

INFORME DE AUDITORÍA N° 18 de					
 2015092111246932143120096 comunicaciones internas o memorandos Septiembre 21, 2015 11:24 Radicado 2015-020096 2015092111246932143120096					
		<small>Bello Ciudad Educativa y Competitiva</small>	<small>CD-SC-CER143989</small>	<small>SC-CER143668</small>	<small>GP-CER143691</small>

Bello, 15 de Septiembre de 2015

Doctor
CARLOS MUÑOZ LÓPEZ
 Alcalde
 Municipio de Bello

Asunto: Auditoría de seguimiento y evaluación al sistema de seguridad informática.

Respetado Doctor Muñoz:

La Secretaría de Control Interno con fundamento en la ley 87 de 1993, artículo 9, practicó Auditoría de seguimiento y cumplimiento al sistema de seguridad informática de la Administración del Municipio de Bello.

La auditoría se llevó a cabo de acuerdo a las normas de auditoría generalmente aceptadas y según el artículo 3 del decreto 1537 de 2001 que enmarca el rol de Control Interno y requirió del procedimiento P-02, documentado en el Sistema Integrado de Gestión en el proceso Evaluación Independiente, que involucra la planeación, ejecución e informe de la Auditoría.

La auditoría incluyó el análisis de las evidencias frente a los criterios establecidos, el cual brinda un nivel de confianza de los controles a los riesgos y a la evaluación y seguimiento de los procesos que operan en la Administración Central del Municipio de Bello, determinando las debilidades que repercuten en la prestación de servicios y cumplimiento de la normatividad vigente.

Como resultado se identificaron 3 conformidades, 5 debilidades y 1 observación en materia de mantener la integridad, confidencialidad y disponibilidad para toda la información institucional relevante.

Como conclusión del proceso auditor, la entidad presenta serias falencias en materia de seguridad informática, por lo tanto, requiere la implementación de políticas de seguridad informática, para dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que puedan afectar a la Alcaldía Municipal de Bello, por esto, preparar y capacitar al personal en temas asociados a la seguridad informática y cómo afrontar incidentes que se llegarán a presentar con el fin de responder de una manera adecuada.

Código: F-EI-09	Versión: 05 Fecha de aprobación: 2013 / 06 / 12	Página 1 de 8
-----------------	--	---------------



**INFORME DE AUDITORÍA N° 18 de
2015**

**Seguimiento y Evaluación al
sistema de seguridad informática**



CO-SC-CER143888



SC-CER143666



GP-CER143891

Con el fin de lograr que la labor de auditoría conduzca a que se emprendan actividades de mejoramiento de la gestión pública, la Secretaría de Servicios Administrativos del Municipio de Bello deberá suscribir en un plazo de 20 días calendario con la Secretaría de Control Interno el correspondiente Plan de Mejoramiento en formato establecido en el procedimiento de Auditoría de control Interno del proceso de Evaluación independiente, que permita subsanar las Debilidades puntualizadas.

JORGE IVAN GIRALDO FLÓREZ
Secretario de Control Interno

JUAN CARLOS VÉLEZ MESA
Subsecretario de Evaluación

Copia a: Doctor Carlos Mario Garcés Díaz, Secretario de Servicios Administrativos.
Doctor Alejandro Posada Mejía, Director Administrativo de Sistemas.



**INFORME DE AUDITORÍA N° 18 de
2015**

**Seguimiento y Evaluación al
sistema de seguridad informática**



CO-SC-CER143688



SC-CER143688



QP-CER143691

SECRETARIA DE CONTROL INTERNO

JORGE IVÁN GIRALDO FLÓREZ
Secretario

JUAN CARLOS VÉLEZ MESA
Subsecretario de Evaluación

SEBASTIAN GAVIRIA LÓPEZ
Auditor Líder
Contratista

JUAN CARLOS VÉLEZ MESA
JOSE HELI VARGAS HINCAPIE
Auditores Acompañantes

Bello
Septiembre 15 de 2015

Código: F-EI-09

Versión: 05
Fecha de aprobación: 2013 / 06 / 12

Página 3 de 8



INFORME DE AUDITORÍA N° 18 de 2015

Seguimiento y Evaluación al sistema de seguridad informática



CO-SC-CER143588



SC-CER142688



GP-CER143891

1. OBJETIVO GENERAL DE LA AUDITORÍA

Evaluar los niveles de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios que desarrolla el Municipio de Bello, mediante el resguardo de los activos de información.

2. CRITERIOS

La Secretaría de Control Interno en su proceso de auditoría verificará el cumplimiento de las normas, políticas, procedimientos y requisitos de acuerdo a lo establecido en:

- Ley 1266/2008, Habeas Data.
- Ley 1273/2009.
- Decreto 1377/ 2013.
- P02 para la gestión tecnológica.

3. ALCANCE

La presente auditoría se delimita a la dirección administrativa de sistemas y apoyo tecnológico, secretarías de despacho, subsecretarías responsables de la seguridad de la información mantener la confidencialidad, la disponibilidad e integridad de la misma.

4. GENERALIDADES

4.1. METODOLOGÍA

Para la realización de la auditoria se solicita información a la entidad, se procede al análisis documental, elaboración de plan de auditoría, lista de chequeo, realización de reuniones con los líderes o responsables de las áreas correspondientes, con el fin de aplicar la metodología determinada (entrevista, encuesta u otros instrumentos) para obtener la evidencia física o electrónica, para construir el informe final de auditoría.

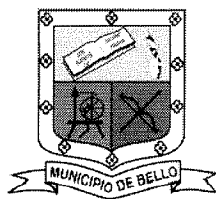
5. RESULTADO DE LA AUDITORIA

Como resultado de la Auditoria, se evidenciaron:

Código: F-EI-09

Versión: 05
Fecha de aprobación: 2013 / 06 / 12

Página 4 de 8



INFORME DE AUDITORÍA N° 18 de 2015

Seguimiento y Evaluación al sistema de seguridad informática



CO-SC-CER143688



SC-CER143688



GP-CER143691

5.1. CONFORMIDADES

- 5.1.1. Se evidencia cumplimiento del control de ingreso a los usuarios al sistema, lo cual consiste en que después de 3 intentos consecutivos fallidos de ingreso al sistema, se bloquea el acceso del usuario y el desbloqueo se realiza por el administrador y/o responsable de la información como lo estipula el "Procedimiento para la gestión tecnológica en el numeral 4.2.5.3 Controles automáticos y de usuario, Ítem 2".
- 5.1.2. Se evidencia que la Dirección Administrativa de Sistemas dispone en las dependencias consideradas críticas para la gestión de los sistemas de información, de puertas de seguridad, cumpliendo con el "Procedimiento para la gestión tecnológica en el numeral 4.2.6.4 Control de acceso físico".
- 5.1.3. La entidad maneja correctamente los mecanismos de control de acceso lógico como lo son los Proxys, además en caso de no contar con estos, establece la conexión a "Internet" en un equipo independiente a la red de comunicaciones de la Alcaldía Municipal de Bello, el cual contempla el "Procedimiento para la gestión tecnológica en el numeral 4.2.7.2 Conexiones con redes públicas e Internet, Ítem 1".

5.2. DEBILIDADES

- 5.2.1 No se evidenció planes de contingencia y de recuperación documentada y actualizada, de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre, incumpliendo el "Procedimiento para la gestión tecnológica en el numeral 4.2.6.6 Planes de emergencia, contingencia y recuperación, ítem 1".
- 5.2.2 No se evidenció en las áreas de los servidores, donde se maneja "Información Confidencial o Crítica", cámaras que registren las actividades realizadas por los funcionarios para mantener la protección física de la información, incumpliendo el "Procedimiento para la gestión tecnológica en el numeral 4.2.6.4 Protección física de la información, ítem 3".
- 5.2.3 No se evidenció que la desconexión de equipos de seguridad instalados para el monitoreo y control de las comunicaciones, sea autorizado por el área de Auditoría, como medida de control, incumpliendo el "Procedimiento para la gestión tecnológica en el numeral 4.2.7.4 Outsourcing, ítem 4".

Código: F-EI-09	Versión: 05 Fecha de aprobación: 2013 / 06 / 12	Página 5 de 8
-----------------	--	---------------



INFORME DE AUDITORÍA N° 18 de 2015

Seguimiento y Evaluación al sistema de seguridad informática



CO-SC-CER143688



SC-CER143688



GP-CER143691

5.2.4 No se evidenció logs de auditoría para los sistemas automáticos que operan y administran “Información Sensible”, como son sistemas de aplicación en Producción, Sistemas Operativos, Sistemas de Bases de Datos y Telecomunicaciones, incumpliendo el “Procedimiento para la gestión tecnológica en el numeral 4.2.5.4 Logs, ítem 1”.

5.2.5 No se evidenció que se llevó a cabo copias adicionales de “Información Sensible” que se registren en un log, donde se indique el número de copias y la cantidad de receptores de éstas, lo cual permite tener la relativa seguridad de que la información que se esta manejando en la gestión de consulta es veraz, incumpliendo el “Procedimiento para la gestión tecnológica en el numeral 4.2.5.4 Logs, ítem 10”.

5.3. OBSERVACIONES

Actualmente el área de sistemas de la entidad, puede dar mejor aprovechamiento en el uso de las Tecnologías de Información, constatando que se lleven a cabo las mejores prácticas y se sigan los procedimientos que aseguren la veracidad, confidencialidad, confiabilidad, disponibilidad de la información y verificación de los controles internos establecidos en el área de Sistemas, así como el estudio de seguridad física y lógica, el análisis de los riesgos a que está expuesta la información y los equipos de cómputo, garantizando de esta manera la prevención ante posibles contingencias que puedan impedir la continuidad del uso de los recursos informáticos.

5.4. CONCLUSION

Como resultado de la auditoria actualmente la entidad se encuentra en un *Nivel Aceptable* en la seguridad informática, presentando falencias en los controles de acceso, planes de contingencia, monitoreo de donde se maneja información crítica; básicamente donde se encontró mayor debilidad de los activos informáticos de la entidad, radica en que no se está llevando el debido proceso que se encuentra documentado y estructurado sobre las políticas de seguridad informática estipulado en el formato “P02 para la gestión tecnológica”, la cual nos indica de manera coordinada como llevar los debidos procesos para conservar la integridad, confidencialidad y disponibilidad para toda la información institucional relevante, además traería consigo mejorar las demás falencias, ya que estarían debidamente identificadas.



INFORME DE AUDITORÍA N° 18 de 2015

Seguimiento y Evaluación al sistema de seguridad informática



CO-SC-CER143666



SC-CER143666

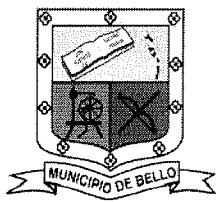


GP-CER143691

6. RECOMENDACIONES

La Secretaría de Control Interno de la Alcaldía Municipal, producto de la presente auditoría, presenta las siguientes recomendaciones para la mejora de los sistemas de seguridad informática:

- 6.1. Reforzar los puntos débiles tales como: planes de emergencia, contingencia y recuperación, el monitoreo y mantenimiento a la protección física de la información, registro de los movimientos de la información sensible; ya que la entidad tiene información sensible que se debe resguardar, frente a una serie de amenazas que es importante proteger, además de disminuir incidencias de seguridad.
- 6.2. Sensibilizar a los funcionarios del Municipio de Bello, periódicamente sobre una correcta y responsable administración y protección del software institucional y de la información que a través de éste se maneja, con el fin de que se operen eficientemente los sistemas de información.
- 6.3. Realizar capacitaciones periódicamente para el debido manejo de información institucional, procedimientos, protocolos para evitar pérdidas, accesos no autorizados y utilización indebida de la misma.
- 6.4. Restringir que un usuario maneje simultáneamente sesiones múltiples en línea, a menos que se tenga un permiso especial concedido por el administrador del sistema.
- 6.5. Eliminar los privilegios automáticamente, cuando no han tenido actividad durante un periodo de 8 días calendario, y no realizarse por medio de talento humano.
- 6.6. Incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debiera limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los diferentes procesos de la entidad.
- 6.7. Desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos municipales críticos.
- 6.8. Brindar capacitación a todos los funcionarios del municipio y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos



**INFORME DE AUDITORÍA N° 18 de
2015**

**Seguimiento y Evaluación al
sistema de seguridad informática**



CO-SC-CER143683



SC-CER143888



GP-CER143891

organizacionales conforme sea relevante para su función laboral.

7. DOCUMENTOS DE REFERENCIA

- ISO/IEC 27000-series
- ISO/IEC 27001
- ISO/IEC 27002
- COBIT
- ITIL
- ISO/IEC 20000

Sebastian Gaviria Lopez

SEBASTIAN GAVIRIA LÓPEZ
Contratista, Profesional Universitario
Auditor Líder

Jose Heli Vargas Hincapie

JOSE HELI VARGAS HINCAPIE
Contratista, Profesional Universitario
Auditor

Juan Carlos Vélez Mesa

JUAN CARLOS VÉLEZ MESA
Subsecretario de Evaluación
Auditor