INFORME DE AUDITORÍA INTERNA No.: 16

FECHA DE EMISIÓN DEL INFORME	Día:	17	Mes:	08	Año:	2018

1. PROCESO:	**Gestión de Infraestructura y Tecnologías de Información.**
2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):	Director de Informática y Desarrollo
3. OBJETIVO DE LA AUDITORÍA:	Se evaluó la gestión del Proceso Gestión de Infraestructura y Tecnologías de Información, el cumplimiento de las normas aplicables y la gestión de la Seguridad de la información en los Grupos que participan en éste, y si su ejecución permitió contribuir a la mejora del Sistema de Gestión Integrado, del Sistema de Control Interno y la Gestión institucional.
4. ALCANCE DE LA AUDITORÍA:	Se realizó auditoría a la gestión del Proceso Gestión de Infraestructura y Tecnologías de Información, para el periodo comprendido entre el 17 de junio de 2017, al 17 de agosto de 2018, fecha de finalización de esta auditoría. El análisis de la información se efectuó mediante prueba selectiva y/o muestreo sobre las actividades realizadas durante el definido periodo. No se hizo necesario incorporar hechos adicionales que estuvieran por fuera del alcance de la evaluación adelantada. Para su desarrollo se aplicó la Guía de Auditoria para Entidades Públicas, Versión 2, expedida por el Departamento Administrativo de la Función Pública y los controles de Seguridad de la Información, contenidos en el Anexo de la Norma ISO 27001:2013.
5. CRITERIOS DE LA AUDITORÍA:	Se evaluó: 1. La adecuada aplicación de la normatividad legal vigente, así como los documentos contenidos en el Sistema de Gestión Integrado aplicables al proceso. 2. El cumplimiento de los Indicadores de Gestión establecidos para el Proceso, de conformidad con lo dispuesto en el Documento Guía para la Implementación de Indicadores de Gestión, Código: GC-G-001, Versión 005, así como el cumplimiento de las metas definidas. 3. Los Riesgos definidos y sus controles frente a la gestión desarrollada, de conformidad con lo dispuesto en el Documento Guía de Administración de Riesgos Institucionales, Código: GC-G-002, Versión 004.

	4. Los controles referidos en el Anexo A de la Norma ISO 27001:2013 numerales A.6.1.5, A.8.1.1, A.8.1.3, A.8.1.4, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.10.1.1, A.10.1.2, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.12.1.2, A.12.1.3, A.12.4.1, A.12.4.4, A.12.6.1, A.13.1.2, A.13.2.3, A.13.2.4, A.14.2.1, A.14.2.6, A.14.2.8, A.14.2.9, A.14.3.1, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 y A.16.1.7

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	23	Mes	07	Año	2018	Desde:	23/07/2018 D / M / A	Hasta:	16/08/2018 D / M / A	Día	17	Mes	08	Año	2018

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

En desarrollo de la auditoria, el equipo auditor destaca como aspecto fuerte, el compromiso y empoderamiento por parte del Director de Informática y Desarrollo, Líder Estratégico del Proceso, y los Coordinadores del Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones, y del Grupo de Sistemas y Arquitectura y Tecnología, al apoyar técnicamente la adquisición de nuevas tecnologías, lo cual fortalece la implementación del Sistema de Gestión de Seguridad de la información en la Entidad.

6.2 OBSERVACIONES

1. El equipo auditor observó que existen seis (6) usuarios habilitados para administrar la herramienta "Team Foundation Server (TFS)", quienes cuentan con el máximo nivel de permisos y privilegios para acceder a los códigos fuente de dicha herramienta sin limitación por proyectos. No se han configurado los roles y perfiles a cada uno de los administradores antes señalados. Esta situación puede generar un posible riesgo de fuga de información del código fuente.

2. El equipo auditor observó que no se cuenta con un documento o guía para la gestión que actualmente se desarrolla, para el manejo de medios removibles, disposición de medios y transferencia de medios físicos. Documento que se hace necesario para el adecuado desempeño de quien realiza esta función, o la pueda llegar a realizar.

3. El equipo auditor observó que no se han realizado visitas al proveedor que custodia las copias de seguridad, a fin de verificar el manejo dado a estos activos de información y las condiciones de control ambiental en las que se encuentran los mismos. Gestión que se convierte en buena práctica, y puede prevenir oportunamente la detección de alguna circunstancia que los afecte.

4. El equipo auditor observó que dentro de las políticas definidas en el Directorio Activo, no se ha implementado el parámetro de bloqueo de cuenta de usuario, ante un determinado número de intentos

6.2 OBSERVACIONES

fallidos para su acceso. Situación que minimizaría el posible riesgo de suplantación de usuario.

5. El equipo auditor observó la necesidad de llevar trazabilidad que dé cuenta del Qué. Quién, Cuándo y Cómo, de las políticas, reglas y cambios que se definan para el Firewall.

6. El equipo auditor observó que el formato "Acuerdo de Confidencialidad y Compromiso de Buen Uso de los Activos de Información", Código: GTH-F-026, no identifica el contrato al que pertenece, en caso de ser firmado por terceros, situación que impide verificar la trazabilidad del contrato al que corresponde.

7. Evaluados los riesgos de Seguridad de la Información definidos en el Sistema "Riesgos y Auditorias" para el proceso auditado, el equipo auditor observó lo siguiente:
   - No se determina la periodicidad de la gestión del control.
   - No se describe cuál es la evidencia de la gestión del control, ni su ubicación.

   Situación que puede generar incertidumbre sobre la huella que se debe conservar, como evidencia de la gestión realizada.

8. El equipo auditor observó que los eventos y Logs de la seguridad perimetral (Firewall) están cubiertos durante la jornada laboral. No obstante, en horas no laborales y fines de semana, la seguridad queda expuesta ante posibles hechos que puedan afectar la plataforma tecnológica de la Entidad al no existir un mecanismo de verificación.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
1. Control contra códigos maliciosos El equipo auditor evidenció que no existe un documento o guía de recuperación de la información ante ataques de virus y códigos maliciosos, conforme lo señala el literal e) del numeral 2.14.4 del Documento de Modelos, Código GC-MO-001. Adicionalmente no hay quien monitoree los Logs que genera el Antivirus Endpoint Protection, del System Center.	Documento de Modelos, Código GC-MO-001 Versión 003 literal e) del numeral 2.14.4 y NTC-ISO 27001:2013 A.12.2.1
2. Respaldo de la Información Dentro de la evaluación y aplicación de este control, el equipo auditor evidenció las siguientes debilidades: a. No se realizan pruebas trimestrales de recuperación y calidad de la información a las copias de seguridad.	A.12.3.1 y Procedimiento Respaldo y Recuperación de Datos de la Infraestructura Tecnológica, Código GINT-PR-001 Versión 002

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
b. Falta actualizar el procedimiento "Respaldo y Recuperación de Datos de la Infraestructura Tecnológica, Código GINT-PR-001, por cuanto: • Se está referenciando cintas como medio de respaldo que ya no se utiliza. • No se referencian los formatos GINT-F-011 Solicitud de Respaldo de Información, GINT-F-012 Programa de respaldo de Información y GINT-F-013 Registro de respaldo de la información, relacionados en la caracterización del proceso. c. Se están realizando copias de respaldo y enviando a custodia externa imágenes y archivos personales de los funcionarios, información que no está catalogada como crítica o sensible para la Entidad.	
3. Datos de Pruebas El equipo auditor evidenció que se generaron sesenta y dos (62) registros de pruebas en el aplicativo Postal, entre el 01 de agosto de 2017 y el 31 de julio de 2018, ejecutadas en ambiente diferente al de pruebas, que a la fecha de la auditoria no han sido anuladas. Registros que en su mayoría fueron generados desde la aplicación XBRL.	Procedimiento Adquisición, Desarrollo, Implementación y Mantenimiento de Sistemas de Información GINT-PR-003 numeral 2.6.2 punto 4
4. Control de la Información Documentada El equipo auditor evidenció que las platillas documentales de los BPM utilizados en los grupos de: Conciliación y Arbitramento, Apoyo Judicial, Gestión de Cobro Persuasivo y Coactivo e Investigaciones administrativas, no se encuentran actualizadas conforme a las aprobadas en el Sistema de Gestión Documental.	ISO 27001:2013 Numeral 7.5.3 literal e)

7. CONCLUSIONES DE LA AUDITORÍA

De la evaluación realizada a las actividades definidas dentro del alcance de la auditoria, el equipo auditor concluye que el grado de conformidad del proceso de Gestión de Infraestructura y Tecnologías de Información, cumple en términos generales con los criterios evaluados, no obstante, *se identifican ocho (8) Observaciones y cuatro (4) No Conformidades,* que requieren la estructuración de las acciones preventivas y correctivas necesarias, que permitan garantizar la mejora continua del proceso y por ende la madurez del

7. CONCLUSIONES DE LA AUDITORÍA

Sistema de Gestión Integrado, la Gestión Institucional y el Sistema de Control Interno.

Para constancia se firma en Bogotá D.C., a los 17 días del mes de agosto del año 2018.

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Arnulfo Suárez Pinzón	Jefe Oficina de Control Interno	
Wilma Rocío Pedrozo Ulloa	Auditor Líder	
Ángela Consuelo López Vargas	Auditor	
Miguel Dario Quintana Sánchez	Auditor	

9. ANEXOS

Sin.