MINISTERIO DE DEFENSA NACIONAL

FONDO ROTATORIO DE LA POLICIA

AUDITORIA AL
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
ISO 27001:2013

INFORME FINAL

Bogota, D.C. 2022 /01 /07

Elaboró:	Revisó:	Aprobó:
Sandra A. Blanco G. **Prof. Admin. Sistemas** **Auditora**	**Economista Omar Antonio Pereira Góez** **Jefe de la Of. de Control Interno**	**Economista Omar Antonio Pereira Góez** **Jefe de la Of. de Control Interno**

TABLA DE CONTENIDO

1. Objetivo General 3
1.1. Objetivos Específicos: 3
2. Contenido del Informe 3
2.1. Alcance 3
2.2. Justificación 3
2.3. Criterios 3
2.4. Fortalezas 4
2.5. Desarrollo de la auditoría 4
2.6. Análisis del control 5
2.7. Limitaciones 5
2.8. No Conformidades 5
2.8.1. Gestión Documental 5
2.8.2. Telemática 6
2.8.3. Créditos 11
2.8.4. Fábrica de confecciones 12
2.8.5. Contratos 12
3. Conclusiones y/o Recomendaciones 13
3.1. Conclusiones 13
3.2. Recomendaciones 13

1. Objetivo General

Evaluar el grado de cumplimiento de la norma ISO 27001:2013, Sistema de Gestión de Seguridad de la Información, y su implementación en los procesos del Fondo Rotatorio de la Policía.

1.1. Objetivos Específicos:

- Determinar la capacidad del Sistema de Gestión de Seguridad de la Información, para asegurar que el Fondo Rotatorio de la Policía cumpla con los requisitos de la norma ISO 27001:2013
- Determinar la eficacia del Sistema de Gestión de Seguridad de la Información, para asegurar que la Organización pueda tener expectativas razonables con relación al cumplimiento de los objetivos especificados.
- Identificar áreas de mejora potencial del Sistema de Gestión de Seguridad de la Información.

2. Contenido del Informe

2.1. Alcance

Los procesos misionales incluidos en el Manual del Sistema de Gestión de Seguridad de la información (Gestión Contractual, Industrial, Créditos, Telemática y Gestión Documental); así como, los numerales de la norma ISO 27011:2013 involucrados en dentro de la Declaración de Aplicabilidad (SoA) del Fondo Rotatorio de la Policía

2.2. Justificación

El Fondo Rotatorio de la Policía tiene como meta propuesta la certificación del Sistema de Gestión de Seguridad de la Información ISO 27001:2013, por tal razón, en cumplimiento de los requisitos de la norma, se ha programado la realización de la auditoría interna, con el fin de evaluar el grado de avance en la implementación de este sistema de gestión.

2.3. Criterios

- Norma ISO 27001:2013

- Gestión del Riesgo
- Gestión de cambios
- Gestión de incidentes
- Matriz de Riesgos
- Código de Buen Gobierno
- Manual de Gestión del Riesgo
- Indicadores de gestión
- Políticas, Procedimientos, instructivos, formatos, manuales involucrados en el SGSI
- Normas Internacionales para el ejercicio profesional de la auditoría interna

2.4. Fortalezas

- La proactividad del Grupo de Créditos en cuanto a:
  - las Correcciones implementadas para evitar la fuga de información, relacionadas con el incidente detectado por ellos y el reporte al Grupo de Telemática - área de Seguridad de la Información, para la toma de las acciones correctivas correspondientes.
  - La toma de decisiones y acciones, en cuanto a la eliminación de documentos innecesarios y que podrían generar necesidad de recursos, riesgos y procedimientos para su custodia
  - Las autocapacitaciones realizadas dentro del grupo de Créditos, evidencia de su compromiso con el SGSI
- La proactividad y compromiso del Grupo de Construcciones, en la identificación de la pérdida de correos enviados, y el reporte inmediatamente evidenciada la situación al grupo de Telemática - área de Seguridad de la Información, para de la toma de las acciones correctivas correspondientes
- Las formaciones periódicas realizadas por el coordinador de créditos en temas de seguridad de la información
- El compromiso del coordinador de gestión documental y reacción inmediata en el cierre de brechas en temas de seguridad de la información

2.5. Desarrollo de la auditoría

Para iniciar la auditoría se solicitó la información a las dependencias de Talento Humano y de Telemática. Posteriormente se envió el programa y el plan de la auditoría a la Subdirección Administrativa y Financiera y a las áreas involucradas en la misma

De acuerdo a las mejores prácticas de auditoría, se realizó una prueba de recorrido con el fin de identificar las actividades que se desarrollan para llevar a cabo las labores del Sistema de Gestión de Información auditado.

Considerando que el grupo de Adquisiciones y Contratos es el área que, estadísticamente, genera el mayor número de documentación, se incluyó dentro de la auditoría; también se tuvieron en cuenta las áreas incluidas en el alcance del Sistema de Gestión de Seguridad de la Información, encabezada por Telemática.

Se realizó la recopilación de información de manera transversal dependiendo del numeral auditado y el responsable de manejo de la información.

El proceso de auditoría se inició en el Grupo de Construcciones, posteriormente se auditó convenios, contratos, Gestión Documental, Créditos, Fábrica de Confecciones y finalmente se auditó el área de Telemática.

2.6. Análisis del control

N/A

2.7. Limitaciones

En el momento de la auditoría la actualización de la documentación relacionada con las políticas de seguridad de la información y el manual de seguridad de la información se encontraba en proceso de revisión por parte de la entidad.

2.8. No Conformidades

2.8.1. Gestión Documental

2.8.1.1. Se evidenció que no hay control en el acceso a las instalaciones del área de Gestión Documental, ubicadas en la Bodega 14C, del Complejo Industrial Santa Lucia de Funza, debido a que:

- La puerta de ingreso a la Bodega 14C permaneció abierta durante el proceso de auditoría, permitiéndose el acceso a cualquier persona al área de Gestión Documental.
- En la oficina en donde se realiza escaneo, allí se encuentra la información en medio magnético de más de 10 años, no se cuenta con seguridades que limiten el acceso al personal
- No se cuenta con seguridades que impidan la apertura de la puerta que colinda con el acceso a la bodega 15C, no se dispone de seguridad que restrinja su apertura.
- En el momento de la auditoría se encontraba personal de contratos en las instalaciones de Gestión documental, realizando revisión de información, sin el debido registro en la minuta de control

Incumpliendo lo establecido en el control relacionado con “controles de acceso físico” 11.1.2 del anexo A de la norma ISO 27001:2013, esto debido a fallas en el control de acceso a las instalaciones de gestión documental, lo que podría acarrear pérdida de la información confidencial de la entidad. (Anexo 1)

2.8.1.2. El equipo en el que se maneja la información de las transferencias documentales se encontró desbloqueado, con información en pantalla y sin el funcionario responsable dentro del área, incumpliendo el control A.11.2.8 “Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada”, lo que podría generar perdida o modificación indebida de la información de la entidad, esta situación se presenta debido a fallas en la aplicación de los controles de seguridad de la información (Anexo 2)

2.8.2. Telemática

2.8.2.1. Teniendo en cuenta que la declaración de aplicabilidad determinada por la entidad solo excluye los numerales 14.4.2 y 6.2.2 del anexo A, de la norma ISO 27001:2013, se analizó el mapa de riesgos de seguridad digital e información de fecha 2021-01-20, se evidenció que no se contemplan riesgos, ni controles relacionados con la seguridad de la información física, como los relacionados con el manejo de documentos, contratos, manuales y archivos de gestión incumpliendo los numerales 6.1.1., 6.1.2. y 6.1.3 de la norma ISO 27001:2013, lo que podría generar la materialización de riesgos no identificados, ni controlados.

2.8.2.2. Las responsabilidades de administración de bases de datos y administración de usuarios de los diferentes aplicativos se encuentran asignadas a la dependencia de telemática, no se evidencia la segregación de deberes, en áreas de responsabilidad en conflicto, incumpliendo el control establecido en el numeral 6.1.2 del anexo A, de la norma ISO 27001:2013. Esta situación podría generar la materialización de riesgos relacionados con la modificación no autorizada o no intencional, o el uso indebido de activos de la organización, más aún cuando no existe evidencia de revisiones esporádicas realizadas a las modificaciones en las bases de datos y/o administración de usuarios.

2.8.2.3. El Fondo Rotatorio ha identificado 5 tipos de activos de información en el numeral 8.2 de la resolución 00074 del 26 de febrero de 2020, los cuales están relacionados con Información electrónica, Información física, Software, Hardware e Infraestructura, al realizar la revisión del inventario

de activos de información, suministrado por la Coordinación de Telemática, no se evidencian los activos relacionados con información física, tales como documentos, contratos, manuales y archivos de gestión documental; incumpliendo el control establecido en el numeral 8.1.1. del anexo A de la norma ISO 27001:2013, que indica que "se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se deberán elaborar y mantener un inventario de estos activos.", esta situación se presenta debido a que solo se tienen contemplados los activos relacionados con tecnología y podría generar la materialización de riesgos relacionados con amenazas de los activos, representados en pérdida de confidencialidad, disponibilidad e integridad de los activos físicos.

2.8.2.4. Al solicitar los procedimientos implementados para el manejo de activos de información, elaborados de acuerdo a la clasificación de información, no fue posible obtenerlos, incumpliendo lo establecido en el control del numeral 8.2.3 del anexo A de la Norma ISO 27001:2013, lo que podría acarrear duplicidad en las tareas, desgaste administrativo, así como des estandarización en el manejo de los activos de información y en los controles de los mismos.

2.8.2.5 La entidad realiza procedimientos de borrado seguro antes de entregar los medios y equipos para disposición final; sin embargo, no se evidenció la existencia de un procedimiento formal que lo involucre, incumpliendo el control establecido en el numeral 8.3.2 del anexo A de la norma ISO 27001:2013, que indica *"se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales*", esta situación podría acarrear el desconocimiento e incumplimiento del procedimiento y poner en riesgo la información de la entidad.

2.8.2.6. Existen actas de desactivación de usuarios; sin embargo, no se evidenció la existencia de un procedimiento formal de registro y cancelación de usuarios, incumpliendo el control 9.2.1 del anexo A de la norma ISO 27001:2013.

2.8.2.7. No se evidenció la existencia de un procedimiento formal de usuarios para asignación y/o revocación de derechos de accesos en los sistemas de información. Incumpliendo el numeral 9.2.2 del anexo A de la norma ISO 27001:2013, esta situación podría acarrear habilitación de usuarios en perfiles inadecuados, posibilitando el acceso a información que no corresponda con sus funciones.

2.8.2.8. No fue posible obtener el procedimiento de asignación de información de autenticación secreta, incumpliendo lo establecido en el control 9.2.4. del anexo A de la Norma ISO 27001:2013, esta situación podría acarrear riesgos relacionados con informalidad en la entrega de información y no asumir las responsabilidades que conlleva el acceso a los diferentes sistemas de información.

2.8.2.9. No se evidenció revisión de los derechos de acceso de los usuarios a intervalos regulares, incumpliendo el control 9.2.5, establecido en el anexo A de la norma ISO 27001:2013, lo que puede ocasionar accesos indebidos de usuarios a los sistemas de información

2.8.2.10. No fue posible encontrar la política de llaves criptográficas dentro del manual de Seguridad de la Información, teniendo en cuenta que este requisito fue incluido dentro de la declaración de aplicabilidad de la entidad, se presenta incumplimiento del control establecido en el anexo A numeral 10.1.2 de la norma ISO 27001:2013

2.8.2.11. No se evidenció la definición de perímetros de seguridad física, incumpliendo el numeral 11.1.1 del anexo A de la norma ISO 27001:2013, lo que podría generar la materialización de riesgos relacionados con fallas en la protección de la información confidencial

2.8.2.12. No se obtuvieron los procedimientos para el trabajo en áreas seguras, incumpliendo el control establecido en el numeral 11.1.5 del anexo A de la norma ISO 27001:2013

2.8.2.13. No se evidenciaron procedimientos de verificación de los medios de almacenamiento, que aseguren que los datos confidenciales hayan sido retirados antes de su reasignación, incumpliendo el numeral 11.2.7 del anexo A de la norma ISO 27001

2.8.2.14. No se obtuvo evidencia del cumplimiento de las actividades relacionadas con el procedimiento de gestión de cambios y evaluación de riesgos, correspondientes a las nuevas funcionalidades de créditos, relacionados con los alivios establecidos por el Gobierno Nacional, , incumpliendo el control establecido en el numeral 12.1.2 del anexo A de la norma ISO 27001:2013,- Gestión de cambios, que indica que "*Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que*

afectan la seguridad de la información" lo cual puede generar materialización de riesgo por fallas en procesos de rollback, monitoreo de los cambios publicados, reacción ante imprevistos.

2.8.2.15. No se obtuvo la evidencia del monitoreo al log de eventos de los diferentes aplicativos tales como ERP, Orfeo, Suite Visión Empresarial, Firewall y las mejoras realizadas ante excepciones o fallas, incumpliendo el control establecido en la norma ISO 27001:2013 Anexo A 12.4.1 situación que podría generar materialización de riesgos relacionados con ciberataques, poniendo en riesgo la información de la entidad.

2.8.2.16. No se evidenció la existencia de monitoreo, ni de protección de los registros de las actividades de los administradores del sistema, incumpliendo los numerales 12.4.2 y 12.4.3 del anexo A de la norma ISO 27001:2013, lo cual podría generar la materialización de riesgos de integridad, disponibilidad y seguridad de la información.

2.8.2.17. El Fondo Rotatorio de la Policía cuenta con las funcionalidades de continuidad de negocio desde el año 2019, al solicitar el plan de pruebas de contingencia y los resultados de las mismas no se evidenció que se hayan ejecutado las pruebas, ni la verificación, revisión y evaluación del plan de continuidad de negocio, incumpliendo el control establecido en el numeral 17.1.3 del anexo A de la norma ISO 27001: 2013, lo cual podría generar la materialización de riesgos relacionados con el afinamiento del plan de contingencia y/o nuevos sistemas que no fueran contemplados dentro del plan

2.8.2.18. No se evidenciaron los requisitos de seguridad de la información establecidos por el Forpo en la contratación del software EDUFILE y en los desarrollos del portal transaccional de la entidad, incumpliendo el numeral 14.1.1 del anexo A de la norma ISO 27001:2013 lo que podría generar exposición a riesgos de incumplimiento con la integridad, confidencialidad y disponibilidad de la información.

2.8.2.19. No se evidencia la existencia de un procedimiento formal de control de cambios que administre los cambios a los sistemas dentro del ciclo de vida del desarrollo, incumpliendo el control establecido en el numeral 14.2.2. del anexo A de la norma ISO 27001:2013 lo que podría generar fallas en el control y/o funcionalidades de los sistemas.

2.8.2.20. No se evidencia la documentación que incluya los principios de

construcción de sistemas seguros en la implementación de sistemas de información. Incumpliendo el numeral 14.2.5 del anexo A de la norma ISO 27001:2013, lo cual no permite garantizar la estandarización de controles de seguridad de la información en la construcción de sistemas de información.

2.8.2.21 No obtuvo la evidencia de las pruebas de seguridad a la ERP, incumpliendo el numeral 14.2.8 del anexo A de la norma ISO 27001:2013 lo cual podría materializar riesgos relacionados con fallas en la seguridad de la información.

2.8.2.22. No se evidenciaron los criterios de aceptación del software EDUFILE ni del ERP, incumpliendo el numeral 14.2.9 del anexo A de la norma ISO 27001:2013 que podría redundar en fallas de las funcionalidades de los aplicativos y/o corrupción de las bases de datos

2.8.2.23. Se evidenciaron eventos/incidentes de seguridad de la información tales como:

- Se evidenció fuga de información de la dependencia de Contratos del Sistema de Gestión Documental Orfeo, relacionada con el contrato de las tazer.
- Pérdida de correos electrónicos del área de Construcciones
- Hackeo y suplantación de la cuenta de correo de atención al cliente, en donde se evidenciaba la adulteración del número de la cuenta del Forpo e indicando que en esa cuenta se deberían realizar los pagos de los créditos
- Fallas en el sistema de reconocimiento facial

Los cuales no siguieron el procedimiento establecido por la entidad:

- No se evidencia el reporte del evento a través del canal establecido por la entidad (sin embargo, fueron reportados por las áreas a través de correos, personalmente, o directamente evidenciados por el área de telemática)
- No se evidencia la Clasificación como evento o incidente
- No se evidenciaron procedimientos documentados para dar respuesta a los mismos
- No se obtuvo la definición y aplicación de procedimientos para la recolección, adquisición y preservación de información que pueda servir como evidencia

Incumpliendo los controles 16.1.2, 16.1.4, 16.1.5, 16.1.7 del anexo A de la norma ISO 27001:2013, lo que podría generar pérdidas económicas y reputacionales para la entidad (anexo 4).

2.8.2.24. El procedimiento y los controles requeridos para asegurar la continuidad de los procesos, se encontraba en construcción; adicionalmente, no fue posible contar con la copia del borrador. La inexistencia del procedimiento y controles de los procesos de continuidad de negocio, implican un incumplimiento del requisito expuesto en el numeral 17.1.2 del anexo A de la norma ISO 27001:2013, lo cual podría generar imposibilidad en la continuidad de las operaciones en caso de presentarte situaciones adversas.

2.8.2.25. Se identificó que diferentes coordinaciones tienen acceso a las carpetas compartidas de otras áreas, permitiendo visualizar información reservada de la entidad que no les compete, como es el caso de temas de investigaciones disciplinarias, lo que podría redundar en pérdida en la confidencialidad de la información, esta situación se presenta debido a fallas en los controles de acceso de la información, incumpliendo el control establecido en el numeral 9.2.3 del anexo A de la norma ISO 27001:2013 (Anexo 5)

2.8.3. Créditos

2.8.3.1. En el área de Créditos se evidenció un equipo de cómputo sin bloqueo, con aplicaciones de software abiertas y desatendidas, incumpliendo el control descrito en el numeral 11.2.8 del anexo A de la norma ISO 27001:2013 situación que podría generar riesgos en cuanto al acceso indebido de la información (Anexo 7).

2.8.3.2 La puerta de acceso a las áreas donde se tiene información confidencial de créditos permanece abierta, no se dispone de mecanismos seguros que restrinjan el acceso a personal ajeno, incumpliendo lo establecido en el control 11.1.3 del anexo A de la norma ISO 27001:2013, lo que podría acarrear acceso indebido a instalaciones que cuentan con información confidencial y pérdida de esta (Anexo 8).

2.8.4. Fábrica de confecciones

2.8.4.1. Se evidenció que los funcionarios de la fábrica de confecciones que manejan el software relacionado con corte y bordados no han recibido formación en temas relacionados con Seguridad de la Información.

2.8.4.2. Se evidenciaron claves de acceso de los equipos de cómputo visibles, sobre las pantallas de los computadores que se encuentran en el área que maneja el software de corte, incumpliendo con el control relacionado en el numeral 9.3.1. de la norma ISO27001:2013 que establece el uso de información de autenticación secreta, lo que puede acarrear acceso indebido a la información de la entidad, así como perdida de la disponibilidad y confidencialidad de esta. (Anexo 9).

2.8.4.3. El locker en donde se almacenan las licencias originales del software de bordados no dispone de las seguridad; de igual manera, el acceso al lugar donde se realiza la programación de las máquinas de bordados carece de elementos físicos que restrinja el ingreso a personal no autorizado, incumpliendo lo establecido en el control 11.1.2 del anexo A de la norma ISO 27001:2013, lo que podría acarrear acceso indebido a instalaciones que cuentas con información confidencial y pérdida de la misma (Anexo 10).

2.8.5. Contratos

2.8.5.1. La puerta de acceso a áreas que manejan información confidencial permanece abierta, la documentación relacionada con los contratos se encuentra sin ningún tipo de seguridad, incumpliendo lo establecido en el control 11.1.3 del anexo A de la norma ISO 27001:2013, lo que podría acarrear acceso indebido a instalaciones que cuentan con información confidencial y pérdida de esta (Anexo 11).

2.8.5.2. Se evidenció un equipo de cómputo sin bloqueo, con aplicaciones de software abiertas y desatendidas, incumpliendo el control descrito en el numeral 11.2.8 del anexo A de la norma ISO 27001:2013 situación que podría generar riesgos en cuanto al acceso indebido de la información (Anexo 13).

2.8.5.3. No se evidenció la implementación del etiquetado de la información de acuerdo al esquema de clasificación de información definido por la entidad, incumpliendo el numeral A.8.2.2. del Anexo A de la ISO27001:2013, esta situación se presenta debido a que no se han desarrollado procedimientos de etiquetado de información física que contenga las características de

confidencialidad, lo que podría generar acceso indebido a la información. (Anexo 14).

3. Conclusiones y/o Recomendaciones

3.1. Conclusiones

Dentro del proceso de certificación ISO 27001:2013, la entidad cumple de manera general con las normar establecidas; sin embargo, se requiere:

- Normalizar la inexistencia de procedimientos informales, puesto que no contribuye en la validación del cumplimiento de las actividades y controles de estos. Los procedimientos formales, son requisito indispensable para garantizar el cumplimiento de la norma ISO 27001:2013.
- Identificar todo tipo de activos de información, junto con el cumplimiento de los controles de la norma es clave para el proceso de certificación.

3.2. Recomendaciones

- Complementar el inventario de activos de información, incluyendo los tipos definidos por la entidad (Información electrónica, Información física, Software, Hardware e Infraestructura) y para cada uno de ellos definir propietarios, custodios, riesgos, controles, validando sobre ellos la aplicabilidad de los 114 controles.
- Levantar los procedimientos definidos en el anexo A de la norma y aplicarlos en cada uno de los procesos relacionados con el manejo de información.
- Incluir las condiciones y responsabilidades de seguridad de la información dentro de la inducción inicial a nuevos funcionarios de la entidad.
- Documentar los estudios de seguridad que viabilizan el ingreso de funcionarios a la institución
- Definir los responsables funcionales y técnicos de las aplicaciones, garantizando la segregación de funciones
- Garantizar el cumplimiento de los procedimientos Gestión de Cambios y Gestión de Incidentes de Seguridad de la Información.
- Es importante que los logs de auditoría de las aplicaciones y gestión de vulnerabilidades en los diferentes sistemas informáticos sean revisados periódicamente, de tal forma que generen alertas tempranas que permitan reaccionar y corregir situaciones de riesgo.
- Generar políticas para el manejo de usuarios, roles y perfiles dentro de las aplicaciones tecnológicas y mantener la documentación actualizada de las mismas.

- Se sugiere que las bitácoras de registro de equipos de cómputo entrante y saliente sean revisadas periódicamente, para garantizar que los equipos de la entidad se encuentren debidamente controlados y evitar su pérdida.
- Se recomienda despejar de cajas y elementos que pueden interrumpir el correcto funcionamiento de los equipos de cómputo y que pueden generar incidentes de seguridad en los diferentes cuartos en donde se almacenan los racks de comunicaciones
- Actualizar los planos incluidos en el documento PR-3.5-02V3 "*Protocolo de seguridad para las instalaciones de la sede administrativa del Fondo Rotatorio de la Policía*", ya que la ubicación de los archivos físicos del primer piso, no corresponden y el área de telemática maneja una distribución diferente a la allí referida. (Anexo 15).