EMPRESA DE
RENOVACIÓN Y DESARROLLO
URBANO DE BOGOTA

COMUNICACIÓN INTERNA

Para : Ursula Ablanque Mejía – Gerente General
Gemma Edith Lozano Ramírez - Subgerente de Gestión Corporativa.
Luis E. Acosta Gutiérrez - Subgerente de Planeación y Administración de Proyectos

De : Janeth Villalba Mahecha - Jefe Oficina de Control Interno.

Asunto: **Informe de auditoría sobre el Sistema de Gestión de Seguridad de la Información.**

En el marco de los roles y competencias legales en materia de evaluación y seguimiento contenidas en el "*Artículo 2.2.21.5.3 De las oficinas de control interno*" del Decreto Nacional No. 648 de 2017 "*Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública*" atentamente se allega el Informe de Auditoría sobre el *Sistema de Gestión de Seguridad de la Información.*

Lo anterior con el propósito de que los resultados de la evaluación, las recomendaciones y sugerencias contribuyan a mejorar el desempeño, la toma de decisiones y la provisión de las instrucciones que sean del caso, toda vez que serán objeto de seguimiento durante los siguientes períodos.

Cordialmente,

Janeth Villalba M.

Janeth Villalba Mahecha
Jefe Oficina de Control Interno

EMPRESA DE
RENOVACIÓN Y DESARROLLO
URBANO DE BOGOTÁ

No: 20181100037303 Folios:1 Anexos:6
Fecha: 26/11/2018 3:24pm Cód veri: cc06b
Remitente: Ursula Ablanque Mejia UABLANQUEM

Anexo: Un (1) informe en tres (3) folios

	Nombre	Cargo	Dependencia	Firma
Elaboró:	Giovanny Mancera Marín	Contratista	Oficina de Control Interno	
Revisó:	Janeth Villalba Mahecha	Jefe	Oficina de Control Interno	
Aprobó:	Janeth Villalba Mahecha	Jefe	Oficina de Control Interno	
Los(as) arriba firmantes, declaramos que hemos revisado el presente documento y lo presentamos para su respectiva firma.				

Proceso Auditado y/o Tema Auditado	Gestión TIC´S / Seguridad de la Información
Auditor (es)	Giovanny Mancera Marín
Objetivo	Evaluar el Sistema de Gestión de Seguridad de la Información en su alcance correspondiente al proceso de Gestión de TIC de la Empresa de Renovación y Desarrollo Urbano de Bogotá, conforme a los requisitos legales vigentes de la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - MIN TIC.
Alcance	El alcance se definió para las fases de diagnóstico y planificación del Modelo de Seguridad y Privacidad de Seguridad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MIN TIC del proceso de Gestión de TIC de la Empresa de Renovación y Desarrollo Urbano de Bogotá.

METODOLOGIA
Técnicas de auditoría basados en los métodos de observación, confrontación, revisión y comparación. De acuerdo con las normas internacionales de auditoria, la presente es una auditoria de cumplimiento legal, es decir se verificará el cumplimiento del sistema, procedimientos, registros, instructivos y demás documentos que soporten el sistema.

NORMATIVIDAD
• Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". • Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". • Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC y se dictan otras disposiciones". • Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008". • Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la Protección de Datos Personales". • Ley 1712 de 2014. "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones". • Decreto 1377 de 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012". • Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012". • Decreto 2573 de 2014. "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones". • Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".

- Decreto 1078 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías Decreto de la Información y las Comunicaciones"
- Decreto 415 de 2016. "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".
- Decreto 1499 de 2017." Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
- Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital.
- Norma ISO 27001:2013. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos.

SITUACIONES GENERALES

- Se realizaron las actividades relacionados con el diagnóstico que conllevaron a determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.
- Se han asignado recursos (físicos, financieros, humanos) para llevar a cabo la planificación del Sistema de Seguridad de la Información en la entidad.
- Se resalta el esfuerzo en cuanto a la actualización de los procedimientos que hacen parte del Sistema de Gestión de Seguridad de la Información -SGSI.
- Se evidenció la disposición y colaboración por parte de los servidores públicos durante el desarrollo de la Auditoría, así como la atención, importancia y respeto que se dio durante el desarrollo de la misma.

SITUACIONES ESPECIFICAS - HALLAZGOS

Observación No 1. Documentación incompleta de componentes en la Fase de Diagnóstico

En la verificación de la fase de diagnóstico del Modelo de Seguridad y Privacidad de la Información – MSPI, se evidenció que de los tres (3) componentes exigidos, uno (1) no cumple con lo establecido en dicho modelo.

A continuación, se describe el estado actual de componentes y requisitos exigidos en la fase de diagnóstico del Modelo de Seguridad y Privacidad de la Información – MSPI:

COMPONENTE	ESTADO	Requisito MSPI
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Se observó que se realizó un diagnóstico sobre el estado de implementación del modelo de seguridad y privacidad de la información en la Empresa.	Diligenciamiento de la herramienta.

	Cumple	
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Se observó que, mediante la realización del diagnóstico sobre el estado de implementación del modelo de seguridad y privacidad de la información en la Empresa, se identificó el nivel de madurez de dicho modelo. **Cumple**	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Se observó que no se han realizado ejercicios de análisis de vulnerabilidades y ethical hacking a los diferentes equipos y dispositivos de red y seguridad informática. **No Cumple.**	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.

De igual modo, al carecer con el desarrollo de los componentes de la fase de diagnóstico se podría llegar a incurrir en una identificación errónea del estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Observación No 2. Documentación incompleta de componentes en la Fase de planificación.
En la verificación de la fase de planificación del Modelo de Seguridad y Privacidad de la Información – MSPI, se evidenció que de los nueve (9) componentes exigidos, cinco (5) no cumplen con lo establecido en dicho modelo.

A continuación, se describe el estado actual de componentes y requisitos exigidos en la fase de planificación del Modelo de Seguridad y Privacidad de la Información – MSPI:

COMPONENTE	**ESTADO**	**Requisito MSPI**
Política de Seguridad y Privacidad de la Información.	Existen una política de seguridad de la información y de tratamiento y protección de datos personales, las cuales fueron aprobadas y publicados en la intranet. No obstante, no han sido socializadas a los trabajadores oficiales y contratistas de la Empresa. **Cumple**	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.
Políticas de seguridad y privacidad de la información.	Se observó que existe una política general de Seguridad de la Información y de protección de datos personales	Manual con las políticas de seguridad y privacidad de la información, debidamente

	aprobadas. No obstante, no se cuenta con un Manual con las políticas de seguridad y privacidad de la información. **No cumple.**	aprobadas por la alta dirección y socializadas al interior de la Entidad.
Procedimientos de seguridad de la información.	Se evidenció que existen publicados cuatro (4) procedimientos asociados a seguridad de la información, los cuales son: PD-70 Soporte técnico y mantenimiento correctivo de dispositivos TI V2 PD-GT-ADIT-06 Adquisición de Infraestructura Tecnológica V1 PD-GT-CR-02 Copias de Respaldo V1 PD-71 Administración de Acceso Lógico V2 **Cumple.**	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información.	Se evidenció que no existe un documento oficial que incluya roles y responsabilidades en temas de seguridad de la información en la Empresa, revisado y aprobado por la Alta Dirección. **No Cumple.**	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.
Inventario de activos de información.	Se evidenció que existe un inventario de activos de información elaborado en la vigencia 2017. Sin embargo, se encuentra en proceso de actualización para la vigencia 2018. **Cumple.**	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.
Integración del MSPI, con el sistema de gestión documental de la entidad.	Para este componente no se evidenció avance.	Documento relacionado con seguridad de la información

	No cumple.	alineado con el sistema de gestión documental conforme a los parámetros emitidos por el Archivo General de la Nación.
Identificación, Valoración y tratamiento de riesgo.	la Empresa de Renovación y Desarrollo Urbano de Bogotá cuenta con un procedimiento denominado Administración del Riesgo con código PD-MC-AR-01 versión 1 del 18/05/2017, el cual se encuentra alineado a la gestión de riesgos a nivel general y no está enfocado a la identificación, evaluación, tratamiento y seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información. **No cumple.**	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.
Plan de Comunicaciones.	Se observó que se han enviado por correo electrónico información sobre seguridad de la información a los trabajadores oficiales y contratistas de la Empresa. No obstante, no existe un documento que contenga el plan de comunicación, sensibilización y capacitación. **Cumple.**	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
Plan de diagnóstico de IPv4 a IPv6.	Para este componente no se evidenció avance. **No Cumple.**	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

De igual modo, al carecer con el desarrollo de los componentes de la fase de planificación se podría llegar a incurrir en una elaboración errónea del plan de seguridad y privacidad de la información que no se encuentre alineado con los objetivos misionales de la entidad.

CONCLUSIONES
Evaluadas las fases de diagnóstico y planificación como alcance del Modelo de Seguridad y Privacidad de la Información conforme por lo establecido por el Min Tic, se concluye que existe un avance del 67% y 44%, respectivamente, de los componentes establecidos como marco de referencia.

RECOMENDACIONES

- Desarrollar un plan de trabajo enfocado a realizar un análisis de vulnerabilidades y pruebas de ethical hacking con el fin de Identificar vulnerabilidades técnicas y administrativas que se encuentran expuestos y comprometidos los diferentes componentes informáticos de la Empresa (equipos de red interna, aplicaciones web).
- Socializar y divulgar la política de seguridad de la información y de tratamiento y protección de datos personales a los trabajadores oficiales y contratistas de la Empresa.
- Documentar y socializar el manual que contenga las políticas de seguridad y privacidad de la información, debidamente aprobadas por la Alta Dirección.
- Elaborar un documento oficial que contenga los roles y responsabilidades establecidos para seguridad de la información en la Empresa aprobado por la Alta Dirección.
- Actualizar los activos de información de la Empresa.
- Realizar un plan de acción orientado a alinear el modelo de seguridad de la información con el sistema de gestión documental conforme a los parámetros emitidos por el Archivo General de la Nación.
- Enfocar el procedimiento actual de administración de riesgos a la identificación, evaluación, tratamiento y seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información.
- Elaborar e implementar un plan de comunicaciones relacionado con los temas de seguridad y privacidad de la información dirigido a todos los funcionarios, contratistas y terceros de la entidad.
- Elaborar un documento que contenga el Plan de diagnóstico para la transición del protocolo IPv4 a IPv6.
- Actualizar el Plan Estratégico de Tecnologías de la Información – PETI.
- Actualizar los riesgos del proceso conforme con lo establecido en la Guía para la Administración del Riesgos y el Diseño de Controles en Entidades Públicas Versión 4.

	Nombre	Responsabilidad	Firma
Elaboró:	Giovanny Mancera Marín	Auditor	
Reviso y Aprobó:	Janeth Villalba Mahecha	Jefe Oficina de Control Interno	