada es conjunta entre quien la entrega y quien la custodia.

  Por lo anterior, se considera que la información contenida en este Modulo, entregada por las Entidades, no está debidamente identificada ni valorada en el INDICE_INFORMACIÓN_CLASIFICADA_RESERVADA_2023_7122023.xls que si bien es cierto que aparece en el sistema e-KOGUI, dentro del inventario se encuentra de la siguiente forma:

Nombre de la Categoría de la información	SOFTWARE
Nombre del titulo de la información	Sistema eKOGUI
Idioma	N/A
Medio de conservación y/o soporte	N/A
Fecha de generación de la información	N/A
Nombre del responsable de la producción de la información	Gestión de Información de Defensa Jurídica
Nombre del responsable de la información	Gestión de tecnologías de la información
Objetivo legítimo de la excepción	Parcial
Fundamento constitucional o legal	Ilimitada
Fundamento jurídico de la excepción	De revelarse los datos personales privados, sensibles, semiprivados o de niños, niñas o adolescentes que pueda contener el activo de información, se vulneraría el derecho a la intimidad del titular de los datos. La individualización del daño estará dado respecto de cada titular de los datos personales que se encuentren en el activo de información. La individualización del daño estará dado respecto de cada titular de los datos personales que se encuentren en el activo de información.
Excepción total o parcial	No
Fecha de la calificación	25/07/2023
Plazo de la clasificación o reserva	No
Observaciones	

Dicho inventario solo se refiere a datos personales privados, sensibles, semiprivados o de niños, niñas o adolescentes que pueda contener el activo de información, como se evidencia en la columna denominada "***FUNDAMENTO JURÍDICO DE LA EXCEPCIÓN***". En el mismo sentido está ocurriendo, con la información de las Entidades territoriales que voluntariamente puedan estar utilizando el Módulo.

Esta situación se configuró inicialmente como una no Conformidad, pero según lo citado normativamente, dada la naturaleza compartida de la responsabilidad en la clasificación de la información ingresada en el sistema por terceros, y el papel de la ANDJE como custodio de dicha información se configura como una Observación, que deberá ser revisada y analizada por el líder de proceso de Gestión de Tecnologías de la Información, teniendo en cuenta su papel como Oficial de Seguridad de la información y protección de Datos personales, conforme a la Resolución 467 del 28 de junio de 2024 artículos 3 y 4

Resumen de los Argumentos Presentados por el Área Auditada Frente a la Observación:

La Oficina Asesora de Sistemas y Tecnologías de Información (OASTI) no aceptó en su momento la presunta No Conformidad en su forma inicial como No Conformidad y argumenta lo siguiente:

- **Clasificación Integral del Sistema eKOGUI**: La OASTI sostiene que el "Módulo de Comités de Conciliación" es parte del activo de información denominado "Sistema eKOGUI", clasificado como un sistema crítico, y afirma que no es necesario el tratamiento individualizado de módulos dentro del sistema, para lo cual presentan concepto de un funcionaria de Mintic **Angela Janeth Cortés Hernández** que firma como Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información - Despacho del Ministro, argumento con el que está de acuerdo la Dirección de Gestión de Información DGI en reunión sostenida el 24 de Octubre de 2024 junto con la Oficina Asesora de Sistemas y tecnologías de Información OASTI y la Oficina de de Control Interno.
- **Cumplimiento de la Guía de Clasificación**: Según la OASTI, la clasificación de la información ha sido realizada conforme a la Guía GTI-G-01 de inventario de activos, documentada a través de la matriz GTI-F-05.
- **Alineación con MinTIC y la Arquitectura Empresarial MRAE 3.0**: Los documentos generados están alineados con las directrices del Ministerio TIC, que orientan a las entidades en la gestión del ciclo de vida de los sistemas de información de manera integral.
- **Revisión del Hallazgo dentro del Contexto de Gestión de Riesgos**: La OASTI solicita que se considere el hallazgo como un riesgo y no como un incumplimiento, en vista de que la responsabilidad de clasificar recae en los terceros que ingresan la información.

Justificación Normativa de la Observación y Recomendaciones:

Se reitera que, aunque el sistema eKOGUI se gestione integralmente, la información reservada contenida en el módulo mencionado y aquella que se almacena en el SGDEA como resultado, requiere un enfoque específico en su identificación y gestión, con base en los siguientes artículos 30, 31 y 32 del decreto 103 de 2015 (compilado en el decreto 1081 de 2015)

- **Fortalecimiento de las Medidas de Seguridad**: Adoptar medidas técnicas, humanas y administrativas para garantizar la seguridad de los datos personales y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado en el sistema eKOGUI.

- **Actualización de la Clasificación de Activos de Información**: Revisar y actualizar la guía de clasificación de activos, asegurando que toda la información contenida en el Sistema, esté debidamente clasificada y valorada.
- **Capacitación y Sensibilización**: Brindar capacitación regular a los responsables y usuarios del sistema sobre la importancia de la clasificación y gestión adecuada de la información crítica, conforme a las normas vigentes y las disposiciones de la Ley 1712 de 2014 y el Decreto 103 de 2015.
- **Evaluaciones Periódicas de Seguridad**: Realizar evaluaciones periódicas del sistema eKOGUI en producción, así como a sus copias de Soporte y Pruebas, utilizando metodologías aplicables para asegurar el cumplimiento de las políticas de seguridad y privacidad de la información, e identificar y mitigar brechas de seguridad en la gestión de datos.

De lo anterior se desprende la siguiente Observación:

***Observación**: "Se observa que el 'Módulo de Comités de Conciliación' en el sistema eKOGUI gestiona información clasificada y reservada ingresada por entidades públicas. Si bien la responsabilidad inicial de clasificar y advertir sobre el carácter reservado de la información recae en las entidades que la aportan, la **Agencia Nacional de Defensa Jurídica del Estado**, como custodio de la información registrada en el sistema eKOGUI y conforme a lo estipulado en la Ley 1712 de 2014 Art 18 , 19 y parágrafo y el Decreto 1081 de 2015 en sus artículos 2.1.1.4.3.1, 2.1.1.4.3.2 y 2.1.1.4.3.3 del Decreto 1081 de 2015, tiene la obligación de identificar, clasificar y gestionar adecuadamente dicha información.*

*A su vez, la OCI recomienda tener en cuenta por parte de la OASTI, en su rol de oficial de seguridad de la información y de protección de datos personales de la Entidad, implementar mecanismos para la clasificación y valoración de los activos de información crítica. Así mismo, en caso de existir brechas de seguridad que comprometan esta información, notificar a la entidad propietaria de la información afectada, en cumplimiento de las normativas de protección de datos y seguridad de la información vigentes, como el **Decreto 1377 de 2013** y la **Ley 1581 de 2012**. Por otra parte, se recomienda que la Entidad implemente exclusiones de responsabilidad y advertencias legales dirigidas a las entidades que ingresan información clasificada y reservada en el sistema eKOGUI, para prevenir filtraciones y posibles consecuencias legales.*

2.3 Implementación de Controles de Protección Adecuados

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.3: Controles de Protección, Numeral: 6.3.1.
- **Evaluación:** Se evidenciaron controles en el mapa de riesgos, se presentan por cada riesgo, pero solo se visualizan aquellos riesgos que tienen plan de mejoramiento activo. Por lo anterior, se recomienda mostrar todos los riesgos inherentes con su respectivo tratamiento y el riesgo residual.

  En relación con lo anterior la OASTI en el informe preliminar indicó que la recomendación hace referencia a la imposibilidad de visualización de los riesgos y su tratamiento a través de la herramienta DARUMA. Por lo cual consideran que la misma sea elevada a la Oficina Asesora de Planeación que es la dependencia responsable de la funcionalidad de este servicio.

Sobre el particular, la OCI resalta que teniendo en cuenta que se tratan de los Riesgos asociados al proceso auditado, le corresponde al área realizar las gestiones directamente con la OAP (responsable del Daruma) para la corrección de esta situación, ya que se encuentra una afectación en su propio proceso.

A su vez se confirma que la presunta causa de esta deficiencia es la limitación en la herramienta Daruma utilizada para la gestión de riesgos. Esto puede llevar a una gestión inadecuada de los riesgos, comprometiendo la efectividad de los controles de seguridad.

2.4. Políticas y Procedimientos de Gestión de Activos de Información

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información, Sección 6.4: Gestión de Activos de Información, Numeral: 6.4.1.
- **Evidencia Presentada**: GUÍA DE INVENTARIO DE ACTIVOS, CLASIFICACIÓN Y PUBLICACIÓN DE INFORMACIÓN GTI-G-01. Documento de uso aceptable de activos de información. Logs de autenticación y configuración de doble factor (Log de accesos Pantalla y a nivel de aplicativo.)
- **Evaluación:** Se evidenció cumplimiento en cuanto a la existencia de políticas y procedimientos, y se realizó el ejercicio de manera anual. El auditado manifestó que en un nuevo plan se están implementando controles de doble factor de autenticación y se están estableciendo nuevas propuestas de capa de seguridad adicional a los correos de la Agencia.

2.5. Procedimientos para la Eliminación Segura de Activos

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.5: Eliminación Segura de Información, Numeral: 6.5.1.
- **Evidencias:** GTI-G-03 Guía para la Manipulación de Medios y Borrado Seguro.
- **Evaluación:** Se evidenció la existencia de las guías y procedimientos, no obstante **se recomienda** actualizar el procedimiento para borrado seguro en la nube y ejecutar el protocolo que aplica en todos los casos de desvinculación de usuario y diferentes dispositivos, no obstante de que la información se encuentre en Office 365 (en la nube), ya que la desvinculación de las cuentas no garantiza que no queden copias o archivos residuales en los equipos, lo que podría comprometer la confidencialidad de la información de la entidad.

  La OASTI aceptó la Observación manifestando que actualmente se encuentra actualizando la Guía de borrado seguro.

  La causa de esta brecha es la presunta falta de actualización en los protocolos de eliminación segura. Las consecuencias de no abordar esta brecha incluyen la posibilidad de que queden copias o archivos residuales en los equipos, comprometiendo la confidencialidad de la información de la entidad.

2.6. Auditorías Periódicas del Inventario de Activos

- Criterio de Auditoría:
  - Política de Seguridad y Privacidad de la Información, Sección 6.4: Gestión de Activos de Información, Numeral: 6.4.2.

- Evidencias: GUÍA DE INVENTARIO DE ACTIVOS, CLASIFICACIÓN Y PUBLICACIÓN DE INFORMACIÓN GTI-G-01.
- Evaluación: Se evidenció un ejercicio anual de actualización.

3. SEGURIDAD OPERATIVA Y GESTIÓN DE INCIDENTES

En esta sección se detalla el análisis de la seguridad operativa y la gestión de incidentes implementados en la organización, basado en la revisión de documentos y evidencias presentadas. A continuación, se presenta un resumen de la evaluación realizada.

3.1. Gestión de Incidentes

- **Criterio de Auditoría**: Conforme a la Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Incidentes de Seguridad, Numeral: 6.6.1.
- **Evidencia Presentada:** Los documentos de políticas y procedimientos documentados están disponibles.
- **Evaluación:** Aunque las políticas y procedimientos están documentados y actualizados, se carece de registros específicos que evidencien la aplicación práctica de estos en incidentes reales. Esto se observó en el registro en Daruma, donde se reportan cero incidentes materializados, y en la página de transparencia del portal de la Agencia solo tiene reportes hasta 2023. Por lo que, se **recomienda** una actualización de la página de la entidad con información de incidentes de 2024 para reflejar la gestión y resolución actual de los mismos.

  La causa principal es la presunta falta de implementación de un sistema de seguimiento adecuado. Las consecuencias potenciales incluyen una respuesta ineficaz a incidentes de seguridad y la incapacidad de demostrar el cumplimiento de los procedimientos de seguridad.

3.2. Registro y seguimiento de incidentes de seguridad

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información, Sección 6.6: Gestión de Incidentes de Seguridad, Numeral: 6.6.2.
- **Evidencia Presentada:** La documentación de políticas y procedimientos está disponible. Se manejan reportes en Daruma y una base de conocimiento.
- **Evaluación:** La falta de registros detallados y actuales de incidentes sugiere que no se está aplicando completamente el procedimiento de registro y seguimiento. Los reportes en el portal de transparencia y en Daruma no concuerdan con los registros de la base de conocimientos interna que muestran tres incidentes documentados de nivel clasificado y reservado. **Se recomienda** establecer las excepciones y declaraciones de aplicabilidad en caso de ser necesario.

Frente a la recomendación el área auditada aceptó la recomendación, verificará el Procedimiento GTI-P-05- Gestión de incidentes de seguridad de la información.

Sin embargo, en cuanto a la falta de registros específicos que evidencien la aplicación práctica de los procedimientos, el área auditada no aceptó la Observación, indicando lo siguiente:

"...en razón a que la OASTI está dando cumplimiento al procedimiento GTI-P-05- gestión de incidentes de seguridad de la información en el cual los reportes de posibles incidentes (Eventos), tienen un manejo similar a aquellos que si son declarados como incidentes de seguridad".

... A su vez, se ponen de presente las siguientes definiciones:

"Un evento de seguridad hace referencia a cualquier suceso o acontecimiento que tiene el potencial de afectar la seguridad de la información. Los eventos de seguridad, en su mayoría, no implican necesariamente una amenaza inmediata o un riesgo significativo para la integridad, confidencialidad o disponibilidad de la información".

"Por su parte, un incidente de seguridad se produce cuando un evento tiene un impacto real y negativo en la seguridad de la información de una organización. Un incidente implica una amenaza o violación de la seguridad que compromete la integridad, confidencialidad o disponibilidad de datos críticos".

"Mientras que un evento de seguridad constituye cualquier suceso que pueda afectar la seguridad de la información, un incidente de seguridad representa la materialización de un riesgo, con consecuencias tangibles y potencialmente perjudiciales para la organización. La distinción clara entre eventos e incidentes es esencial para una respuesta eficaz y una gestión proactiva de la seguridad en el entorno empresarial."

Para el caso específico de la base consultada para esta auditoria los casos registrados no llegaron a materializarse razón por la cual no se registran en el portal de Internet en donde si deben ser reportados los incidentes de seguridad".

Se precisa que la mejora no aplica en razón a que el informe que se publica en la página web tiene una periodicidad anual y se reportó en enero de 2024, el siguiente reporte se hará en enero de 2025..."

La OCI luego de analizados los argumentos del auditado, retira la recomendación de *"Actualizar la página de incidentes de la Agencia con la información de Incidentes 2024",* sin embargo, se *sugiere precisar* en el procedimiento las definiciones de "*Evento*" e "*Incidente*", manteniendo coherencia entre estas y el indicador Indicador 05-GTI-24 #268 en Daruma.

A su vez, se recomienda establecer las excepciones y declaraciones de aplicabilidad en caso de ser necesario para asegurar que todos los incidentes sean registrados y gestionados adecuadamente. El área auditada ha aceptado la recomendación y verificará el Procedimiento GTI-P-05 para la gestión de incidentes de seguridad de la información.

3.3. Análisis de causa raíz y acciones correctivas

- **Criterio de Auditoría**: Política de Seguridad y Privacidad de la Información Sección 8.3: Análisis de Causa Raíz y Acciones Correctivas, Numeral: 8.3.1.
- **Evidencia Presentada**: La documentación de políticas y procedimientos está disponible, igualmente la de Incidentes en la base de conocimiento.
- **Evaluación:** Se evidenció el análisis de causa raíz en los documentos de incidentes en la sección Respuesta, allí se indican las acciones tomadas.

Descripción: Existe falta de registros específicos que evidencien la aplicación práctica de los procedimientos.

La OASTI aceptó la recomendación y se comprometió a incluir un capítulo de seguridad de la información que contenga la temática relacionada con la gestión de incidentes. Además, se evaluará la inclusión como control de los requerimientos no funcionales de seguridad para el sistema Ekogui en el Módulo de Comités de Conciliación, asegurando una gestión más eficaz y robusta de los incidentes de seguridad.

3.4. Pruebas y simulacros de respuesta a incidentes

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Pruebas y Simulacros de Respuesta a Incidentes, Numeral: 6.6.1.
- **Evidencia Presentada:** Se realizaron 2 simulacros en 2023, incluyendo uno de phishing y una simulación de sala de crisis con alta dirección.
- **Evaluación:** Aunque se realizaron los simulacros, no se ha difundido adecuadamente la información sobre los resultados y efectividad de estos. Se sugiere realizarlo.

En relación con lo anterior, el área No aceptó la Observación, manifestando que cuenta con las evidencias de la socialización de los resultados y efectividad de los simulacros las cuales se pueden consultar en link adjunto PHISHIN_SIMULADO_2023.pptx y PHISHIN_SIMULADO_2022.pptx

La OCI acepta la difusión para los simulacros de Phishing efectuados, sin embargo, no se evidenció divulgación de los resultados de simulacros de sala de crisis, o el documento técnico circulado que lo soporte.

Por lo anterior, la recomendación quedará en los siguientes términos: Aunque se realizaron simulacros de respuesta a incidentes, no se ha difundido adecuadamente la información sobre los resultados y efectividad de estos. Los criterios según la Política de Seguridad y Privacidad de la Información (Sección 6.6, Numeral 6.6.1) exigen la documentación y comunicación de los resultados de dichos simulacros. La presunta falta de difusión se debe a una deficiente gestión en la comunicación interna. Esto puede llevar a una respuesta inadecuada ante incidentes reales, comprometiendo la seguridad y eficiencia operativa.

4. GESTIÓN DE CAMBIOS Y DESARROLLO DE SOFTWARE SEGURO

La auditoría se centró en evaluar las políticas, procedimientos y controles implementados en la gestión de cambios y el desarrollo de software seguro. El objetivo fue verificar el cumplimiento con los estándares de seguridad y normativas establecidas, asegurando la integridad y la protección de los sistemas de información.

4.1. Políticas y Procedimientos de Gestión de Cambios

- **Criterio de Auditoría**: Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Cambios, Numeral: 6.6.1
- **Evidencia Presentada**: Documento: GTI-F-10 Solicitud de Cambios RFC, Archivo: GTI-F-10_ SOLICITUD DE CAMBIOS RFC.docx
- **Evaluación:** las políticas y procedimientos de gestión de cambios están debidamente documentados y aprobados, cumpliendo con los procedimientos. Se evidenció su cumplimiento.

4.2. Desarrollo de Software Seguro

- **Criterio de Auditoría**: Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Desarrollo de Software Seguro, Numeral: 6.6.1
- **Evidencia Presentada:** Documento: Validación Buzón Factura Electrónica opción No, Archivo: _validación Buzon Factura, Electrónica opción No.docx, Documento: Validación Buzón Arbitramiento, Archivo: _validación Buzon Arbitramiento.docx
- **Evaluación**: Se evidenció el cumplimiento para las pruebas de seguridad y las auditorías de código fueron exitosas, cumpliendo con los estándares de seguridad establecidos.

4.3. Pruebas de Seguridad en el Software Desarrollado

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.7: Pruebas de Seguridad en el Software, Numeral: 6.7.1
- **Evidencia Presentada:** Documento: Validación Buzón Jurisprudencia, Archivo: _Validación Buzon Jurisprudencia.docx, Documento: Validación Buzón Conciliaciones Nacionales y Territoriales, Archivos: _Validación Buzon Conciliaciones Nacionales Opción No.docx, _validación Buzon Conciliaciones Territorial Opción No.docx
- **Evaluación:** Las pruebas de seguridad realizadas fueron exitosas y documentadas adecuadamente en el ámbito realizado.

4.4. Gestión de Versiones y Despliegue de Software

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Cambios y Desarrollo de Software Seguro, Numeral: 6.6.3
- **Evidencia Presentada:** Documento: Cambio de Logos Ekogui1.0 y Ekogui2.0, Archivo: [#ARQ-4204] Cambio de Logos Ekogui1.0 y Ekogui2.0.pdf
- **Evaluación**: Los cambios de versión y despliegue fueron correctamente gestionados y documentados.

4.5. Evaluación de Riesgos antes de Implementar Cambios

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información , Sección 6.6: Evaluación de Riesgos, Numeral: 6.6.1
- **Evidencia Presentada:** Documento: GTI-F-10 Solicitud de Cambios RFC, Archivo: GTI-F-10_ SOLICITUD DE CAMBIOS RFC.docx
- **Evaluación:** se evidencia cumplimiento ya que la evaluación de riesgos está adecuadamente documentada y se han implementado controles para mitigar riesgos antes de realizar cambios.

4.6. Procedimientos de Retroceso y Recuperación ante Fallos

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Continuidad del Negocio, Numeral: 6.6.2
- **Evidencia Presentada:** Documento: GTI-F-10 Solicitud de Cambios RFC, Archivo: GTI-F-10_ SOLICITUD DE CAMBIOS RFC.docx
- **Evaluación**: se videncia su cumplimiento, los procedimientos de retroceso y recuperación están documentados adecuadamente y se han implementado controles para asegurar la continuidad del negocio.

5. RESPALDO Y RESTAURACIÓN DE DATOS

Esta sección de la auditoría se centra en evaluar las políticas, procedimientos y prácticas relacionadas con el respaldo y la restauración de datos dentro de la organización. El objetivo es asegurar que se cuente con medidas adecuadas para proteger la información crítica, garantizar su integridad y disponibilidad, y permitir una recuperación efectiva en caso de fallos.

5.1. Políticas y Procedimientos de Respaldo de Datos

- **Criterio de Auditoría**: MSPI Documento Maestro, Sección 12.3.1; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información Sección 6.4.
- **Evidencia Presentada**: Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png), Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png)
- **Evaluación**: Se revisaron los documentos relacionados con las políticas y procedimientos de respaldo de datos. Se encontraron bien documentados, cumpliendo con los estándares establecidos. Las políticas y procedimientos de respaldo de datos están documentados adecuadamente y alineados con las normativas.

5.2. Frecuencia y Tipo de Respaldos Realizados

- **Criterio de Auditoría**: MSPI Documento Maestro, Sección 12.3.2; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4.
- **Evidencia Presentada**: Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png), Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png)
- **Evaluación**: Se verificó la frecuencia y tipos de respaldos realizados. Los registros muestran que se siguen las políticas establecidas, están adecuadamente registrados y cumplen con las políticas establecidas.

5.3. Pruebas de Restauración de Datos

- **Criterio de Auditoría**: MSPI Documento Maestro, Sección 12.3.3; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4.
- **Evidencia Presentada**: Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png), Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png)
- **Evaluación**: Se revisaron las pruebas de restauración de datos, las cuales se realizan periódicamente y están documentadas correctamente.

5.4. Almacenamiento Seguro de Respaldos Fuera del Sitio Principal

- **Criterio de Auditoría**: MSPI Documento Maestro, Sección 12.3.4; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información Sección 6.4.
- **Evidencia Presentada**: Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png), Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png), Los respaldos se almacenan en ubicaciones seguras fuera del sitio principal, según los registros.
- **Evaluación**: Se verificó el almacenamiento seguro de respaldos fuera del sitio principal. Los registros demuestran que los respaldos se almacenan en ubicaciones seguras.

5.5. Procedimientos para la Recuperación de Datos en Caso de Fallo

- **Criterio de Auditoría**: MSPI Documento Maestro, Sección 12.3.5; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.6.
- **Evidencia Presentada**: Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png), Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png)
- **Evaluación**: Se revisaron los procedimientos para la recuperación de datos en caso de fallo, están documentados y han sido probados.

5.6. Auditorías y Revisiones de los Procedimientos de Respaldo

- **Criterio de Auditoría**: MSPI Documento Maestro, Sección 12.3.6; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4.
- **Evidencia Presentada**: Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png), Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png), Pantalla Veeam herramienta que indica si la copia quedó bien para restauración (VEAM.png)
- **Evaluación**: Se verificaron las auditorías y revisiones de los procedimientos de respaldo. Estas se realizan periódicamente y cumplen con los estándares de auditoría establecidos.

6. PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Esta sección de la auditoría se centra en evaluar la efectividad del Plan de Sensibilización y Comunicación de Seguridad de la Información. Se revisaron las políticas, la implementación de programas de sensibilización, la evaluación de la efectividad de estos programas, las campañas de concienciación, la documentación de las sesiones y actividades, la planificación y seguimiento de la capacitación, y la actualización continua del material de sensibilización.

6.1. Políticas de sensibilización y comunicación de seguridad

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Sensibilización y Comunicación Numeral: 6.9.1
- **Evidencia Presentada:** Documentación de la política, Encuesta de seguridad por Daruma, consolidado en encuestas, informe sobre los resultados, actividades de "lunes seguro", "Día de la seguridad", reinducción, alertas de incidentes, acompañamientos, y encuesta de apropiación y réplica de situaciones en alerta.
- **Evaluación:** Se verificó la existencia de las políticas y su cumplimiento con la realización de una encuesta y actividades adicionales de sensibilización y comunicación en seguridad de la información,

6.2. Implementación de programas de sensibilización

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Sensibilización y Comunicación Numeral: 6.9.2

- **Evidencia Presentada:** Establecimiento de políticas y procedimientos para la implementación de programas de sensibilización sobre seguridad de la información. Encuesta de seguridad por Daruma, consolidado en encuestas, informe sobre los resultados, actividades de "Lunes seguro", "Día de la seguridad", reinducción, alertas de incidentes, acompañamientos, y encuesta de apropiación y réplica de situaciones en alerta. Se realizo también Curso de seguridad de Fortinet para todos los funcionarios, banners en los computadores sobre seguridad, eventos de sensibilización de febrero, marzo, mayo y junio, la encuesta y las piezas.
- **Evaluación:** De acuerdo con la evidencia, se implementaron adecuadamente los programas de sensibilización.

6.3. Evaluación de la efectividad de los programas

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Evaluación de Programas de Sensibilización Numeral: 6.9.3
- **Evidencia Presentada:** Encuesta de seguridad realizada en Daruma.
- **Evaluación:** Si bien se evalúa y se presentan los resultados de la encuesta, el documento es muy pobre en análisis y no permite validar la efectividad del programa, por lo tanto, se realiza una **Observación** que permita establecer e implementar una metodología para medir dicha efectividad, analizar y permitir la retroalimentación para la toma de decisiones.

6.4. Campañas de concienciación sobre seguridad de la información

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Sensibilización y Comunicación Numeral: 6.9.4
- **Evidencia Presentada:** Encuesta de seguridad por Daruma, consolidado en encuestas, informe sobre los resultados, actividades de "Lunes seguro", "Día de la seguridad", reinducción, alertas de incidentes, acompañamientos y encuesta de apropiación y réplica de situaciones en alerta.
- **Evaluación:** Se observó la realización de las campañas evidenciando su cumplimiento.

6.5. Documentación de sesiones y actividades de sensibilización

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Documentación de Actividades de Sensibilización Numeral: 6.9.5
- **Evidencia Presentada:** Registro de Sensibilizaciones, informe de uso y apropiación, e informe de phishing.
- **Evaluación:** Aunque se encuentra el informe de uso y apropiación e informe de phishing, no se tienen estadísticas o consolidados de cuántas personas participaron. Se **recomienda** llevar un registro detallado de las participaciones en las actividades de sensibilización, incluyendo estadísticas de asistencia y participación. Esto permitirá un mejor seguimiento y evaluación de la efectividad de las actividades de sensibilización en seguridad.

6.6. Planificación y seguimiento de la capacitación en seguridad

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Planificación y Seguimiento de Capacitación Numeral: 6.9.6

- **Evidencia Presentada:** Plan de seguridad en el portal de la Agencia Plan de acción, gestión de planes y programas, planes institucionales 2024, plan de seguridad, y se encuentra en el capítulo de sensibilización y su seguimiento en Daruma.
- **Evaluación:** Se evidenció cumplimiento del Plan de seguridad en el portal de la Agencia, gestión de planes y programas, planes institucionales 2024, plan de seguridad, y se encuentra en el capítulo de sensibilización.

Como respuesta al informe preliminar la OASTI aceptó la recomendación y aclaró que se incluirá un capítulo de seguridad de la información el cual contendrá la temática relacionada con la gestión de incidentes. Así mismo, la inclusión de control de los requerimientos no funcionales de seguridad para el sistema Ekogui en el Módulo de Comités de Conciliación, que permita asegurar así un seguimiento más efectivo y continuo de las capacitaciones en seguridad.

6.7. Actualización continua del material de sensibilización

- **Criterio de Auditoría:** Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Actualización de Material de Sensibilización Numeral: 6.9.7
- **Evidencia Presentada:** Se presentan las carpetas en el sharepoint con las sesiones realizadas
- **Evaluación:** Se evidencio que se dan charlas de actualización y se actualizan de acuerdo con el plan de sensibilización, sin embargo, no hay documentación, ni versionamiento del material pedagógico. Por lo cual se recomendó llevar un control de dichos materiales Revisión periódica de su actualización.

Sobre el particular, el área no aceptó la Observación en razón a que la OASTI anualmente presenta un plan de Seguridad y Privacidad de la información que contine un ítem relacionado con la sensibilización y los contenidos no se repiten. Los planes se pueden consultar en los siguientes links:

2022: https://www.defensajuridica.gov.co/gestion/Planes-Programas-Proyectos/planes_institucionales/Documents/2022/Plan_de_Seguridad_y_Privacidad_de_la_Informacion.pdf

2023: https://www.defensajuridica.gov.co/gestion/Planes-Programas-Proyectos/planes_institucionales/Documents/2023/11_Plan_de_Tratamiento_de_Riesgos_de_Seguridad_y_Privacidad_de_la_Informacion_300123.pdf

2024: https://www.defensajuridica.gov.co/gestion/Planes-Programas-Proyectos/planes_institucionales/Documents/2024/12_Plan_Seguridad_Privacidad_Informacion_2024.pdf

A su vez, manifiesta el área auditada que, *"hay temáticas que por su reincidencia se debe mantener la sensibilización en dichos temas como por ejemplo phishing, ransomware, suplantación de identidad, contraseñas robustas, entre otras"*-

De acuerdo con la evidencia presentada, la OCI deja como sugerencia llevar control de los registros del material pedagógico desarrollado.

7. CONTRATOS CON TERCEROS

Dentro de la auditoría desarrollada se revisaron 14 contratos con terceros relacionados con TI, para evaluar el cumplimiento de las políticas y procedimientos establecidos para la gestión y supervisión de estos, encontrando que existen 2 de proveedores y 12 de prestación de servicios profesionales, principalmente con enfoque en desarrollo de software In-House, como se evidencia a continuación:

Tabla 1. Contratos

NOMBRE CONTRATISTA	No. ITEM PAA	No. EXPEDIENTE ORFEO	NATURALEZA DEL CONTRATISTA	TIPO DE CONTRATO	MODALIDAD DE CONTRATACIÓN	OBJETO
CLAUDIA MILENA RODRIGUEZ ALVAREZ	80	2024101080-1000001E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para apoyar la Oficina Asesora de Planeación en el cumplimiento de los requisitos establecidos en el Marco de Referencia de Arquitectura Empresarial del Estado v 3.0 en la ANDJE.
CAMILO ANDRÉS DORIA VARGAS	57	2024400080-1000001E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para análisis, registro y validación de información de procesos y conciliaciones en el Sistema eKOGUI, de acuerdo con las piezas procesales, así como la consulta Nacional Unificada de Rama Judicial.
CLAUDIA MARCELA PEÑA HERNANDEZ	113	2024110080-1000002E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para la migración y calidad de datos de eKOGUI.
SEBASTIAN BATISTA BARBOSA	58	2024400080-1000002E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para análisis, registro y validación de información de procesos y conciliaciones en el Sistema eKOGUI, de acuerdo con las piezas procesales, así como la consulta Nacional Unificada de Rama Judicial.
SOLANYE GUERRERO FUNEME	110	2024110080-1000004E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para revisión de flujos de procesos y pruebas para la operación del eKOGUI.
LILIANA MARITZA URUEÑA RODRÍGUEZ	111	2024110080-1000003E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para revisión de flujos de procesos y pruebas para la operación del eKOGUI.
GIGLIOLA ESMERALDA MONTAÑEZ MURILLO	114	2024110080-1000006E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para apoyar la articulación de los roles de pruebas funcionales para la evolución y transformación del e-KOGUI.
HARDY DEIMONT NIÑO VELASQUEZ	83	2024110080-1000001E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para acompañar a la Oficina de Tecnologías de la Información en el desarrollo de las nuevas funcionalidades en los portales o cualquier otra aplicación que permita tener contacto con los grupos de interés de la ANDJE.
ANGELA MARIA FRANCO PEREZ	112	2024110080-1000005E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales como analista de bodega de datos del Sistema e-KOGUI.

NOMBRE CONTRATISTA	No. ITEM PAA	No. EXPEDIENTE ORFEO	NATURALEZA DEL CONTRATISTA	TIPO DE CONTRATO	MODALIDAD DE CONTRATACIÓN	OBJETO
JUAN SEBASTIAN CASTILLO BAYONA	59	2024400080-1000003E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para análisis, registro y validación de información de procesos y conciliaciones en el Sistema eKOGUI, de acuerdo con las piezas procesales, así como la consulta Nacional Unificada de Rama Judicial.
COMPUTEL SYSMTEM SAS	94	2024110080-3000001E	PERSONA JURÍDICA	CONTRATO DE LICENCIAMIENTO	SELECCIÓN ABREVIADA POR SUBASTA INVERSA	Renovación de soporte y garantía de equipo de infraestructura.
SANTIAGO CORTES OCAÑA	92	2024400080-1000007E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para el acompañamiento a la Dirección de Gestión de la Información para la definición de soluciones de inteligencia artificial y/o iniciativas de inteligencia de negocios, teniendo como base los datos contenidos en los sistemas misionales de la Entidad.
CAMERFIRMA COLOMBIA S.A.S	86	2024110080-6000001E	PERSONA JURÍDICA	PRESTACIÓN DE SERVICIOS PROFESIONALES	MÍNIMA CUANTÍA	Renovación y compra de certificados digitales de la ANDJE.
FREDY GEOBANY ZEA RODRÍGUEZ		2024110080-1000007E	PERSONA NATURAL	PRESTACIÓN DE SERVICIOS PROFESIONALES	DIRECTA	Prestación de servicios profesionales para acompañar a la OASTI en el desarrollo de las nuevas funcionalidades en los portales o cualquier otra aplicación que permita tener contacto con los grupos de interés de la ANDJE.

7.1. Evaluación de contratos con terceros relacionados con TI

- **Criterio de Auditoría**: "Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Evaluación de Contratos Numeral: 7.10.1: Descripción: Establecimiento de políticas y procedimientos para la evaluación de contratos con terceros. Controles: Auditorías de Terceros: Implementación de auditorías de seguridad a los terceros contratados."
- **Evidencia Presentada**: Contratos de Terceros, Informes de Auditoría de Terceros, Evaluaciones de Contratos
- **Evaluación**: Evaluaciones y auditorías realizadas según lo requerido.

7.2. Cumplimiento de políticas de seguridad por parte de terceros

- **Criterio de Auditoría**: "Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Cumplimiento de Políticas de Seguridad Numeral: 7.10.2: Descripción: Se deben establecer políticas y procedimientos claros para asegurar el cumplimiento de políticas de seguridad por parte de terceros. Controles: Auditorías de Cumplimiento: Realización de auditorías periódicas de cumplimiento de seguridad a terceros."
- **Evidencia Presentada**: Políticas de Seguridad de Terceros, Informes de Auditoría de Terceros, Registros de Cumplimiento, Se menciona la necesidad de políticas de seguridad como parte de la arquitectura de referencia de sistemas de información y seguridad. Así "Apoyar a la Agencia en la definición, orientación y actualización de las arquitecturas de referencia de sistemas de información, seguridad y datos"(Estudios Previos contrato MRAE).

- **Evaluación**: Se evidenciaron las políticas de seguridad implementadas y auditorías realizadas, a su vez, en los contratos se encontraron cláusulas de confidencialidad.

7.3. Gestión de accesos de terceros a la infraestructura TI

- **Criterio de Auditoría**: "Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Gestión de Accesos Numeral: 7.10.3: Descripción: Se deben establecer políticas y procedimientos claros para la gestión de accesos de terceros a la infraestructura TI. Controles: Control de Accesos: Implementación de controles de acceso para terceros."
- **Evidencia Presentada**: Se evidenciaron Registros de Acceso de Terceros, Informes de Auditoría de Accesos, Planes de Gestión de Accesos. Se observó que en el centro de datos hay seguridad de acceso físico. La definición y orientación de las arquitecturas de referencia implican la asignación de roles y responsabilidades, así como Controles de Acceso y Autenticación. Así: "Brindar acompañamiento técnico y especializado a la Agencia Nacional de Defensa Jurídica del Estado en la implementación y adopción del Marco de Referencia de Arquitectura empresarial versión 3.0" y más adelante dice "Apoyar a la Agencia en la definición, orientación y actualización de las arquitecturas de referencia de sistemas de información, seguridad y datos"(Estudios Previos Contrato MRAE).
- **Evaluación**: una vez revisada la evidencia se encontró que los controles de acceso de terceros esta implementados debidamente.

7.4. Procedimientos de evaluación y selección de proveedores

- **Criterio de Auditoría**: "Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Selección de Proveedores Numeral: 7.10.4: Descripción: Se deben establecer políticas y procedimientos claros para la evaluación y selección de proveedores. Controles: Evaluación de Proveedores: Realización de evaluaciones periódicas de los proveedores."
- **Evidencia Presentada**: Procedimientos de Evaluación de Proveedores, Informes de Selección, Registros de Evaluación de Proveedores. Se verifico SECOP y expedientes en ORFEO para revisión de los contratos existentes y se verificaron las cláusulas de seguridad y confidencialidad en los contratos tanto de Prestación de Servicios Profesionales como de Proveedores de acuerdo con del procedimiento de Gestión Contractual.
- **Evaluación**: una vez revisada la evidencia se encontró que las evaluaciones y procedimientos de selección realizados debidamente de acuerdo con los procedimientos documentados.

7.5. Monitoreo y revisión del desempeño de terceros

- **Criterio de Auditoría**: "-Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Monitoreo de Desempeño Numeral: 7.10.5: Descripción: Se deben establecer políticas y procedimientos claros para el monitoreo y revisión del desempeño de terceros. Controles: Monitoreo Continuo: Implementación de un sistema de monitoreo continuo del desempeño de terceros."
- **Evidencia Presentada**: Informes de Monitoreo, Informes de Auditoría de Desempeño, Registros de Seguimiento Secop y Orfeo
- **Evaluación**: Se evidenció que el monitoreo y auditorías de desempeño son realizados según lo requerido.

7.6. Gestión de riesgos asociados a proveedores externos

- **Criterio de Auditoría**: "Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Gestión de Riesgos Numeral: 7.10.6: Descripción: Se deben establecer políticas y procedimientos claros para la gestión de riesgos asociados a proveedores externos. Controles: Evaluación de Riesgos: Realización de evaluaciones de riesgos periódicas."
- **Evidencia Presentada**: Informes de Evaluación de Riesgos, Planes de Mitigación, Registros de Seguimiento matriz de riesgos de gestión contractual.
- **Evaluación**: Evaluaciones de riesgos y planes de mitigación documentados, no obstante, no se menciona explícitamente, la gestión de riesgos que es inherente a la implementación del MRAE. Así: "Apoyar y coordinar la implementación del procedimiento de diseño, gestión y gobierno de la Arquitectura Empresarial en la Agencia Nacional de Defensa Jurídica del Estado"(Estudios Previos Contrato MRAE). En los contratos de Prestación de Servicios Profesionales y de Proveedores se encontraron cláusulas de confidencialidad, por lo tanto, se evidenció cumplimiento.

7.7. Procedimientos para la terminación de contratos con terceros

- **Criterio de Auditoría**: "Política de Seguridad y Privacidad de la Información (G8) Sección 7.10: Terminación de Contratos Numeral: 7.10.7: Descripción: Se deben establecer políticas y procedimientos claros para la terminación de contratos con terceros. Controles: Procedimientos de Terminación: Implementación de procedimientos claros para la terminación de contratos."
- **Evidencia Presentada**: Procedimientos de Terminación de Contratos, Registros de Finalización, Informes de Auditoría de Terminación
- **Evaluación:** Se evidenció en ORFEO paz y salvo y liquidación de los contratos, se da visto bueno para personas naturales, por lo que se cumple con los procedimientos establecidos

7.8. Contratación del Modelo de Referencia Arquitectura Empresarial

Se incluyó una revisión a la contratación del Modelo de referencia de Arquitectura Empresarial por cuanto este debe estar implementado al 100% al 31 de Julio de 2024 con el objetivo de identificar áreas de refuerzo

7.8.1. Auditoría y Monitoreo

- **Referencia**: "Ejecutar actividades de uso y apropiación en las áreas de la Agencia Nacional de Defensa Jurídica del Estado, sobre el marco de referencia de arquitectura empresarial versión 3.0 y la práctica de Arquitectura Empresarial"(Estudios Previos Contrato MRAE).
- **Evidencia Presentada**: Sí. Aunque no se menciona explícitamente, la auditoría y el monitoreo son componentes esenciales de la gestión de la arquitectura empresarial. El tema de seguridad está a cargo del ingeniero Oficial de Seguridad y se recomienda incorporar al documento del Modelo de Arquitectura Empresarial.
  Se retira la recomendación por cuanto no se encuentra incluido en el contrato

7.8.2. Gestión de Incidentes

- **Referencia**: No encontrado específicamente en los estudios previos. Se tiene gestión de incidentes a cargo del Oficial de Seguridad
- **Evidencia Presentada**: No explícitamente mencionado: Necesita confirmación específica en los informes y políticas internas de seguridad. El tema seguridad está a cargo del ingeniero Oficial de Seguridad y se recomienda incorporar al documento del Modelo de Arquitectura Empresarial.

7.8.3. Desarrollo Seguro

- **Referencia**: "Apoyar a la Agencia en la definición, orientación y actualización de las arquitecturas de referencia de sistemas de información, seguridad y datos"(Estudios Previos)
- **Evidencia Presentada:** Forma parte de la actualización y orientación de las arquitecturas de referencia. Las pruebas de software que realizan en los contratos señalados son funcionales, las pruebas de seguridad se realizan por medio de la metodología, recursos y herramientas del **OWASP** (Open Web Aplicación Security Project), por parte de la empresa COEM – Controles Empresariales para 2024, en la orden de compra BID 127948 en ejecución, sin embargo, adolece de pruebas de Software para los requerimientos no funcionales, por lo cual se **recomienda** incluir en la siguiente iteración especialmente para el módulo de comités de conciliación del sistema Ekogui.
- Se retira la recomendación por cuanto no se encuentra incluido en el contrato

7.8.4. Protección de Datos

- **Referencia**: "Apoyar a la Agencia en la definición, orientación y actualización de las arquitecturas de referencia de sistemas de información, seguridad y datos"(Estudios Previos)
- **Evidencia Presentada**: Es parte de la arquitectura de referencia de seguridad.

7.8.5. Resiliencia y Recuperación ante Desastres

- **Referencia**: No encontrado específicamente en los estudios previos.
- **Evidencia Presentada**: No explícitamente mencionado: Necesita confirmación específica en los informes y políticas internas de seguridad.
  Sin recomendación por cuanto no se encuentra incluido en el contrato

7.8.6. Cumplimiento MRAE Modelo de referencia de Arquitectura Empresarial frente a temas de seguridad

Se realizó una evaluación de la inclusión de los componentes del MRAE en la contratación para su implementación, como se muestre a continuación:

Tabla 2.

Componente	Tipo de Anotación	Observaciones
Políticas de Seguridad	Ninguna	Mencionado en la definición y orientación de las arquitecturas de referencia de seguridad (Estudios Previos).
Roles y Responsabilidades	Ninguna	Implícitamente incluido en la implementación y adopción del MRAE (Estudios Previos).
Gestión de Riesgos	Ninguna	Implícitamente incluido en la gestión y gobierno de la arquitectura empresarial (Estudios Previos).
Controles de Acceso y Autenticación	Recomendación	Incluido en la arquitectura de referencia de seguridad (Estudios Previos). Se recomienda la inclusión de requerimientos no funcionales de seguridad para el sistema Ekogui, especialmente en el módulo de Comités de Conciliación. En los contratos para desarrollo ya sea por fábrica de Software o desarrollo In House.
Auditoría y Monitoreo	Ninguna	Implícitamente incluido en la práctica de arquitectura empresarial (Estudios Previos).
Gestión de Incidentes	Observación	No se menciona explícitamente, pero está a cargo de la Agencia en el contrato del Oficial de Seguridad. Se recomienda incluir formalmente en el MRAE
Desarrollo Seguro	Ninguna	Implícitamente incluido en la práctica de arquitectura empresarial (Estudios Previos).

8. FURAG

La auditoría incluyó la revisión del Formulario Único de Reporte y Avance de la Gestión (FURAG) correspondiente al año 2023, con el objetivo de verificar el correcto diligenciamiento y la disponibilidad de los soportes respectivos para cada pregunta del formulario, en relación con el tema auditado, a saber:

- **Criterio de Auditoria:** Correcto Diligenciamiento del Furag 2023.
- **Evidencias Presentadas:** Se presentaron evidencias para cada pregunta se pueden consultar en *https://defensajuridica.sharepoint.com/sites/OASTI/Documentos%20compartidos/Forms/AllItems.aspx?ct=1721157646835&or=Teams%2DHL&ga=1&LOF=1&id=%2Fsites%2FOASTI%2FDocumentos%20compartidos%2FGeneral%2F2024%2FFURAG&viewid=616555f4%2Dbdf3%2D4a0a%2D9df4%2Dc37168815544*
- **Evaluación:** se revisó el FURAG 2023 diligenciado y se encontró que fue alimentado de manera oportuna, correcta y se encuentran evidencias adecuadas para cada pregunta.

C. Resumen Observaciones y Recomendaciones

1. Observaciones

Clasificación de la Información según su Criticidad (Sección B, Numeral 2.2)

*"Se observa que el 'Módulo de Comités de Conciliación' en el sistema eKOGUI gestiona información clasificada y reservada ingresada por entidades públicas. Si bien la responsabilidad inicial de clasificar y advertir sobre el carácter reservado de la información recae en las entidades que la aportan, la **Agencia Nacional de Defensa Jurídica del Estado**, como custodio de la información registrada en el sistema eKOGUI y conforme a lo estipulado en la Ley 1712 de 2014 Art 18 , 19 y parágrafo y el Decreto 1081 de 2015 en sus artículos 2.1.1.4.3.1, 2.1.1.4.3.2 y 2.1.1.4.3.3 del Decreto 1081 de 2015, tiene la obligación de identificar, clasificar y gestionar adecuadamente dicha información.*

*A su vez, la OCI recomienda tener en cuenta de parte de la OASTI, que en su rol de oficial de seguridad de la información y de protección de datos personales, el jefe de la Oficina Asesora de Sistemas y Tecnologías de la Información (OASTI) debe establecer mecanismos efectivos para la clasificación y valoración de los activos de información crítica. Así mismo en caso de brechas de seguridad que comprometan esta información, la Agencia debe notificar a la entidad propietaria de la información afectada, en cumplimiento de las normativas de protección de datos y seguridad de la información vigentes, como el **Decreto 1377 de 2013** y la **Ley 1581 de 2012**. Por otra parte, se recomienda que la Entidad implemente exclusiones de responsabilidad y advertencias legales dirigidas a las entidades que ingresan información clasificada y reservada en el sistema eKOGUI, para prevenir filtraciones y posibles consecuencias legales."*

2. *Recomendaciones*

Gestión de Cuentas de Usuario (Sección B, Numeral 1.2)

Descripción: Se evidenció cumplimiento a través de las políticas en los sistemas Ekogui, Daruma, Orfeo y Mercurio. Sin embargo, los criterios de la Política de Seguridad y Privacidad de la Información (Sección 5.4,) sugieren la implementación de controles adicionales de autenticación. La falta de estos controles adicionales se debe a la presunta priorización de otras medidas de seguridad. Mejorar estos controles podría incrementar la seguridad de las cuentas de usuario y reducir el riesgo de accesos no autorizados.

Implementación de Controles de Protección Adecuados (Sección B, Numeral 2.3)

Descripción: Se evidenciaron controles en el mapa de riesgos, pero no se visualizan todos los riesgos inherentes con su respectivo tratamiento. Los criterios según la Política de Seguridad y Privacidad de la Información (Sección 6.3, Numeral 6.3.1) requieren la visualización completa de todos los riesgos con su tratamiento. La presunta causa de esta deficiencia es la limitación en la herramienta Daruma utilizada para la gestión de riesgos. Esto puede llevar a una gestión inadecuada de los riesgos, comprometiendo la efectividad de los controles de seguridad.

Procedimientos para la Eliminación Segura de Activos (Sección B, Numeral 2.5)

Descripción: Se recomienda actualizar el procedimiento para el borrado seguro en la nube. La evidencia indica que los procedimientos actuales no cumplen con los criterios establecidos en la Política de Seguridad y Privacidad de la Información (Sección 6.5, Numeral 6.5.1). La causa de esta brecha es la presunta falta de actualización en los protocolos de eliminación segura. Las consecuencias de no abordar esta brecha incluyen la posibilidad que queden copias o archivos residuales en los equipos, comprometiendo la confidencialidad de la información de la entidad.

Gestión de Incidentes (Sección B, Numeral 3.1)

Descripción: Aunque las políticas y procedimientos están documentados, se carece de registros específicos que evidencien la aplicación práctica de estos en incidentes reales. Los criterios establecidos en la Política de Seguridad y Privacidad de la Información (Sección 6.6, Numeral 6.6.1) requieren un registro detallado de los incidentes de seguridad. La causa principal es la presunta falta de implementación de un sistema de seguimiento adecuado. Las consecuencias potenciales incluyen una respuesta ineficaz a incidentes de seguridad y la incapacidad de demostrar el cumplimiento de los procedimientos de seguridad.

Registro y seguimiento de incidentes de seguridad (Sección B, Numeral 3.2)

Descripción: *Después de analizar los argumentos del auditado, la OCI ha decidido retirar la recomendación de "Actualizar la página de incidentes de la Agencia con la información de Incidentes 2024". No obstante, se sugiere precisar en el procedimiento las definiciones de "Evento" e "Incidente", manteniendo coherencia entre estas y el indicador 05-GTI-24 #268 en Daruma. Además, se recomienda establecer las excepciones y declaraciones de aplicabilidad en caso de ser necesario para asegurar que todos los incidentes sean registrados y gestionados adecuadamente. El área auditada ha aceptado la recomendación y verificará el Procedimiento GTI-P-05 para la gestión de incidentes de seguridad de la información.*

Análisis de causa raíz y acciones correctivas (Sección B, Numeral 3.3)

Recomendación: El área auditada ha aceptado la recomendación y se ha comprometido a incluir un capítulo de seguridad de la información que contenga la temática relacionada con la gestión de incidentes. Además, se evaluará la inclusión como control de los requerimientos no funcionales de seguridad para el sistema Ekogui en el Módulo de Comités de Conciliación, asegurando una gestión más eficaz y robusta de los incidentes de seguridad.

Pruebas y simulacros de respuesta a incidentes (Sección B, Numeral 3.4)

Descripción: *Aunque se realizaron simulacros de respuesta a incidentes, no se ha difundido adecuadamente la información sobre los resultados y efectividad de estos. Los criterios según la Política de Seguridad y Privacidad de la Información (Sección 6.6, Numeral 6.6.1) exigen la documentación y comunicación de los resultados de dichos simulacros. La presunta falta de difusión se debe a una deficiente gestión en la comunicación interna. Esto puede llevar a una respuesta inadecuada ante incidentes reales, comprometiendo la seguridad y eficiencia operativa.*

Documentación de sesiones y actividades de sensibilización (Sección B, Numeral 6.5)

Recomendación: Llevar un registro detallado de las participaciones en las actividades de sensibilización, incluyendo estadísticas de asistencia y participación. Esto permitirá un mejor seguimiento y evaluación de la efectividad de las actividades de sensibilización en seguridad. La OASTI no respondió a esta recomendación en el informe preliminar, pero es crucial para garantizar la implementación efectiva y la mejora continua de las políticas de seguridad y privacidad de la información.

Planificación y seguimiento de la capacitación en seguridad (Sección B, Numeral 6.6)

Recomendación: Actualizar el plan de acción para incluir un capítulo específico sobre seguridad de la información que abarque la gestión de incidentes y la planificación de la capacitación en seguridad. El área auditada ha aceptado esta recomendación y ha indicado que se incluirá este capítulo en el plan de seguridad de la información, además de evaluar la inclusión de controles de los requerimientos no funcionales de seguridad para el sistema Ekogui en el Módulo de Comités de Conciliación, asegurando así un seguimiento más efectivo y continuo de las capacitaciones en seguridad.

D. Conclusiones

La auditoría realizada al Plan de Seguridad y Privacidad de la Información de la Agencia Nacional de Defensa Jurídica del Estado ha evidenciado un compromiso significativo con la seguridad y privacidad de la información, cumpliendo en gran medida con los estándares establecidos. Sin embargo, se identificaron aspectos que requieren atención y mejoras específicas para garantizar la efectividad continua del modelo de seguridad.

En **gestión de la información crítica** (Sección B, Numeral 2.2), se observó una debilidad en la clasificación y valoración de activos de información, especialmente en el "Módulo de Comités de Conciliación" del Sistema Ekogui. Es crucial que se implementen medidas correctivas para garantizar la protección adecuada de la información reservada, conforme a las políticas establecidas.

En cuanto a la **gestión de incidentes** (Sección B, Numerales 3.1 y 3.2), aunque la documentación de políticas y procedimientos está disponible, se identificó una falta de registros específicos que evidencien la aplicación práctica en incidentes reales. Es fundamental establecer un sistema de seguimiento que asegure la correcta gestión y registro de todos los incidentes de seguridad, así como definir claramente las categorías de "Evento" e "Incidente" para mantener la coherencia en los reportes.

En el ámbito de la **sensibilización y capacitación en seguridad de la información** (Sección B, Numerales 6.5 y 6.9), se destacó la necesidad de llevar un registro detallado de las participaciones en las actividades de sensibilización, incluyendo estadísticas de asistencia y participación, para mejorar el seguimiento y la evaluación de la efectividad de estas actividades.

En cuanto a la **contratación del Modelo de Referencia de Arquitectura Empresarial** (Sección B, Numeral 7.8), se recomendó incluir requerimientos no funcionales de seguridad para activos de información críticos y formalizar la gestión de incidentes en el Modelo de Arquitectura Empresarial para asegurar una implementación robusta y segura.

Finalmente, en la **implementación de controles de protección** (Sección B, Numeral 2.3), se observó que no todos los riesgos inherentes están siendo visualizados con su respectivo tratamiento, lo cual compromete la efectividad de los controles de seguridad. Es necesario asegurar que todos los riesgos se gestionen adecuadamente para mantener la integridad y seguridad de la información.

En conclusión, aunque la Agencia Nacional de Defensa Jurídica del Estado ha mostrado un cumplimiento adecuado en la mayoría de los aspectos auditados, se debe fortalecer la gestión de la seguridad y privacidad de la información, por lo que la implementación de las recomendaciones propuestas será esencial para asegurar la continuidad y robustez del modelo de seguridad de la Entidad en el futuro.

Para constancia se firma en Bogotá D.C., a los 27 días de enero de 2025.

ADRIANA MILENA HERRERA ABRIL
Jefe de la Oficina de Control Interno
Nota. Los anexos al presente informe hacen parte integral.

Anexo 1. Auditoria al Modelo de Seguridad y Privacidad de la Información

A-P-GTI-MSPI-2024

Este listado condensa todos los documentos examinados que fueron presentados como evidencia durante la auditoría:

1. ***Control de Acceso y Gestión de Usuarios***
    - Política de Gestión de Acceso (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.2, Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Gestión de Acceso Numeral: 5.4.2)
    - Política de Autenticación (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.3, Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Autenticación Numeral: 5.4.3)
    - Política de Gestión de Acceso Privilegiado (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.4, Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Gestión de Acceso Numeral: 5.4.4)
    - Política de Revisión de Accesos (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.5, Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Revisión de Accesos Numeral: 5.4.5)
    - Política de Gestión de Cuentas de Usuario (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.6, Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Gestión de Cuentas de Usuario Numeral: 5.4.6)
    - Política de Monitoreo y Registro de Accesos (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.7, Política de Seguridad y Privacidad de la Información (G8) Sección 5.4: Monitoreo y Registro de Accesos Numeral: 5.4.7)
    - Política de Detección y Respuesta a Accesos No Autorizados (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.5, Política de Seguridad y Privacidad de la Información (G8) Sección 5.5: Detección y Respuesta a Accesos No Autorizados Numeral: 5.5.1)
    - Política de Evaluación de Cumplimiento de Acceso (Manual de Políticas de Gestión y Desempeño Institucional (DE-M-02) Sección 6.4.6, Política de Seguridad y Privacidad de la Información (G8) Sección 5.6: Evaluación de Cumplimiento de Políticas de Acceso Numeral: 5.6.1)

2. ***Gestión de Activos de Información y Clasificación de la Información***
    - Inventario de Activos de Información (Política de Seguridad y Privacidad de la Información (G8), Sección 6.1: Inventario de Activos de Información, Numeral: 6.1.1)
    - Clasificación de Información (Política de Seguridad y Privacidad de la Información (G8), Sección 6.2: Clasificación de Información, Numeral: 6.2.1)
    - Controles de Protección (Política de Seguridad y Privacidad de la Información (G8), Sección 6.3: Controles de Protección, Numeral: 6.3.1)
    - Gestión de Activos de Información (Política de Seguridad y Privacidad de la Información (G8), Sección 6.4: Gestión de Activos de Información, Numeral: 6.4.1)

- Eliminación Segura de Información (Política de Seguridad y Privacidad de la Información (G8), Sección 6.5: Eliminación Segura de Información, Numeral: 6.5.1)
- Auditorías Periódicas del Inventario de Activos (Política de Seguridad y Privacidad de la Información (G8), Sección 6.4: Gestión de Activos de Información, Numeral: 6.4.2)

3. Seguridad Operativa y Gestión de Incidentes

- Gestión de Incidentes de Seguridad (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Incidentes de Seguridad, Numeral: 6.6.1)
- Registro y Seguimiento de Incidentes (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Incidentes de Seguridad, Numeral: 6.6.2)
- Análisis de Causa Raíz y Acciones Correctivas (Política de Seguridad y Privacidad de la Información (G8), Sección 8.3: Análisis de Causa Raíz y Acciones Correctivas, Numeral: 8.3.1)
- Pruebas y Simulacros de Respuesta a Incidentes (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Pruebas y Simulacros de Respuesta a Incidentes, Numeral: 6.6.1)

4. Gestión de Cambios y Desarrollo de Software Seguro

- Gestión de Cambios (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Cambios, Numeral: 6.6.1)
- Desarrollo de Software Seguro (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Desarrollo de Software Seguro, Numeral: 6.6.1)
- Pruebas de Seguridad en el Software (Política de Seguridad y Privacidad de la Información (G8), Sección 6.7: Pruebas de Seguridad en el Software, Numeral: 6.7.1)
- Gestión de Versiones y Despliegue de Software (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Gestión de Cambios y Desarrollo de Software Seguro, Numeral: 6.6.3)
- Evaluación de Riesgos (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Evaluación de Riesgos, Numeral: 6.6.1)
- Continuidad del Negocio (Política de Seguridad y Privacidad de la Información (G8), Sección 6.6: Continuidad del Negocio, Numeral: 6.6.2)

5. Respaldo y Restauración de Datos

- Políticas y Procedimientos de Respaldo de Datos (MSPI Documento Maestro, Sección 12.3.1; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4)
- Frecuencia y Tipo de Respaldos (MSPI Documento Maestro, Sección 12.3.2; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4)
- Pruebas de Restauración de Datos (MSPI Documento Maestro, Sección 12.3.3; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4)
- Almacenamiento Seguro de Respaldos (MSPI Documento Maestro, Sección 12.3.4; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4)
- Recuperación de Datos en Caso de Fallo (MSPI Documento Maestro, Sección 12.3.5; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.6)

- Auditorías de Respaldo (MSPI Documento Maestro, Sección 12.3.6; GTI-G-06 Guía de Gestión de Respaldo; Política de Seguridad y Privacidad de la Información (G8) Sección 6.4)

6. Plan de Sensibilización y Comunicación de Seguridad de la Información

- Sensibilización y Comunicación (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Sensibilización y Comunicación Numeral: 6.9.1)
- Programas de Sensibilización (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Sensibilización y Comunicación Numeral: 6.9.2)
- Evaluación de Programas de Sensibilización (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Evaluación de Programas de Sensibilización Numeral: 6.9.3)
- Campañas de Concienciación (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Sensibilización y Comunicación Numeral: 6.9.4)
- Documentación de Actividades de Sensibilización (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Documentación de Actividades de Sensibilización Numeral: 6.9.5)
- Planificación y Seguimiento de Capacitación (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Planificación y Seguimiento de Capacitación Numeral: 6.9.6)
- Actualización de Material de Sensibilización (Política de Seguridad y Privacidad de la Información (G8), Sección 6.9: Actualización de Material de Sensibilización Numeral: 6.9.7)

7. Contratos con Terceros

- Evaluación de Contratos (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Evaluación de Contratos Numeral: 7.10.1)
- Cumplimiento de Políticas de Seguridad (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Cumplimiento de Políticas de Seguridad Numeral: 7.10.2)
- Gestión de Accesos (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Gestión de Accesos Numeral: 7.10.3)
- Selección de Proveedores (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Selección de Proveedores Numeral: 7.10.4)
- Monitoreo de Desempeño (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Monitoreo de Desempeño Numeral: 7.10.5)
- Gestión de Riesgos (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Gestión de Riesgos Numeral: 7.10.6)
- Terminación de Contratos (Política de Seguridad y Privacidad de la Información (G8), Sección 7.10: Terminación de Contratos Numeral: 7.10.7)

Anexo 2. Documentos Examinados Presentados como Evidencia
A-P-GTI-MSPI-2024

1. ***Control de Acceso y Gestión de Usuarios***
    - GTI P01: Pasos de creación de usuarios y accesos, por talento humano.
    - Gestión de servicio de TI P01.
    - Guía de gestión de usuarios GTIG10.
    - Logs de autenticación y configuración de doble factor (Log de accesos Pantalla, A nivel aplicativo GLPI).
    - CORREOS_ELCTRONICOS_2023: Gestión de Usuarios.
    - Creación usuarios GLPI 1.
    - Log de accesos: Pantallazo de configuración Ekogui.
    - Procedimientos de respuesta a incidentes (A nivel aplicativo GLPI).

2. ***Gestión de Activos de Información y Clasificación de la Información***
    - GTI-F-05: Matriz de Inventario Clasificación y Publicación de Información.
    - Guía de inventario de activos, clasificación y publicación de información GTI-G-01.
    - GTI-G-03: Guía para la Manipulación de Medios y Borrado Seguro.

3. ***Seguridad Operativa y Gestión de Incidentes***
    - Documentos de políticas y procedimientos documentados.

4. ***Gestión de Cambios y Desarrollo de Software Seguro***
    - GTI-F-10: Solicitud de Cambios RFC.
    - Validación Buzón Factura Electrónica.
    - Validación Buzón Arbitramiento.
    - Validación Buzón Jurisprudencia.
    - Validación Buzón Conciliaciones Nacionales y Territoriales.
    - Cambio de Logos Ekogui1.0 y Ekogui2.0 ([#ARQ-4204] Cambio de Logos Ekogui1.0 y Ekogui2.0.pdf).

5. ***Respaldo y Restauración de Datos***
    - Registro de Copias de Respaldo (4.1 REGISTRO COPIAS RESPALDO.png).
    - Bitácora de Administración y Control de Copias (4.2 BITACORA ADMON y CONTROL COPIAS.png).
    - Veeam herramienta que indica si la copia quedó bien para restauración (VEAM.png).

6. **Plan de Sensibilización y Comunicación de Seguridad de la Información**
    - Encuesta de seguridad por Daruma, consolidado en encuestas, informe sobre los resultados, actividades de "Lunes seguro", "Día de la seguridad", reinducción, alertas de incidentes, acompañamientos, y encuesta de apropiación y réplica de situaciones en alerta.
    - Curso de seguridad de Fortinet para todos los funcionarios, banners en los computadores sobre seguridad, eventos de sensibilización de febrero, marzo, mayo y junio.

- Encuesta realizada en Daruma.
- Registro de Sensibilizaciones, informe de uso y apropiación, e informe de phishing.

7. Contratos con Terceros

- Contratos de Terceros.
- Informes de Auditoría de Terceros.
- Evaluaciones de Contratos.
- Políticas de Seguridad de Terceros.
- Informes de Auditoría de Terceros.
- Registros de Cumplimiento.
- Registros de Acceso de Terceros.
- Informes de Auditoría de Accesos.
- Planes de Gestión de Accesos.
- Procedimientos de Evaluación de Proveedores.
- Informes de Selección.
- Registros de Evaluación de Proveedores.
- Informes de Monitoreo.
- Informes de Auditoría de Desempeño.
- Registros de Seguimiento.
- Informes de Evaluación de Riesgos.
- Planes de Mitigación.
- Registros de Seguimiento.
- Procedimientos de Terminación de Contratos.
- Registros de Finalización.
- Informes de Auditoría de Terminación.

8. FURAG

- Soportes respectivos del FURAG correctamente diligenciado.