INFORME DE AUDITORÍA INTERNA No.: 8

FECHA DE EMISIÓN DEL INFORME	Día:	25	Mes:	05	Año:	2017

1. **PROCESO:**	Sistema de Gestión de Seguridad de la Información ISO-IEC 27001:2013
2. **LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):**	Hoslander Adlai Sáenz Barrera
3. **OBJETIVO DE LA AUDITORÍA:**	• Determinar la conformidad del sistema de Gestión de Seguridad de la Información establecido en la entidad con los requisitos de la norma ISO-IEC 27001:2013. • Determinar la capacidad del Sistema de Gestión de la Seguridad de la Información para asegurar que la Organización cumpla con los requisitos legales y reglamentarios aplicables en el alcance del sistema.
4. **ALCANCE DE LA AUDITORÍA:**	Se realizó auditoría al Sistema de Gestión de Seguridad de la Información de la entidad, el análisis se efectuó mediante prueba selectiva a 20 hojas de vida de funcionarios y 8 de judicantes y pasantes de la vigencia 2016 a la fecha de auditoría y/o muestreo sobre las actividades realizadas durante el periodo comprendido entre Octubre de 2016 a Mayo de 2017 a los procesos de Gestión Integral, Infraestructura física, Infraestructura y tecnología de la Información, Talento Humano y Atención al Ciudadano; cubriendo la plataforma computacional, los activos de la información y los servicios de procesamiento de datos necesarios de acuerdo con la declaración de aplicabilidad GC-F-016 del 2016-09-30. Para la evaluación y análisis de la presente auditoría se aplicó la norma ISO 19011, versión 2012. No se consideró necesario incluir hechos adicionales en el desarrollo de la auditoría, a los ya definidos en el plan de trabajo.

5. CRITERIOS DE LA AUDITORÍA:	Verificar la adecuada aplicación de la norma de requisitos del SGSI aplicable a los procesos del alcance. Verificar la conformidad de la ISO-IEC 27001:2013 Numerales 4, 5, 6, 7, 8, 9 y 10. Verificar el cumplimiento del Plan de Mejoramiento establecido por la entidad a la Auditoría realizada por ICONTEC en el año 2016. Verificar la conformidad de la ISO 27002:2013 Anexo A numerales A7,A8,A9,A11,A16,A17y A18

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	15	**Mes**	05	**Año**	2017	**Desde:**	08/08/2017 D / M / A	**Hasta:**	25/05/2017 D / M / A	Día	31	Mes	05	Año	2017

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

No se encontraron aspectos a resaltar.

6.2 OBSERVACIONES

1. Se observó en el numeral 36 de la declaración de aplicabilidad, que se señala como implementación del control el formato 46001, este código corresponde a un trámite denominado autorización de servicios automáticos, que se encuentra referenciado en la tabla de retención documental y forma parte de la información que sirve de control al procedimiento.

Igualmente en el numeral 21 de la declaración de aplicabilidad, se menciona el Procedimiento Clasificación y Etiquetado como parte del Proceso de Gestión Documental, siendo este, actualmente parte del documento GC-DP-002 Identificación Gestión y Clasificación de Activos de Información a cargo del proceso de Gestión Integral, es preciso hacer los ajustes pertinentes, para brindar información veraz en el documento inicialmente mencionado.

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
1. DEBILIDAD EN LOS CONTROLES DEFINIDOS PARA LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN. El equipo auditor evidenció que a la fecha de la auditoria se llevan en la oficina de Control disciplinario, cinco (5) procesos por vulnerabilidad a la seguridad de la información, situación que muestra debilidad en los controles establecidos para los riesgos del Sistema de Gestión de Seguridad de la Información.	Guía Administración de Riesgos Institucional GE-G-004 numeral 8.1 Fortaleza del control
2. INCUMPLIMIENTO AL PROCEDIMIENTO GUÍA PARA CONTRASEÑAS SEGURAS. El equipo auditor evidenció en la guía para contraseñas seguras, numeral 2.6 que se utiliza como control establecido en la declaración de aplicabilidad para el cumplimiento del numeral 9.4.3 anexo A, que no se está cumpliendo con el procedimiento de cambio de contraseñas, el cual establece que "Las contraseñas tendrán un periodo de vigencia de CUARENTA Y CINCO (45) días, fecha en la cual se obligará a cambiarse de acuerdo con las mejores prácticas y políticas de seguridad, de lo contrario se desactiva la cuenta" , situación que denota debilidad en el control establecido.	Guía de contraseñas de Seguras GINT-G-001 Numeral 2.6
3. FALTA DE CONOCIMIENTO Y TOMA DE CONCIENCIA SOBRE LAS POLÍTICAS DE SI: A pesar que la entidad realiza capacitación a los funcionarios nuevos y ha efectuado re inducción a algunos funcionarios antiguos sobre la política de Seguridad de la información, se evidenció falta de conocimiento y de toma de conciencia por parte de los funcionarios entrevistados; teniendo en cuenta que en el desarrollo de la auditoria se indagó sobre el tema y no se obtuvo respuesta al respecto, situación que indica debilidad en el control A.7.2.2 Educación, formación, y concientización sobre la Seguridad de la información.	ISO-IEC 27001:2013 Numeral 7.3 literal a Declaración de Aplicabilidad ISO-IEC 27001:2013 Anexo A.7.2.2 Educación, formación y concientización sobre la Seguridad de la información
4. USUARIOS ACTIVOS EN EL SISTEMA: Dentro de la muestra analizada por el equipo auditor en cuanto a los usuarios activos en los sistemas de Información de la entidad se encontraron 3 usuarios que ya terminaron su vínculo con la entidad hace 6 meses, 2 meses y 12 días respectivamente, entre los cuales se encuentran 2 personas con acceso privilegiado de administrador del sistema, lo anterior incumple el control A.9.2.6 Retiro o ajuste de los derechos de acceso.	ISO-IEC 27001:2013 Anexo A A.9.2.6 Política de acceso a los Sistemas 2.3.4

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
5. ACUERDO DE CONFIDENCIALIDAD: Se evidenció que los pasantes y judicantes no están firmando oportunamente el formato GTH-F 026 - Acuerdo de confiabilidad y compromiso de buen uso de los activos de información, como lo establece el procedimiento GTH -PR-001- Cooperación Académica institucional (Pasantías y Judicantes), situación que se comprobó en cuatro judicantes que están bajo la Dirección de la Delegatura de Procedimientos de Insolvencia, quienes firmaron el acuerdo en un lapso de dos (2) a seis(6) meses, después de que estos judicantes han tenido autorización de servicios informáticos por parte de la Dirección de informática, para manejar información confidencial teniendo acceso a los diferentes sistemas de la entidad autorizados mediante el trámite 46001.	Documento de Políticas 2.3.5 Política de seguridad del talento humano Documento de Políticas SGI 2.3.1 Política de organización de seguridad de la información Procedimiento GTH-PR-002 Procesos Gestión del Talento Humano.
6. POLITICA DE ESCRITORIO LIMPIO : El equipo auditor evidenció que en 9 equipos revisados a funcionarios de los Grupos de Atención al Ciudadano, Administrativo y Notificaciones, se encontraron documentos de Word, Excel, música con información de carácter personal; Igualmente se encontraron 2 equipos desatendidos por parte de sus usuarios sin bloqueo de sesión en la ausencia de los mismos, lo anterior incumpliendo la política de escritorio despejado y pantalla limpia, numeral 2.3.3 del Documento de Políticas de Gestión Integral, donde dice "todo usuario dentro de la Superintendencia de Sociedades deberá conservar la pantalla libre de accesos directos a información no pública (confidencial) de los funcionarios o de la compañía"; situación que se presentó por desconocimiento de las políticas de seguridad de la información al interior de los grupos.	Documento de Políticas de Gestión Integral numeral 2.3.3 ISO-IEC 27001:2013 A..11.2.9 Política de escritorio limpio.
7. SEGURIDAD FISICA Y AMBIENTAL. CONTROLES FISICOS DE ENTRADA : De la visita in situ realizada a las instalaciones de la superintendencia de Sociedades el día 19 de Mayo de 2017, recorrido realizado con el coordinador del Grupo Administrativo, el supervisor de la empresa de seguridad y un funcionario de la Oficina de Control Interno, en la cual se revisaron los protocolos de seguridad teniendo como pauta el instructivo de ingreso a las instalaciones (GINF-1-001) del 7 de Abril de 2017, se evidenció lo siguiente: • Incumplimiento a la Norma técnica NTC- ISO – IEC 27001, Numeral A 11, Seguridad física y Ambiental, control Anexo A 11.1.2, de igual forma al	ISO–IEC 27001:2013 A 11 Controles

6.3 NO CONFORMIDAD

DESCRIPCIÓN	NORMATIVIDAD INCUMPLIDA
sótano, declarado zona segura, 23 vehículos sin la respectiva tarjeta de acceso. (ver cuadro anexo) • Falta de control del ingreso de vehículos de visitantes dentro del perímetro de la entidad, se evidencio que el vehículo de placas BSQ 068, ubicado en el sector de parqueo de visitantes, no se encontraba registrado en el libro de minutas de ingreso de visitantes, por lo que se procedió a la revisión de las cámaras de seguridad para su respectiva identificación de ingreso logrando comprobar que efectivamente se trataba de un visitante. • El Vehículo BYL 708, ubicado en sector de parqueo de visitantes. El propietario del vehículo se identificó como funcionario y en el momento del recorrido el vehículo no contaba con la respectiva tarjeta de autorización de acceso.	física Instructivo Ingreso Instalaciones Código GINF-1-001 2.2.2.3 literales a,b,c,g,
8. PERÍMETRO SEGURIDAD FÍSICA: Dentro de las áreas seguras se encuentran los cuartos de UPS y banco de baterías. En el recorrido realizado el día 24/05/2017, con el coordinador Grupo Administrativa se encontró la puerta de la planta eléctrica de corriente regulada sin candado y el cuarto planta circuito de emergencia el cual cuenta con chapa de seguridad abierto. De acuerdo con la norma Técnica NTC-ISO-27001, se deben definir y usar perímetros de seguridad y usarlos para proteger áreas que contengan información confidencial. Se debe proporcionar protección física contra los accesos que no estén autorizados. La protección tiene que ser proporcional a los riesgos identificados.	ISO–IEC 27001:2013 A 11 Seguridad física y Ambiental A 11.1.1Perímetro de seguridad física Instructivo Ingreso Instalaciones Código GINF-1-001 2.3 literales e
9. PLAN DE MEJORAMIENTO : Se evidenció que en el Plan de Mejoramiento correspondiente a la Auditoría ICONTEC vigencia 2016, están vencidas 13 acciones a realizar y no se cuenta con los soportes en la herramienta Share point.	ISO-IEC 27001:2013 Numeral 10.1 literal f
10. ÁREAS DE ACCESO PÚBLICO, CARGA Y DESCARGA: De acuerdo con la norma Técnica NTC-ISO-27001, Cualquier área de carga y descarga de material u otro tipo de punto de acceso público debería estar aislado y distante del lugar donde se encuentran áreas seguras, así como cualquier material que entre a la entidad deberá ser registrado y revisado para protegerla de cualquier amenaza. El parqueadero sótano está dentro de las zonas seguras, sin embargo se evidencio el descargue de materiales fuera de la zona de carga y descarga e ingresando por el parqueadero del sótano,	Norma técnica NTC- ISO – IEC 27001 Numeral A 11 Seguridad física y Ambiental A 11.1.6 Áreas de acceso público. Carga y descarga Instructivo Ingreso Instalaciones Código GINF-1-001 2.2.2.4 literales a

6.3 NO CONFORMIDAD	
DESCRIPCIÓN	**NORMATIVIDAD INCUMPLIDA**
estas labores sin ningún acompañamiento por el personal de seguridad (ver foto archivo digital).	

7. CONCLUSIONES DE LA AUDITORÍA

Las actividades auditadas a los procesos de Gestión Integral, Infraestructura física, Infraestructura y tecnología de la Información, Talento Humano y Atención al Ciudadano, se desarrollaron conservando los parámetros establecidos para el cumplimiento del objetivo del sistema, en este sentido, el grado de conformidad del mismo cumple en términos generales con los criterios evaluados en la presente auditoría. No obstante, se identificaron no conformidades las cuales impiden tener la gestión del Sistema totalmente asegurada. Por lo anterior, se deben estructurar las acciones preventivas para la observación identificada y las acciones correctivas para las no conformidades que permitan garantizar la mejora continua de los procesos y por ende la maduración del Sistema de Seguridad de la Información.

Para constancia se firma en Bogotá D.C., a los 25 días del mes de mayo del año 2017

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Arnulfo Suárez Pinzón	Jefe Oficina de Control Interno	
Myriam del Carmen Berdugo S	Líder de Auditoría	
Lola Graciela Venegas Castro	Auditor	
Luis Miguel Delgadillo Perez	Auditor	

9. ANEXOS

HALLAZGO 7. SEGURIDAD FISICA Y AMBIENTAL. CONTROLES FISICOS DE ENTRADA

Parqueadero sótano (Área Segura), placas de los vehículos que no contaban con la tarjeta de autorización de acceso vehicular entregado por la entidad:

ZYM 377	RJM 307	CZP 587
BVF 289	OBH 519	COA 614
BLB 073	OBH 186	EKH 774
RNX 891	HYQ956	HJF 467
RCQ 051	DPX 289	RCL 962
BRF 219	IWZ 607	INY 813
UCK 593	JEK 014	MCU 875
ZZK 013	LKZ 088	

Total 23 Vehículos

Parqueadero (exterior) placas de los vehículos que no contaban con la tarjeta de autorización de acceso vehicular entregado por la entidad:

BMW 361	BJE 805	RAS 235
DOY 667	CCX 701	VCR 443
RLL 270	UCY 865	CZN 871
DUH 031	GGK 956	ZYP 337
DBO 427	BYA 705	BPH 635
DON 229	IXP 027	JEP 533
BYS 587	IJO 257	MCU579
HJM 129	JFN 491	

Total 23 Vehículos

Vehículo parqueado en zona de visitantes que según los vigilantes pertenece a un funcionario sin embargo no contaba con la tarjeta de autorización de acceso vehicular entregado por la entidad: BYL 708

Vehículo parqueado en zona de visitantes el cual no cuenta con registro en el libro de visitantes BSQ 068