



SECRETARÍA  
JURÍDICA  
DISTRITAL

**INFORME DE AUDITORIA SISTEMA INTEGRADO LEGALBOG  
(EN DESARROLLO POR UNA ENTIDAD EXTERNA A LA  
SECRETARIA JURÍDICA DISTRITAL).**

Carrera 8 No. 10 – 65  
Código Postal: 111711  
Tel: 3813000  
[www.bogotajuridica.gov.co](http://www.bogotajuridica.gov.co)  
Info: Línea 195



Certificado No. SG 2018007982

2310300-FT-046 Versión 04



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA JURÍDICA DISTRITAL

## TABLA DE CONTENIDO

1. DATOS GENERALES.....	3
2. OBJETIVO.....	3
3. ALCANCE .....	3
4. CRITERIOS .....	3
5. PROCESO, UNIDAD Y/O ÁREA FUNCIONAL, PROGRAMA, PROYECTO DE INVERSIÓN O SISTEMA DE INFORMACIÓN A AUDITAR:.....	4
6. PROCEDIMIENTO, SUBUNIDAD Y/O ÁREA FUNCIONAL, SUBPROGRAMA, COMPONENTE Y/O SUBSISTEMA DE INFORMACIÓN A AUDITAR:.....	4
7. FORTALEZAS .....	4
8. NO CONFORMIDADES .....	4
9. OPORTUNIDADES DE MEJORA .....	5



SECRETARÍA  
JURÍDICA  
DISTRITAL

SECRETARÍA JURÍDICA DISTRITAL

EVALUACIÓN INDEPENDIENTE

INFORME DE AUDITORIA

1. DATOS GENERALES

Fecha: 09 de octubre 2020  
 Lugar: Oficina de Tecnologías de la Información y las Telecomunicaciones  
 Oficina Unión temporal Softmanagement supportical  
 Informe N°: 02  
 Cliente de la Auditoria: Oficina de Tecnologías de la Información y las Telecomunicaciones  
 Líder Auditor: Oscar Alonso Rodríguez Fontecha

2. OBJETIVO

Verificar la conformidad y cumplimiento de los requisitos de seguridad de la información establecidos en la política de seguridad de la información para la Secretaria Jurídica Distrital en el proyecto "Sistema integrado Legalbog (En desarrollo)".

3. ALCANCE

Sistema integrado LEGALBOG.

En el desarrollo de la presente Auditoria se presentaron las siguientes limitaciones que afectaron el alcance de la auditoria:

Debido a la emergencia sanitaria generada por la pandemia del COVID19, se dispuso aislamiento obligatorio, por medio de las siguientes normas nacionales y distritales:

Decreto 1109 del 10/08/2020 "Por el cual se crea, en el Sistema General de Seguridad Social en Salud – SGSSS, el Programa de Pruebas, Rastreo y Aislamiento Selectivo Sostenible – PRASS para el seguimiento de caos y contactos del nuevo Coronavirus – COVID-19 y se dictan otras Disposiciones".

Decreto Distrital 186 del 15/08/2020 "Por medio del cual se adoptan medidas transitorias de policía para garantizar el orden público en diferentes localidades del Distrito Capital y se toman otras determinaciones"

Decreto 1168 del 25/08/2020 "Por el cual se imparten instrucciones en virtud de la emergencia sanitaria generada por la pandemia del Coronavirus COVI-19, y el mantenimiento del orden público y se decreta el aislamiento selectivo con distanciamiento individual responsable"

Decreto Distrital 193 del 26/08/2020 "Por medio del cual se adoptan medidas transitorias de policía para garantizar el orden público en el Distrito Capital y mitigar el impacto social y económico causado por la pandemia de Coronavirus SARS-Cov-2 (COVID-19) en el periodo transitorio de nueva realidad"

Ello implicó que no se adelantaran ni entrevistas ni visitas físicas y se complementaran con actividades virtuales, y realizar análisis a la información allegada y publicada.

## 5. CRITERIOS

1. Norma ISO 27001:2013: Sistema de Gestión de Seguridad de la Información.
2. Políticas específicas de seguridad de la información para la implementación de controles de la norma ISO/IEC 27001:2013.
3. Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital".
4. Modelo de Seguridad y Privacidad de la Información - MSPI. MINTIC.
5. Resolución 184 de 2019 "Por la cual se adopta la Política General de Seguridad de la Información de la Secretaría Jurídica Distrital".
6. 2310200-MA-009 - Manual de políticas de seguridad de la información.
7. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"

## 5. PROCESO UNIDAD NO AREA FUNCION / PROGRAMA / PROYECTO DE INICIATIVA O SISTEMA DE INFORMACIÓN / PRODUCTO

Gestión de TIC

## 6. PROCEDIMIENTO / SUBPROCESO / AREA FUNCION / SUBPROYECTO / COMPONENTE O SUBSISTEMA DE INFORMACIÓN / PRODUCTO

Sistema Integrado LegalBog en desarrollo.

## 7. FORTALEZAS

- La OTI, cuenta con un Oficial de seguridad de la información.
- Disposición y compromiso por parte del responsable del proceso y de los profesionales del área, con relación a la atención de la auditoría y la entrega de información.
- Proposición de acciones de mejoramiento para dar cumplimiento a los criterios evaluados.

## 8. NO CONFORMIDADES



SECRETARÍA  
JURÍDICA  
DISTRITAL

SECRETARÍA JURÍDICA DISTRITAL

EVALUACIÓN INDEPENDIENTE

INFORME DE AUDITORIA

Como resultado de la revisión realizada a la documentación y evidencias recibidas sobre el Sistema integrado LegalBog, en desarrollo, se identificaron las siguientes no conformidades:

No se evidencia que se hayan realizado acciones para establecer el etiquetado de la información, lo cual incumple con lo establecido en el MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, numeral 8.2.2 *“El nivel de confidencialidad requerido para la información tratada por la Secretaría Jurídica Distrital, debe estar marcado en todas las páginas que contengan información confidencial y/o sensible y siempre de forma que resulte fácilmente legible.”* Al cumplir con este etiquetado se garantiza el manejo confidencial y seguro de la información sensible.

No hay evidencias de que se hayan realizado las pruebas solicitadas sobre (instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación de errores) al sistema de información Como lo determina el MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN en el numeral, 14.2.6. Prueba de Seguridad en los Sistemas de Información. Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software, criterios de seguridad y de calidad en el desarrollo de software. Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

No se evidencia la firma del formato Compromiso Confidencialidad de la Información - 2310200-FT-268, en el contrato de prestación de servicios No 060 de 2019, incumpliendo con lo establecido en el MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, numeral 15.2. *Tratamiento de Seguridad en los Acuerdos con Terceras Partes. En los Contratos o Acuerdos con terceras partes y que implique un intercambio, uso o procesamiento de información de la entidad, se debe contemplar la posibilidad de celebrar Acuerdos de Confidencialidad en el manejo de la información. Estos acuerdos deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio. El contrato o acuerdo debe definir claramente el tipo de información que intercambiarán las partes. De esta manera se garantiza la integridad y confidencialidad del código desarrollado y la información suministrada a los terceros.*

No se evidencia que se hayan realizado visitas anuales por parte del Oficial de Seguridad al proveedor del sistema legalbog, en cumplimiento de lo establecido en el documento de MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, numeral 15.2. *Tratamiento de Seguridad en los Acuerdos con Terceras Partes. El Oficial de Seguridad de la información, realizará una visita anual al proveedor, para revisar in situ el cumplimiento de la seguridad de la información del objeto contratado, el tratamiento de los riesgos que se encuentren dentro del acuerdo de servicios y adicionalmente, realizará el respectivo seguimiento a los planes de acción y remediación en tiempos prudentes definidos en conjunto con el proveedor.*

Como resultado de la revisión realizada a la documentación y evidencias recibidas sobre el Sistema integrado LegalBog en desarrollo, se identificaron las siguientes oportunidades de mejora:

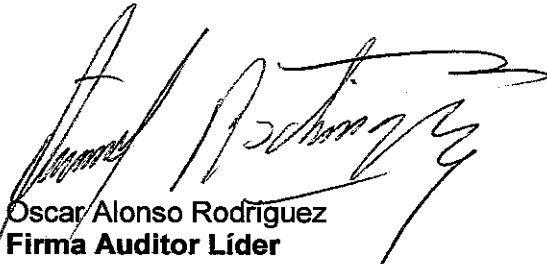
Definir entre el administrador de las Bases de Datos y el Oficial de Seguridad de la Información, las fechas de ejecución de las Copias de Respaldo (Backup), que se ajusten a la periodicidad definida en el MANUAL DE COPIAS DE RESPALDO, ya que se podría estar afectando la disponibilidad de la información del sistema.

Realizar una depuración, revisión y actualización de las VPN que se tienen asignadas al desarrollo del proyecto LEGALBOG, pues de acuerdo con la evidencia allegada se observa que

- Existen 43 accesos con relación a LEGALBOG.
- El campo accesos, se divide en: Pruebas LEGALBOG, LegalBog QA, Interventoria LEGALBOG, Pruebas Funcionales, LegalBog.
- De los 43 accesos, solo 4 tienen el campo de Fecha de vencimiento diligenciado.

Se debe limitar el acceso a la información de la entidad al mínimo requerido (principio del mínimo privilegio), para la realización de los roles o funciones, y de esta forma mitigar el riesgo frente a la afectación de la confidencialidad de la información por un mal uso de las cuentas de usuario genéricas las cuales impiden identificar un usuario responsable de la cuenta y su trazabilidad.

Determinar y documentar qué prácticas de desarrollo seguro se están implementando para mitigar las vulnerabilidades asociadas con problemas de memoria, privilegios y bypass de acceso.



Oscar Alonso Rodríguez  
Firma Auditor Líder



Dik Martínez Velásquez  
Firma Jefe Oficina de Control Interno