## 1. INFORMACIÓN GENERAL

**1.1. ORGANIZACIÓN**

CONSEJO SUPERIOR DE LA JUDICATURA - RAMA JUDICIAL DEL PODER PÚBLICO DE COLOMBIA/CONSEJO SUPERIOR DE LA JUDICATURA

**1.2. SITIO WEB:** www.ramajudicial.gov.co

**1.3. LOCALIZACIÓN DEL SITIO PERMANENTE PRINCIPAL:** Carrera 8 No 12B – 82, Bogotá D.C., Colombia.

**1.3.1 LOCALIZACION DE OTROS SITIOS PERMANENTES INCLUIDOS EN EL CERTIFICADO**

| # Sitios Permanentes adicionales | Número de certificado | Dirección | Localización (ciudad - país) | Actividades del alcance del sistema de gestión, desarrollados en este sitio |
|---|---|---|---|---|
| 1 | SI-CER969331 | Carrera 7 # 27-18 | Bogotá D.C., Colombia | Servicio público de administrar justicia en la Rama Judicial |

**1.4. ALCANCE DE LA CERTIFICACIÓN:**

Gestión tecnológica referente al servicio público de administrar justicia en la Rama Judicial. Declaración de Aplicabilidad DEAJ-BTA-GT-A-F-03 con fecha 06-06-2024.

Technological managament regarding the public service of administering justice in the judicial Branch. Statement of Applicability DEAJ-BTA-GT-A-F-03 dated 06-06-2024.

**1.5. CÓDIGO IAF:** SI - 4

**1.6. REQUISITOS DE SISTEMA DE GESTIÓN**: ISO/IEC 27001:2022 + documentación del sistema de gestión.

**1.7. REPRESENTANTE DE LA ORGANIZACIÓN**

| | |
|---|---|
| Nombre: | Clara Milena Higuera Guio |
| Cargo: | Directora UDAE – Rama Judicial |
| Correo electrónico | chiguerg@cendoj.ramajudicial.gov.co |

**1.8. TIPO DE AUDITORÍA:**

- ☐ **Inicial o de Otorgamiento**
- ☐ **Seguimiento 1**
- ■ **Seguimiento 2**
- ☐ **Renovación**
- ☐ **Renovación (con restauración)**
- ☐ **Renovación (anticipada)**
- ☐ **Renovación (anticipada para unificar ciclos)**
- ☐ **Ampliación**
- ☐ **Reducción**
- ☐ **Auditoria especial (reactivación/extraordinaria)**
- ■ **Actualización**

Es organización multisitio: Si ■ No □

Auditoría combinada: Si □ No ■

Auditoría integrada: Si □ No ■

| 1.9. Tiempo de auditoría | FECHA | Días de auditoría) |
|---|---|---|
| Etapa 1 (Si aplica) | N/A | N/A |
| Preparación de la auditoría y elaboración del plan | 2024-10-15 | 0.5 |
| Auditoria remota | N/A | N/A |
| Auditoría en sitio | 2024-10-28 al 2024-11-01 | 5.0 |

| 1.10. EQUIPO AUDITOR | |
|---|---|
| Auditor Coordinador | OSCAR FERANDO RAMOS BENAVIDES |
| Auditor líder | OSCAR FERANDO RAMOS BENAVIDES |
| Auditor | N/A |
| Experto Técnico | N/A |
| Observador | N/A |

| 1.11. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN | |
|---|---|
| Código asignado por ICONTEC | SI-CER969331 |
| Fecha de aprobación inicial | 2022-12-01 |
| Fecha de próximo vencimiento: | 2025-11-30 |

## 2. OBJETIVOS DE LA AUDITORÍA

2.1. Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión.

2.2. Determinar la capacidad del sistema de gestión para asegurar que la Organización cumple los requisitos legales, reglamentarios y contractuales aplicables en el alcance del sistema de gestión y a la norma de gestión

2.3. Determinar la eficacia del sistema de gestión para asegurar que la Organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados.

2.4. Identificar áreas de mejora potencial del sistema de gestión.

## 3. ACTIVIDADES DESARROLLADAS

3.1. Los criterios de la auditoría incluyen la norma de requisitos de sistema de gestión, la información documentada del sistema de gestión establecida por la organización para cumplir los requisitos de la norma, otros requisitos aplicables que la organización suscriba y documentos de origen externo aplicables.

3.2. El alcance de la auditoría, las unidades organizacionales o procesos auditados se relacionan en el plan de auditoría, que hace parte de este informe.

3.3. La auditoría se realizó por toma de muestra de evidencias de las actividades y resultados de la Organización y por ello tiene asociada la incertidumbre, por no ser posible verificar toda la información documentada.

3.4. Se verificó la capacidad de cumplimiento de los requisitos legales o reglamentarios aplicables en el alcance del sistema de gestión, establecidos mediante su identificación, la planificación de su cumplimiento, la implementación y la verificación por parte de la Organización de su cumplimiento.

3.5. El equipo auditor manejó la información suministrada por la Organización en forma confidencial y la retornó a la Organización, en forma física o eliminó la entregada en otro medio, solicitada antes y durante el proceso de auditoría.

3.6. Al haberse ejecutado la auditoría de acuerdo con lo establecido en el plan de auditoría, se cumplieron los objetivos de ésta.

3.7. ¿Se evidenciaron las acciones tomadas por la Organización para solucionar las áreas de preocupación, reportadas en el informe de la Etapa 1? (Se aplica solo para auditorías iniciales o de otorgamiento):
Si □ No □ NA ■

3.8. Si se aplicó toma de muestra de múltiples sitios, indicar cuáles sitios permanentes se auditaron, en qué fechas: No se realizó toma de muestra pero se auditaron las dos sedes.

3.9. ¿En el caso del Sistema de Gestión auditado están justificados los requisitos no aplicables acordes con lo requerido por el respectivo referencial?
Si ■ No □ NA □

| Control | Descripción | Justificación |
|---|---|---|
| A.8.4 | Acceso al código fuente | La Unidad de Informática no desarrolla software, no cuenta con fábrica de desarrollo, no alquila servicios de desarrollo de manera externa |
| A.8.25 | Ciclo de vida de desarrollo seguro | |
| A.8.26 | Requisitos de seguridad de la información | |
| A.8.27 | Arquitectura de sistemas seguros y principios de ingeniería | |
| A.8.28 | Codificación segura | |
| A.8.29 | Pruebas de seguridad en el desarrollo y la aceptación | |
| A.8.30 | Desarrollo tercerizado | |
| A.8.31 | Separación de los entornos de desarrollo, prueba y producción | |
| A.8.33 | Información de la prueba | |

3.10. ¿Se auditaron actividades en sitios temporales o fuera del sitio de acuerdo al listado de contratos o proyectos entregado por la Organización?:
Si □ No □ NA ■

3.11. ¿Es una auditoría de ampliación o reducción?
Si □ No ■

3.12. ¿En el caso de los esquemas en los que es aplicable el requisito de diseño y desarrollo del producto o servicio? (Por ejemplo, el numeral 8.3, de la norma ISO 9001:2015), este se incluye en el alcance del certificado?:

Si □ No □ NA ■

3.13. ¿Existen requisitos legales para el funcionamiento u operación de la Organización o los proyectos que realiza, por ejemplo, habilitación, registro sanitario, licencia de funcionamiento, licencia de construcción, licencia o permisos ambientales en los que la Organización sea responsable?:
Si □ No ■

3.14. ¿Se evidencian cambios significativos en la Organización, desde la anterior auditoría, por ejemplo, relacionados con alta dirección, estructura organizacional, sitios permanentes bajo el alcance de la certificación, cambios en el alcance de la certificación diferentes a ampliación o reducción, entre otros?
Si ■ No □
En caso afirmativo, cuáles:

La implementación de los requisitos y controles nuevos presentados por la nueva versió de la ISO/IEC 27001:2022, por tanto, además el cambio en la declaración de aplicabilidad codificada como DEAJ-BTA-GT-A-F-03 con fecha 06-06-2024.

¿Debido a los cambios que ha reportado la Organización, se requiere aumentar el tiempo de auditoría de seguimiento?
Si □ No ■

3.15. ¿La organización consideró las cuestiones relativas al cambio climático dentro de la planificación del sistema de gestión?
Si ■ No □ NA □

Documento Plan de Accción de Unidad de Transformación Digital e Informática desde el análisis DOFA, identificando el cambio climático como fortaleza en la medida que está soportado y apoyado desde los diferentes contextos del sistema de gestión ambiental.

3.16. ¿Si la organización realiza actividades del alcance en turnos nocturnos que no pueden ser visitadas en el turno diurno, estas fueron auditadas en esta auditoría?
Si □ No ■ NA □

3.17. ¿Se tienen actividades, productos y servicios declarados en el alcance del certificado que han sido tercerizados con proveedores o contratistas?
Si ■ No □

¿En caso afirmativo, se encontraron controlados los proveedores o contratistas de estas actividades, productos y servicios?
Si ■ No □

En el caso en el cual la organización subcontrate el suministro de actividades, productos y servicios que hacen parte del alcance certificado, relaciónelos en la siguiente tabla:

| Actividades, productos y servicios incluidos en el alcance de certificación que son subcontratados: | Proveedor/Contratista: | Requisito legal para el funcionamiento u operación (en caso de ser aplicable) |
|---|---|---|
| Nube Privada | IFX Networks<br>Microsoft Azure | N/A |
| Servicio de ciberseguridad y servicios de SOC | Earns & Young | N/A |

3.18. ¿Se presentaron, durante la auditoría, cambios que hayan impedido cumplir con el plan de auditoría inicialmente acordado con la Organización?
Si □ No ■

3.19. ¿Existen aspectos o resultados significativos de esta auditoría, que incidan en el programa de auditoría del ciclo de certificación?

Si □ No ■

3.20. ¿Quedaron puntos no resueltos en los casos en los cuales se presentaron diferencias de opinión sobre las NC identificadas durante la auditoría?
Si □ No ■ NA □

3.21. ¿Aplica reactivación para este servicio?
Si □ No ■ NA □

3.22. Se verificó si la Organización implementó o no, el plan de acción establecido para solucionar las no conformidades menores pendientes de la auditoría anterior de ICONTEC y si fueron eficaces. N/A

| NC | Descripción de la no conformidad (se relaciona el numeral de la norma y la evidencia del incumplimiento) | Evidencia obtenida que soporta la solución | ¿Fue eficaz la acción? Si/No |
|---|---|---|---|
| 1 | A.17.1.3 - No se han realizado pruebas de continuidad que contemplen escenarios de falla completa de la aplicación “EFINÓMINA”. | Se identificó la definición de plan de acción para la realización de las pruebas de la aplicación “EFINOMINA”. | SI |

| | | | |
|---|---|---|---|
| | | Se evidenciaron los resultados de la prueba de continuidad de la aplicación “EFINOMINA”, siendo estos relevantes y con la toma de las conclusiones y lecciones aprendidas | |

3.23. Esta auditoria NO fue testificada por el Organismo de acreditación

## 4. HALLAZGOS DE LA AUDITORÍA

Como resultado de la auditoría, el equipo auditor declara la conformidad y eficacia del sistema de gestión auditado basados en el muestreo realizado. A continuación, se hace relación de los hallazgos de auditoría.

**4.1 Hallazgos que apoyan la conformidad del sistema de gestión con los requisitos.**

- La inclusión de los Servicios digitales como objetivo del plan sectorial de desarrollo en la medida que se enfoca en acceso a éstos y la implementación de transformación digital (internet y soporte)
- El completo ejercicio de análisis del cambio climático como factor de organización, en la medida que permitió establecer estrategias y planes de acción para una estrecha alineación con el SGSI.
- La implementación y uso de Intune para los propósitos de operación de la seguridad lógica y en general en las soluciones en la nube, permitiendo además la administración de las aplicaciones e implementación automatizada de directivas y de la integración con los dispositivos finales.
- La segregación de funciones que permte establecer y asegurar la asignación de los permisos a los usuarios en los sistemas de información.
- El uso de hubspot por lo que permite la gestión de la información de los clientes y bajo el control de actividades de los usuarios y bajo la generación de registros de auditoría., por tanto, permite trazabilidad de la información.
- La inclusión de cláusula de medidas de seguridad digital que debe conocer y cumplir los teletrabajador.
- EL uso de fimas con certificados digitales por lo que asegura un uso autoizado.
- La realización de sesiones de trabajo para consolidar los resultados de los análisis de riesgos de seguridad de la información y su aceptación por arte de los directores de todas las divisiones operativas.
- El soporte tecnológico de registro, análisis de eventos de seguridad y ciberseguridad obtenido por parte del proveedor, por tanto permite mantener análisis sobre los estados de protección de la infraestructura tecnológica, bien en la nube, como on premise.
- La seguridad física y ambiental dispuesta en el Datacenter alojado en la zona del CAN, por lo que asegra siempre accesos autorizados y la disponibilidad de los servicios tecnológicos.
- La definición del plan estructurado para la realización de las pruebas de restauración de información, con alto nivel de detalle para asegurar el resultado de la prueba (minutograma), por tanto, la disponibilidad de la información.
- El uso de herramienta Vertiv (TerippLite) en la medida que permite realizar monitoreos en línea del estado de la temperatura y humedad
- La gestión de configuración bajo las prácticas de SISCONTROL, en la medida que define las mejores prácticas para las líneas base de configuración

- El apoyo con el que se cuenta para los propósitos de ciberdefensa y el SOC desde un tercero, las herramientas que son dispuestas para el servicio y el soporte por parte de proveedor, permiten monitoreo permanente.
- La definición de las matrices de información de configuración de seguridad de líneas base de componentes TI, perite mantener estándares y fuente de información para las revisiones periódicas.
- El control de asignación de responsabilidad en cuanto a la aplicación de controles con propósitos de remediación de las vulnerabilidades técnicas ientificadas en los informes correspondientes.

**4.2 Oportunidades de mejora**

- Ampliar y fortalecer el ejercicio de identificación de la información de cambios en las necesidades y expectativas de las partes interesadas pertinentes de SGSI.
- Fortalecer la identificación con datos exactos de los estados de avance de los planes de tratamiento de los riesgos, aquellos que se identifican en zona fuera de la aceptación de los riesgos.
- Fortalecer el ejercicio y estrategias de recolección adicionales de información de retroalimentación pertinente de seguridad de la información de las partes interesadas identificadas.
- Incluir en el programa de auditoría la planeación de las auditorías de seguridad de la información a procesos de apoyo al SGSI tales como tal, gestión humana, gestión de compras, áreas jurídicas, aquellas áreas que tienen ciertas responsabilidades sobre el SGSI.
- Acercarse al conocimiento de la ISO/IEC 27005 de gestión de riesgos para conocer y adoptar las propuestas a calatolagción de los lod diferentes tipos de activos de información.
- Revisar la identificación de los riesgos de manera que determinen los efectos sobre los cuales los activos de información podrían afectar.
- Incluir el mensaje de responsabilidad de protección de datos privilegiados en el documento “Registro Instrucciones a seguir para el ingreso al cuarto técnico del Piso 10”, de modo tal, se asegure o evite reclamaciones a la organización por uso inadecuado de información sensible como la firma.
- Conocer acerca de la norma ISO/IEC 27035 de manera permita ampliar escenarios de operación y control posibles de los potenciales incidente de seguridad de la información.
- Instalar señalización de condiciones de seguridad de la información para el trabajo en áreas seguras, de mod tal se esté atento a cualquier incumplimiento de ellas.

## 5. INFORMACIÓN RELACIONADA CON EL DESEMPEÑO Y LA EFICACIA DEL SISTEMA DE GESTIÓN

### 5.1. Análisis de la eficacia del sistema de gestión certificado

5.1.1. Incluir las reclamaciones o quejas válidas del cliente en los sistemas de gestión que aplique durante el último año.

| Principales quejas o reclamaciones recurrentes | Principal causa | Acciones tomadas |
|---|---|---|
| N/A | N/A | N/A |

5.1.2. Incluir la ocurrencia de incidentes (accidentes o emergencias) en los sistemas de gestión que aplique y explique brevemente cómo fueron tratados:

Un incidente de seguridad de la información relacionado con un ataque de defacement sobre la página web de la Entidad, el cual que fue atendido de acuerdo al procedimiento de gestión de incidentes de

seguridad de la información, por tanto, mitigo el impacto al mínimo posible dado que la contención y solución se dio en un mínimo tiempo.

5.1.3. En los casos que aplique verificar que la Organización haya informado a ICONTEC durante los plazos especificados en el Reglamento R-PS-0007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN, eventos que hayan afectado el desempeño del sistema de gestión certificado, relacionados con el alcance de certificación que sean de conocimiento público. El auditor verificará las acciones pertinentes tomadas por la Organización para evitar su recurrencia y describirá brevemente cómo fueron atendidas. N/A

5.1.4. ¿Existen quejas de usuarios de la certificación recibidas por ICONTEC durante el último periodo evaluado? (Aplica a partir del primer seguimiento)?
Si □ No ■

5.1.5. ¿Se evidencia la capacidad del sistema de gestión para cumplir los requisitos aplicables y lograr los resultados esperados?:
Si ■ No □

5.1.6. ¿Se concluye que el alcance del sistema de gestión es apropiado frente a los requisitos que la Organización debe cumplir? (consultar E-PS-0080 ALCANCE DE CERTIFICACIÓN DEL SISTEMA DE GESTION)
Si ■ No □.

**5.2. Relación de no conformidades detectadas durante el ciclo de certificación**

| Auditoría | Número de no conformidades | Requisitos |
|---|---|---|
| Otorgamiento | 3 | 9.2 a) y b), A.12.4.4, A.15.2.1 |
| 1ª de seguimiento del ciclo | 1 | A.17.1.3 |
| 2ª de seguimiento del ciclo | N/A | A.7.2, A.8.9, A.5.22 |
| Renovación | N/A | N/A |
| Auditorias especiales (Extraordinaria, reactivación) | N/A | N/A |
| Auditoria de ampliación | N/A | N/A |

¿Se evidencia recurrencia de no conformidades detectadas en las auditorías de ICONTEC en el último ciclo de certificación?
Si □ No ■

**5.3 Análisis del proceso de auditoría interna**

La auditoría se realizó en la fecha 18 de septiembre de 2024 con la participación de dos profesionales externo con la competencia idónea con los soportes de la formación acordes a los sistemas de gestión; el programa de auditoría interna indica las fechas y la duración por cada auditoría; el plan de auditoría incluyó la evaluación de requisitos, procesos y sedes dentro del alcance por cada sistema de gestión; , adecuación e implementación oportuna de los planes de acción definidos para el tratamiento y cierre de las no conformidades identificadas, orientación de la auditoría interna de acuerdo con directrices de ISO 19011, entre otros.

**5.4 Análisis de la revisión del sistema por la dirección**

La revisión por la dirección se llevó a cabo de acuerdo a la planeación el 28 de junio de 2024 en la cual se incluyó la totalidad de las entradas de información. Se evidenció la salidad del ejercicio bajo una minuta registrando los resultados, salidas y conclusiones en general evidenciaron el cumplimiento de los propósitos de la organización a mantener un proceso de mejora continua.

## 6. USO DEL CERTIFICADO DE SISTEMA DE GESTIÓN Y DE LA MARCA O LOGO DE LA CERTIFICACIÓN

6.1. ¿El logo o la marca de conformidad de certificación de sistema de gestión de ICONTEC se usa en publicidad (página web, brochure, papelería, facturas, etc…)?
Si ■ No □

En documentos internos y de acuerdo lo exigido por el reglamento.

6.2. ¿La publicidad realizada por la Organización está de acuerdo con lo establecido en el R-PS-0007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN y el Manual de aplicación E-GM-0001 USO DE LA MARCA DE CONFORMIDAD DE LA CERTIFICACIÓN ICONTEC PARA SISTEMAS DE GESTIÓN?
Si □ No □ NA ■.

6.3. ¿El logo o la marca de conformidad se usa sobre el producto o sobre el empaque o el envase o el embalaje del producto, o de cualquier otra forma que denote conformidad del producto?
Si □ No □ NA ■

6.4. ¿Se evidencia la adecuación de la información contenida en el certificado (¿vigencia del certificado, logo de organismo de acreditación, razón social registrada en documentos de existencia y representación legal, direcciones de sitios permanentes cubiertos por la certificación, alcance, etc.?
Si ■ No □

## 7. RESULTADO DE LA REVISIÓN DE LAS CORRECCIONES Y ACCIONES CORRECTIVAS PARA LAS NO CONFORMIDADES MAYORES DETECTADAS EN ESTA AUDITORÍA, MENORES QUE GENERARON COMPLEMENTARIA Y, MENORES DETECTADAS EN ESTA AUDITORÍA QUE POR SOLICITUD DEL CLIENTE FUERON REVISADA

¿Se presentaron no conformidades mayores? SI □ NO ■

¿Se presentaron no conformidades menores de la auditoria anterior que no pudieron ser cerradas en esta auditoría? SI □ NO ■
¿Se presentaron no conformidades menores detectadas en esta auditoría que por solicitud del cliente fueron revisadas durante la complementaria? SI □ NO ■

En caso afirmativo diligencie el siguiente cuadro:

Fecha de la verificación complementaria: N/A

| NC | Descripción de la no conformidad (se relaciona el numeral de la norma y la evidencia del incumplimiento) | Evidencia obtenida que soporta la solución | ¿Fue eficaz la acción? Si/No |
|---|---|---|---|
| **No conformidades mayores identificadas en esta auditoría** | | | |
| | | | |
| **No conformidades pendientes de la auditoría anterior que no se solucionaron** | | | |
| | | | |
| **No conformidades detectadas en esta auditoría que fueron cerradas** | | | |
| | | | |

| 8. RECOMENDACIÓN DEL EQUIPO AUDITOR DE ACUERDO CON EL R-PS-007 | | | | |
|---|---|---|---|---|
| | | | **SI** | **NO** |
| Se recomienda otorgar la Certificación del Sistema de Gestión | | | | |
| Se recomienda mantener el alcance del certificado del Sistema de Gestión | | | **X** | |
| Se recomienda renovar el certificado del Sistema de Gestión | | | | |
| Se recomienda renovar anticipadamente el certificado del Sistema de Gestión | | | | |
| Se recomienda ampliar el alcance del certificado del Sistema de Gestión | | | | |
| Se recomienda reducir el alcance del certificado | | | | |
| Se recomienda reactivar el certificado | | | | |
| Se recomienda actualizar el certificado del Sistema de Gestión | | | **X** | |
| Se recomienda restaurar el certificado, una vez finalice el proceso de renovación | | | | |
| Se recomienda suspender el certificado | | | | |
| Se recomienda cancelar el certificado | | | | |
| **Nombre del auditor líder: OSCAR FERNANDO RAMOS BENAVIDES** | Fecha | **2024** | **12** | **16** |

| 9. ANEXOS QUE FORMAN PARTE DEL PRESENTE INFORME | | |
|---|---|---|
| Anexo 1 | Correcciones, análisis de causa y acciones correctivas | X |
| Anexo 2 | Información específica de esquemas de certificación de sistema de gestión | X |
| Anexo 3 | Plan de auditoría F-PS-0530 PLAN DE AUDITORIA EN SITIO – SISTEMAS DE GESTIÓN (Adjuntar el plan a este formato y el F-PS-0654 FORMATO DE PROYECTOS EJECUTADOS Y EN EJECUCIÓN, cuando aplique) | X |
| Anexo 4 | Aceptación de los resultados de la auditoria firmada por la organización. | X |

## ANEXO 1 CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS.

- Se recibió la propuesta de correcciones, análisis de causas y acciones correctivas para la solución de no conformidades el 2024-11-21.
- Las correcciones, análisis de causas y acciones correctivas propuestas por la organización, fueron aceptadas por el auditor líder el 2024-11-22.

| **SOLICITUD DE ACCIÓN CORRECTIVA** | | **No.** 1 de 3 |
|---|---|---|
| ☐ No - Conformidad Mayor | Norma(s): **ISO/IEC 27001:2022** | Requisito(s): |
| ☒ No - Conformidad Menor | | A.7.2 |
| **Descripción de la no conformidad:** No se segura el control de acceso físico al área segura "*Data center*" | | |
| **Evidencia:** Los registros físicos "Bitácora de Acceso" definidos para el registro de ingreso de terceros a Datacenter identifican únicamente fecha y hora de ingreso, pero no de salida. | | |

| Corrección | Evidencia de Implementación | Fecha |
|---|---|---|
| Comunicar a la división de Infraestructura de hardware y centros de datos, encargada del Datacenter del CAN, cumplir adecuadamente con el diligenciamiento, organización y aseguramiento de las bitácoras de acceso (ingreso - salida), asociada al control A.7.2. | Correo electrónico | 18/diciembre/2024 |

- Porque no se registró en la bitácora de acceso la hora de salida del personal que ingresó.
- Porque los ingenieros encargados olvidaron solicitar el diligenciamiento del formato del personal que ingresó.
- Porque no se tuvo rigurosidad en llevar el control del registro en el formato físico, ya que no lo consideraban necesario, al tener cámaras de seguridad.
- Porque los ingenieros a cargo consideraban que, al tener el registro de las cámaras de seguridad, no era necesario diligenciar la salida en el formato físico establecido para tal fin, ya que las cámaras de seguridad cuentan con la hora de ingreso/salida del Datacenter.
- Porque no tenían claridad de los controles definidos para el Datacenter, y, además, no había un seguimiento al control de los registros de ingreso y salida de este.

**Causa Raíz**
Debilidades en la sensibilización en el propósito y aplicación del control de ingreso y salida del Datacenter, específicamente en el control de registro de la "*Bitácora de accesos*".

| Acción correctiva | Evidencia de Implementación | Fecha |
|---|---|---|
| Socializar con el personal encargado del Datacenter los objetivos de cada uno de los controles implementados, específicamente el control de registro de ingreso y salida "*Bitácora de accesos*", haciendo énfasis en que son controles de acceso complementarios y la responsabilidad de ellos en cada control. | Acta de mesa de trabajo. | 31/enero/2025 |
| Realizar periódicamente la validación del correcto diligenciamiento, organización y aseguramiento de las bitácoras de acceso al Datacenter, según lo definido en el manual de políticas del SGSI. | Correo con la evidencia fotográfica del diligenciamiento de las bitácoras del Datacenter y las recomendaciones (si aplican) por parte del encargado de controles físicos del SGSI. | Marzo, junio, septiembre, diciembre |
| Realizar la revisión del cumplimiento y eficacia de las acciones correctivas a través de auditoría interna. | Informe de Auditoría interna | 30/septiembre/2025 |

| SOLICITUD DE ACCIÓN CORRECTIVA | No. 2 de 3 |
|---|---|

| | | |
|---|---|---|
| ☐ No - Conformidad Mayor | Norma(s): **ISO/IEC 27001:2022** | Requisito(s): |
| ☒ No - Conformidad Menor | | A.8.9 |

**Descripción de la no conformidad:**
No se determinan las acciones o estrategias para realizar las actividades de monitoreo y seguimiento a las configuraciones de seguridad.

**Evidencia:**
No se suministró evidencia asociada al control de monitoreo y revisión de la información de configuración de seguridad.

| Corrección | Evidencia de Implementación | Fecha |
|---|---|---|
| Realizar actividades exhaustivas de sensibilización del propósito del control, para definir las estrategias y acciones de monitoreo y revisión. | Informe de actividades | 30/junio/2025 |

- Porque no existen procedimientos claros documentados que establezcan cómo realizar el monitoreo y la revisión.
- Porque no se ha asignado un responsable específico para desarrollar, implementar y mantener dichos procedimientos.
- Porque no se incluyó en la planificación inicial del proyecto la necesidad de roles específicos para el monitoreo y revisión.
- Porque no se identificaron el monitoreo y la revisión como actividades críticas en la gestión de configuraciones durante la etapa de diseño del control.
- Porque no se realizó un análisis de requerimientos exhaustivo ni se consultaron las mejores prácticas o estándares aplicables al control.

**Causa Raíz**
La falta de un análisis de requerimientos exhaustivo en la etapa de diseño del control, lo que derivó en la omisión de la definición de actividades críticas como el monitoreo y revisión de este, y de los roles y responsabilidades para llevar a cabo dichas actividades.

| Acción correctiva | Evidencia de Implementación | Fecha |
|---|---|---|
| Definición de las actividades, roles y responsabilidades, asociados al control de Gestión de la configuración. | Documento con la definición de las actividades.<br>Documento de roles, responsabilidades asociadas al monitoreo y revisión de la configuración de la seguridad en el manual de políticas de seguridad. | 07/marzo/2025 |
| Revisión de las actividades, roles y responsabilidades definidas, asociadas al control de Gestión de la configuración. | Acta de reunión / grabación Teams. | 15/abril/2025 |
| Socialización de la definición de roles responsabilidades y frecuencia asociadas al monitoreo y revisión de la configuración de seguridad. | Acta de reunión / grabación Teams. | 27/junio/2025 |
| Monitoreo y revisión a la Gestión de la configuración de seguridad. | Acta de reunión / grabación Teams. | Marzo, junio, septiembre, diciembre |

| SOLICITUD DE ACCIÓN CORRECTIVA | No. 3 de 3 |
|---|---|

[ ] No - Conformidad Mayor
[X] No - Conformidad Menor

Norma(s): **ISO/IEC 27001:2022**

Requisito(s): A.5.22

**Descripción de la no conformidad:**
No se monitorea y revisa el cumplimiento de controles de configuración de seguridad equipo de cómputo de usuarios de propiedad de los proveedores

**Evidencia:**
Equipo de cómputo de Ing. Juan Carlos Chocontá, proveedor de ETB, se identificó con el sistema operativo pendiente por activar.

| Corrección | Evidencia de Implementación | Fecha |
|---|---|---|
| Activar el sistema operativo en el equipo de cómputo identificado en la N.C., y revisar la activación del sistema operativo en los demás equipos de cómputo del proveedor ETB. | Informe de la revisión de la activación del sistema operativo en los equipos de cómputo del proveedor ETB. | 31/enero/2025 |
| Solicitar a los interventores y supervisores de contratos, realizar la revisión de los acuerdos o compromisos con respecto a seguridad de la información. Y en los casos de incumplimiento realizar los llamados de atención o sanciones correspondientes. | Solicitud | 31/marzo/2025 |

- Porque los supervisores e interventores (según el caso), no verifican las políticas de seguridad en los equipos de cómputo de los proveedores.
- Porque desconocen sus responsabilidades en el monitoreo y revisión de estas políticas y desconocen la obligación contractual de cumplimiento de dichas políticas.
- Porque no han recibido socialización de las políticas de seguridad aplicables a equipos de los proveedores.
- Porque no existe una obligación contractual que les permita exigir el cumplimiento de dichas políticas a los proveedores.
- Porque no se incluyó la sociabilización de esta política como parte de las estrategias de control y seguimiento en los contratos.
- Porque no se incluyó inicialmente en el cronograma de sensibilización, una “capacitación” dirigida a supervisores e interventores de contratos, en lo relacionado a los equipos de cómputo propiedad de los proveedores.

**Causa Raíz**
Desconocimiento por parte de proveedores, supervisores e interventores sobre el cumplimiento de las políticas de seguridad asociadas a equipos de cómputo de proveedores.
Solicito se incluya la información del resultado del análisis de causas, de modo tal permita identificar las acciones correctivas adicionales idóneas.

| Acción correctiva | Evidencia de Implementación | Fecha |
|---|---|---|
| Socializar los lineamientos y obligaciones asociadas a las responsabilidades de proveedores (terceros) en materia de seguridad de la información en lo relacionado con equipos de cómputos. Socializar el lineamiento podría ser una acción de corrección, pero definir un plan de socializaciones con periodicidad SI es una acción correctiva | Correo electrónico | 31/enero/2025 |
| Validar cada tres meses el cumplimiento de la política en una muestra de los equipos de los terceros de la unidad de transformación digital e informática. | Documento con los resultados de validación del cumplimiento de la política de seguridad en equipos de los terceros. | Febrero/Octubre |

| | | |
|---|---|---|
| Presentar a la Unidad de Compras Públicas solicitud para incluir dentro de los contratos aspectos específicos en materia de seguridad de la información. | Solicitud | 31/marzo/2025 |

**ANEXO 2**

**INFORMACIÓN ESPECÍFICA DE ESQUEMAS DE CERTIFICACIÓN DE SISTEMA DE GESTIÓN**

Esta sección se completa solo para los siguientes casos:

**Sistema de gestión de seguridad de la información ISO/IEC 27001**
**Sistema de gestión de privacidad de la información ISO/IEC 27701**

Marque con una X si el sistema de gestión auditado.

ISO/IEC 27001 ■ ISO/IEC 27001 + ISO/IEC 27701 □

**Objetivos de la auditoría**

Evaluar las implicaciones de los cambios en el SGSI/SGPI, iniciadas como consecuencia de cambios en la operación del cliente y cubrir al menos:
a) El sistema de mantenimiento de elementos tales como la evaluación y control de riesgos de seguridad de la información y privacidad, mantenimiento, auditorías internas del SGSI/SGPI, revisión por la dirección y las acciones correctivas;
b) Las comunicaciones de las partes externas como es requerido por la norma ISO/IEC 27001 e ISO/IEC 27701;
c) Los cambios en la documentación del SGSI/SGPI;
d) Las zonas sujetas a cambio;
e) los requisitos de la norma ISO/IEC 27001 e ISO/IEC 27701 cuando sea aplicable.

**Actividades desarrolladas**

- La metodología de la auditoría fue verificación de registros físicos y electrónicos, interacción, observación bajo técnica de muestreo

- ¿Se modificó la declaración de aplicabilidad?
  Si ■ No □

| VERSIÓN VIGENTE: | JUSTIFICACIÓN DEL CAMBIO |
|---|---|
| DEAJ-BTA-GT-A-F-03 con fecha 06-06-2024 | El cambio está sustentado en la nueva estructura de los controles del anexo A en |

| | |
|---|---|
| | transición a la versión ISO/IEC 27001:2022, con la identificación de las estrategias de control para mitigar todos los escenarios de riesgo potenciales en el SGSI. |

- ¿Los procedimientos adoptados por el cliente brindan confianza en el SGSI/ SGPI?
  Si ■ No □

- Describa brevemente los documentos revisados como evidencia de las muestras tomadas para la evaluación del SGSI/ SGPI (Ver PE-PS-0079 PROCEDIMIENTO ESPECIFICO PARA CERTIFICACION ISO/IEC 27001 y el PE-PS-0133 PROCEDIMIENTO ESPECIFICO PARA LA GESTION DE LA PRIVACIDAD DE LA INFORMACION ISO/IEC 27701).

  Se verificó la nueva declaración de aplicabilidad, el inventario y enfoque de valoración de los activos de información, la matriz de riesgos de seguridad de la información y los resultados de la eficacia de los controles, el modelo de servicio de ciberseguridad prestado por el tercero, los procedimientos de control de acceso de usuarios a sistemas de información, informe de gestión de vulnerabilidades técnicas, procedimiento de gestión de incidentes y la estrategia de continuidad de negocio. Adicionalmente se verificaron las políticas de seguridad de la información, el procedimiento de soporte a la gestión de cambios en TI.

**Análisis de la eficacia del sistema de gestión certificado**

- Describa brevemente el análisis de riesgos, de la revisión de los planes de tratamiento y del riesgo residual (Ver PE-PS-0079 y PE-PS-0133).

  El ejercicio de valoración de los riesgos está enfocado a identificar y analizar los actividades, activos de información, las potenciales causas (amenazas) y vulnerabilidades (debilidades) que, con el registro de cada una de ellas, permite a la organización identificar sus riesgos con los niveles de riesgo inherentes, de esta manera también y bajo la implementación de controles se obtiene los riesgos residuales de seguridad de la información.

  Cuentan con la metodología de riesgos para identificar tanto los riesgos inherentes como aquellos residuales bajo el análisis y resultado de los controles implementados y la fortaleza de éstos.

## ANEXO 3

## PLAN DE AUDITORÍA

| | | | |
|---|---|---|---|
| EMPRESA: | CONSEJO SUPERIOR DE LA JUDICATURA - RAMA JUDICIAL DEL PODER PÚBLICO DE COLOMBIA/CONSEJO SUPERIOR DE LA JUDICATURA | | |
| Dirección del sitio: | Carrera 8 No 12B – 82, Bogotá D.C., Colombia.<br>Carrera 7 # 27-18, Bogotá D.C., Colombia. | | |
| Representante de la organización: | CLARA MILENA HIGUERA GUIO | | |
| Cargo: | Directora UDAE – Rama Judicial | Correo electrónico | chiguerg@cendoj.ramajudicial.gov.co |
| **Alcance de la auditoría 27001**<br>Gestión tecnológica referente al servicio público de administrar justicia en la Rama Judicial. Aplicabilidad DEAJ-BTA-GT-A-F-03 con fecha 06-06-2024 | | | |
| **Alcance de la certificación 27001:**<br>Gestión tecnológica referente al servicio público de administrar justicia en la Rama Judicial. Aplicabilidad DEAJ-BTA-GT-A-F-03 con fecha 06-06-2024 | | | |
| Criterios de Auditoría ISO/IEC 27001:2022 **+** la documentación del Sistema de Gestión | | | |
| Tipo de auditoría:<br>☐ Inicial u otorgamiento ■ **Seguimiento** ☐ Renovación ☐ Ampliación ☐ Reducción<br>☐ Auditorias especiales (Reactivación/extraordinaria) ☐ Extraordinaria ■ **Actualización / Migración**<br>☐ Renovación (con restauración) ☐ Renovación (anticipada) | | | |
| Modalidad: ■ **Auditoría en sitio** ☐ Auditoria parcialmente remota ☐ Auditoría totalmente remota | | | |
| Es organización multisitio: | ■ Si ☐ No | | |
| Sitio(s) a ser muestreado(s) en la presente auditoria: | Actividades del sistema de gestión/alcance a auditar en sitio durante la auditoría: | | |
| Sitio 1 muestreado para el esquema ISO 27001: Carrera 8 No 12B – 82, Bogotá D.C., Colombia | Servicios de Tecnología | | |
| Existen actividades/procesos que requieran ser auditadas en turno nocturno: | ☐ Si<br>■ No | | |

Con un cordial saludo, enviamos el plan de la auditoría que se realizará al Sistema de Gestión de su organización. Por favor indicar en la columna correspondiente, el nombre y cargo de las personas que atenderán cada entrevista y devolverlo al correo electrónico del auditor líder. Así mismo, para la reunión de apertura de la auditoría le agradezco invitar a las personas del grupo de la alta dirección y de las áreas/procesos/actividades que serán auditadas.

Para la reunión de apertura le solicitamos disponer de un proyector para computador y sonido para video, si es necesario, (sólo para auditorías de certificación inicial y actualización).

En cuanto a las condiciones de seguridad y salud ocupacional aplicables a su organización, por favor informarlas previamente al inicio de la auditoría y disponer el suministro de los equipos de protección personal necesarios para el equipo auditor.

La información que se conozca por la ejecución de esta auditoría será tratada confidencialmente, por parte del equipo auditor de ICONTEC.

El idioma de la auditoría y su informe será en español.

Los objetivos de la auditoría son:

- Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión.
- Determinar la capacidad del sistema de gestión para asegurar que la organización cumple los requisitos legales, reglamentarios y contractuales aplicables al alcance del sistema de gestión y a la norma de requisitos de gestión.
- Determinar la eficacia del sistema de gestión para asegurar que la organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados.
- Identificar áreas de mejora potencial del sistema de gestión.

Las condiciones de este servicio y las responsabilidades del equipo auditor se encuentran indicadas en el R-PS-0007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN.

| | | | |
|---|---|---|---|
| Auditor Líder: | OSCAR F RAMOS - ORB | Correo Electrónico | oramos@icontec.net |
| Experto técnico: | N/A | | |
| Observador – Profesional de apoyo | N/A | | |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| **DIA 1: Lunes – 2024/10/28** | | | | | |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| 2024/10/28 | 08:00 | 09:00 | Reunión de apertura | ORB | Ing. Johanna Pimiento Quintero<br>Directora Unidad de Transformación Digital e Informática<br><br>Ing. Francisco Gonzalez Mendez<br>Director División de Seguridad y Protección de Datos |
| | 09:00 | 11:30 | **PLATAFORMA ESTRATÉGICA**<br>**Revisión por la Dirección**<br><br>Análisis del contexto organizacional, estratégica, políticas, objetivos<br>revisión por la dirección<br><br>Numerales: 4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 6.1, 6.2, 6.3, 9.3 | ORB | Ing. Johanna Pimiento Quintero<br>Directora Unidad de Transformación Digital e Informática<br>Ing. Francisco Gonzalez Mendez<br>Director División de Seguridad y Protección de Datos<br>Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI<br>Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos - UTDI |
| | 11:30 | 13:00 | **MEJORAMIENTO CONTINUO**<br>Auditoría interna<br>Cierre no conformidades año anterior<br>27001: 6.3, 9.2, 10 | ORB | Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos - UTDI<br>Ing. Jazmín Beltrán Chávez – Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| | | | | | |
| | 13:00 | 14:00 | **RECESO DE MEDIO DIA** | | |
| | 14:00 | 16:00 | **TALENTO HUMANO**<br><br>Numerales: 7.1, 7.2, 7.3, 7.4<br>Controles: A.6.1, A.6.2, A.6.3, A.6.4, A.6.5, A.6.6, A.6.7, A.6.8, A.5.9, A.5.11, A.5.12, A.5.13 | ORB | Iris Patricia Cabrera Montoya – U. talento Humano<br>Sandra Maritza Giraldo Carmona – U. Talento Humano<br>Javier Chaparro Montezuma – director División de Almacén General e Inventarios<br>Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Libardo Bahamón Guarín – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Cristian Alexander Laguna Rodríguez - Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 16:00 | 17:00 | Balance Diario D1 – Preparación de Informe | ORB | |
| **DIA 2: Martes 2024/10/29** | | | | | |
| 2024/10/29 | 08:00 | 16:00 | **UNIDAD DE TRANSFORMACIÓN DIGITAL E INFORMÁTICA - UTDI**<br><br>**DIVISIÓN DE SEGURIDAD Y PROTECCIÓN DE DATOS** | ORB | Ing. Laura Magaly Almeida Gonzalez– Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Maricela Londoño – Profesional División Seguridad y Protección de Datos – UTDI |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| | | | Gobierno de Seguridad de la información, activos de información, riesgos, tratamiento de riesgos, gestión de configuración, gestión de cambios, gestión de capacidad, copias de respaldo, prevención fuga de datos, entre otros<br><br>**Numerales:** 8.1, 8.2, 8.3, 91<br><br>**(controles organizacionales y controles de acceso)**<br>Controles: A.5.1, A.5.2, A.5.3, A.5.4, A.5.5, A.5.6, A.5.7, A.5.8, A.5.9, A.5.10, A.5.15, A.5.16, A.5.17, A.5.18, A.8.1, A.8.2, A.8.3, A.8.5, A.5.14, A.5.37, A.8.32, A.8.34<br><br>**(Controles físicos)**<br>8.2, 8.3, A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.12, A.7.7, A.7.8, A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14<br><br>**(controles tecnológicos)**<br>Controles: A.8.6, A.8.7, A.8.9, A.8.10, A.8.11, A.8.12, A.8.13, A.8.14, A.8.15, A.8.16, A.8.17, A.8.18, A.8.19, A.8.20, A.8.21, A.8.22, A.8.23, A.8.24, A.5.14, A.5.37, A.8.34 | | Inge Jorge Eliecer Pachón Ballen – director División Infraestructura de Software<br>Ing. David Andrés Márquez Castillo – Profesional División Infraestructura de Software<br>Ing. Carlos Alberto Méndez López – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI<br>Ing. Raúl Fernando Flórez Ramos – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Leonel Gustavo Torres Rincón – Profesional División Infraestructura de Hardware – UTDI<br>Ing. Diego Andrés Sarmiento Campos Profesional División Infraestructura de Hardware – UTDI<br>Equipo central de Monitoreo y Reacción - Flórez Ramos – Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 13:00 | 14:00 | **RECESO DE MEDIO DIA** | | |
| | 16:00 | 17:00 | Balance Diario D2 – Preparación de Informe | ORB | |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| **DIA 3: Miércoles 2024/10/30** | | | | | |
| 2024/10/30 | 08:00 | 12:00 | **VISITA PRESENCIAL DATACENTER SEDE – CAN**<br><br>Controles de acceso, riesgos, seguridad física, operación, redundancia, incidentes, entre otros.<br><br>Controles: A.5.1, A.5.15, A.5.16, A.5.17, A.5.18,<br><br>**(controles tecnológicos)**<br>Controles: A.8.5, A.8.6, A.8.7, A.8.12, A.8.14, A.8.17, A.8.23, A.8.32, A.5.36, A.5.37<br><br>**(Controles físicos)**<br>8.2, 8.3, A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6, A.7.7, A.7.8, A.7.9, A.7.10, A.7.11, A.7.12, A.7.13, A.7.14 | ORB | Ing. Leonel Gustavo Torres Rincón – Profesional División Infraestructura de Hardware – UTDI<br>Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br><br>Ing. Erin José Mendoza – Profesional División Infraestructura de Hardware – UTDI<br>Ing. Eduardo Velásquez – Profesional División Infraestructura de Hardware – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 12:00 | 13:00 | **RETORNO A SEDE CARRERA 8 No. 12 B - 82, Bogotá D.C** | | |
| | 13:00 | 14:00 | **RECESO DE MEDIO DIA** | | |
| | 14:00 | 16:30 | **UNIDAD DE TRANSFORMACIÓN DIGITAL E INFORMÁTICA - UTDI**<br><br>Carrera 8 No 12B – 82, Bogotá D.C<br><br>**SEGURIDAD DE LA INFORMACION EN LA CONTINUIDAD DE LAS TIC**<br><br>Controles: A.7.5, A.7.6, A.8.14, A.5.29, A.5.30 | ORB | Ing. Raúl Fernando Flórez Ramos – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 16:30 | 17:00 | | ORB | |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| | | | Balance Diario D3 – Preparación de Informe | | |
| **DIA 4: Jueves - 2024/10/31** | | | | | |
| 2024/10/31 | 08:00 | 11:00 | **INTELIGENCIA DE AMENAZAS /EVENTOS/EVALUACION DE VULNERABILIDADES TECNICAS DE SEGURIDAD DE LA INFORMACION**<br><br>Controles: A.6.8, A.5.23, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.5.29, A.5.30, A.8.8, A.8.15, A.5.37 | ORB | Equipo Central de Monitoreo y Reacción - División Seguridad y Protección de Datos – UTDI<br>Ing. Libardo Bahamón Guarín – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Carlos Alberto Méndez López – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Cristian Alexander Laguna Rodríguez - Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 11:00 | 13:00 | **COMPRAS PUBLICAS**<br><br>Controles A.5.19, A.5.20, A.5.21, A.5.22 | ORB | Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Jazmín Beltrán Chávez – Profesional División Seguridad y Protección de Datos – UTDI |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| | | | | | Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 13:00 | 14:00 | **RECESO DE MEDIO DIA** | | |
| | 14:00 | 16:00 | **INCIDENTES DE SEGURIDAD DE LA INFORMACION**<br><br>Controles: A.5.24, A.5.25, A.5.26, A.5.27, A.5.28 | ORB | Equipo Central de Monitoreo y Reacción - División Seguridad y Protección de Datos – UTDI<br>Ing. Libardo Bahamón Guarín – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Carlos Alberto Méndez López – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Cristian Alexander Laguna Rodríguez - Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Raúl Fernando Flórez Ramos – Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 16:00 | 17:00 | Balance Diario D4 – Preparación de Informe | ORB | |
| **DIA 5: Viernes - 2024/11/01** | | | | | |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| 2024/11/01 | 08:00 | 10:00 | **CUMPLIMIENTO REQUISITOS LEGAL/NORMATIVOS**<br><br>Controles A.5.31, A.5.32, A.5.33, A.5.34, A.5.35 | ORB | Ing. Laura Magaly Almeida Gonzalez – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Francisco Gonzalez Méndez<br>Director División de Seguridad y Protección de Datos<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI |
| | 10:00 | 12:00 | **MONITOREO DE EVENTOS DE SEGURIDAD Y CIBERSOC**<br><br>Controles: A.5.19, A 5.20, A.5.21, A.5.22, A.5.29, A.5.30, A.8.14 | ORB | Equipo Central de Monitoreo y Reacción - División Seguridad y Protección de Datos – UTDI<br>Ing. Libardo Bahamón Guarín – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Carlos Alberto Méndez López – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Cristian Alexander Laguna Rodríguez - Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Laura Magaly Almeida González – Profesional División Seguridad y Protección de Datos – UTDI<br>Ing. Raúl Fernando Flórez Ramos – Profesional División Seguridad y Protección de Datos – UTDI<br>Apoyo Ing. Yancy Jazmín Castellanos Sánchez – |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| | | | | | Profesional División Arquitectura – UTDI |
| | 12:00 | 13:00 | **RECESO DE MEDIO DIA** | | |
| | 13:00 | 15:30 | Preparación del balance general | ORB | |
| | 15:30 | 16:00 | Reunión Pre-cierre | ORB | Ing. Francisco González Méndez<br>Director División de Seguridad y Protección de Datos<br>Ing. Yancy Jazmín Castellanos Sánchez – Profesional División Arquitectura – UTDI<br>Ing. Laura Magaly Almeida González – Profesional División Seguridad y Protección de Datos - UTDI |
| | 16:00 | 17:00 | Reunión de Cierre | ORB | Ing. Johanna Pimiento Quintero<br>Directora Unidad de Transformación Digital e Informática<br><br>Ing. Francisco González Mendez<br>Director División de Seguridad y Protección de Datos |
| Los requisitos comunes que serán auditados en todos los procesos para ISO 27001 son:<br>5.2 Política, 7.1 Recursos, 7.2 Competencia, 7.3 Toma de conciencia, 7.4 Comunicación, 7.5 Información Documentada, 9.1. Seguimiento, medición, análisis y evaluación, 10 Mejora | | | | | |
| Entre las partes se deberá coordinar el desplazamiento a la sede CAN el Miércoles 30 de octubre para realizar allí reconocimiento y auditoría. | | | | | |
| Esta auditoría no es testificada por algún Organismo de Acreditación | | | | | |

| Fecha | Hora de inicio de la actividad de auditoría | Hora de finalización de la actividad de auditoría | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|---|---|---|---|---|
| Para el balance diario de información del equipo auditor le agradecemos disponer de la información documentada (Documentos y registros) solicitados por el auditor en el curso de la auditoria, así como también de acceso a la documentación del sistema de gestión. | | | | | |

| | |
|---|---|
| Fecha de emisión del plan de auditoría: | **2024 – 10 - 15** |

## ANEXO 4

**ACEPTACIÓN DE LOS RESULTADOS DE LA AUDITORIA FIRMADA POR LA ORGANIZACIÓN:**
CONSEJO SUPERIOR DE LA JUDICATURA - RAMA JUDICIAL DEL PODER PÚBLICO DE COLOMBIA/CONSEJO SUPERIOR DE LA JUDICATURA

Número de no conformidades por esquema detectadas en esta auditoría:

ISO/IEC 27001:2022 ( 0 ) Mayores ( 3 ) Menores

Número de no conformidades pendientes que no se cerraron en esta auditoría: ( ) menores ( X ) N.A.

Plazo para la entrega de propuesta de corrección y acción correctiva (de acuerdo con lo establecido en el R-PS-007) hasta: 2024 – 11-15

Fecha tentativa de verificación complementaria, cuando aplique NA

**ACEPTACIÓN DE LA ORGANIZACIÓN: CONSEJO SUPERIOR DE LA JUDICATURA - RAMA JUDICIAL DEL PODER PÚBLICO DE COLOMBIA/CONSEJO SUPERIOR DE LA JUDICATURA**

Declaro que los servicios previstos fueron integralmente ejecutados y soy consciente de los resultados obtenidos.

La organización acepta la (s) no conformidad (es) reportada (s) en el presente informe y se compromete a presentar los planes de acción en los tiempos establecidos en el reglamento de certificación R-PS-007.

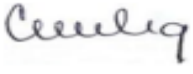
En caso de no aceptarse alguna no conformidad relacione él número de la no conformidad ___N/A____ y el requisito al que fue reportada _N/A_. En este caso la organización deberá solicitar una reposición dirigida al Gerente de Certificación.

**ACEPTACIÓN DE LA ORGANIZACIÓN DE RECIBIR AUDITORIAS TESTIFICADAS: N/A**

Dando cumplimiento al requisito 4.7 del R-PS-007 la Organización se compromete a permitir la participación de equipos evaluadores de organismos de acreditación, en calidad de observadores, en las auditorías testificadas que dichos organismos seleccionen como parte de sus actividades de acreditación.

Consulte el Reglamento de la certificación ICONTEC de Sistemas de Gestión

mailto:https://www.icontec.org/wp-content/uploads/2021/07/Reglamento-de-la-certificaci%C3%B3n-ICONTEC-de-sistemas-de-gesti%C3%B3n.pdf

| **Nombre del Representante de la Organización:** | Firma: |
|---|---|
| **CLARA MILENA HIGUERA GUÍO**<br>Directora<br>Unidad de Desarrollo y Análisis Estadístico<br>Consejo Superior de la Judicatura |  |