INFORME DE AUDITORÍA INTERNO

INFORME DE AUDITORÍA INTERNA AL SGSI CON BASE EN LA NORMA ISO 27001:2013

MAYO 18 AL 21 DE 2015

ABC S.A.

BOGOTA D.C. COLOMBIA

1 INTRODUCCIÓN

1.1 Objeto de la Auditoría

Identificar el nivel de cumplimiento del Sistema de Gestión de la Seguridad de la Información (SGSI) de ABC S.A. con respecto a los controles y cláusulas de la norma internacional ISO 27001 versión 2013.

1.2 Alcance de la Auditoría

El alcance del SGSI está definido como: "los sistemas de información que apoyan el proceso de **"Gestión de Servicios de Call Center"**, los cuales se especifican a continuación:

- E-Client
- Request Tracker
- Correo Electrónico".

1.3 Fecha de la Auditoría

Las actividades de auditoría fueron ejecutadas los días 18,19,20 y 21 de mayo de 2015.

1.4 Lugar

La auditoría al SGSI fue realizada en las oficinas de ABC S.A. incluyendo visitas a los centros de cómputo principal y de contingencia.

1.5 Areas Auditadas

Se auditaron todas las áreas de ABC S.A. que están relacionadas con el alcance del SGSI, es decir:

- Administrativa y Financiera
- Tecnología
- Call Center
- Recursos Humanos

1.6 Equipo Auditor

La auditoría fue ejecutada por el auditor Renán Quevedo Gómez.

1.7 Personal Auditado

Se auditó al siguiente personal de ABC S.A.

- Gerente General
- Director Administrativo y Financiero
- Director de Recursos Humanos
- Director de Tecnología
- Director de Call Center
- Coordinador de Recursos Humanos

- Coordinador de Sistemas
- Auxiliar de Selección
- Ingeniero de Mantenimiento
- Ingeniero de Soporte
- Coordinador de Sistemas
- Coordinador de Campañas Bancarias
- Agenes de Call Center

2 HALLAZGOS DE AUDITORÍA

Hallazgos de Auditoría				
ID	**Hallazgo**	**Numeral de la Norma**	**Descripción**	**Tipo de Hallazgo**
1	Contacto con las autoridades	A.6.1.3	No se encuentra evidencia suficiente de que exista un contacto con las autoridades ni procedimientos que especifiquen en qué momento y quién debe contactar a las autoridades y cómo deben ser reportados los incidentes de seguridad a tiempo.	**No Conformidad Menor**
2	Propietario de los activos	A.8.1.2	No se ha asignado un propietario a los activos	**No Conformidad Menor**
3	Gestión de derechos de acceso privilegiado	A.9.2.3	Esto se ha venido haciendo bajo necesidad y de acuerdo al criterio del administrador de dominio, esto debe establecerse en un procedimiento para garantizar que los derechos de acceso son restringidos y controlados.	**No Conformidad Menor**
4	Revisión de los derechos de acceso de usuarios	A.9.2.5	No se ha contemplado en ninguna política la revisión de los derechos de acceso de manera periódica, esto debe ser definido e implementado. Puede considerarse la inclusión de este control dentro de la política de control de acceso que está planeada para ser implementada.	**No Conformidad Menor**
5	Contacto con grupos de interés especial	A.6.1.4	Teniendo en cuenta que la organización tiene planeada la tercerización de la atención de incidentes de seguridad, puede evaluarse la posibilidad de exigir a los posibles proveedores que hagan parte de un CERT reconocido por FIRTS.	**Oportunidad de Mejora**
6	Inventario de Activos	A.8.1.1	Este control se aplica de manera intuitiva sin embargo es recomendable que se establezca un procedimiento para que sea repetible, se pueda gestionar y medir y posiblemente posteriormente automatizar.	**Oportunidad de Mejora**
7	Uso de información de autenticación secreta	A.9.3.1	Para lograr aumentar el nivel de madurez de este control se recomienda incluirlo en una política específica y dentro del temario de concienciación y capacitación.	**Oportunidad de Mejora**
8	Procedimiento de ingreso seguro	A.9.4.2	Se recomienda implementar un procedimiento que permita medir y mejorar este control.	**Oportunidad de Mejora**
9	Uso de programas utilitarios privilegiados	A.9.4.4	La revisión y gestión de la consola centralizada del antivirus se hace solamente por demanda y a criterio del administrador, es aconsejable madurar este control por medio de un procedimiento y guías de revisión y gestión de la consola de antivirus u otras herramientas de apoyo.	**Oportunidad de Mejora**
10	Protección contra las amenazas externas y ambientales	A.11.1.4	Se ha implementado este control por demanda, sin embargo no hay una revisión periódica ni se encuentra definido formalmente.	**Oportunidad de Mejora**

Hallazgos de Auditoría				
ID	**Hallazgo**	**Numeral de la Norma**	**Descripción**	**Tipo de Hallazgo**
11	Servicios de suministro	A.11.2.2	Se cuenta con UPS suficientes para dar autonomía a los servidores así como redes reguladas de energía. Sin embargo no está definido formalmente el mantenimiento y gestión de estos equipos.	**Oportunidad de Mejora**
12	Disposición segura o reutilización de equipos	A.11.2.7	El área de tecnología tiene la costumbre de hacer un borrado a bajo nivel de los discos duros de equipos de personal que se retira de la compañía o en el caso de reasignación de equipos. Sin embargo no está formalizado.	**Oportunidad de Mejora**
13	Controles contra códigos maliciosos	A.12.2.1	Se tiene implementada una solución de antivirus centralizada y administrada por el área de tecnología, esto cubre los servidores y equipos de escritorio. Sin embargo no está formalizada su gestión y medición de desempeño.	**Oportunidad de Mejora**
14	Sincronización del relojes	A.12.4.4	Está implementado pero se aconseja que se formalice su implementación y se inicien mediciones de efectividad del mismo.	**Oportunidad de Mejora**
15	Separación en las redes	A.13.1.3	Ha sido implementado por necesidad, sin embargo no está formalizado ni documentado.	**Oportunidad de Mejora**
16	Planificación de la continuidad de la seguridad de la información	A.17.1.1	La organización tiene desarrollado un un Plan de continuidad de negocio en donde tiene en cuenta ciertos controles de seguridad de acuerdo con el criterio del área de tecnología.	**Oportunidad de Mejora**
17	Implantación de la continuidad de la seguridad de la información	A.17.1.2	Si bien existe el BCP, este no detallad de manera explícita procesos, procedimientos y controles para mantener la seguridad de la información durante una situación adversa. Los controles implementados han sido elegidos por el área de tecnología.	**Oportunidad de Mejora**

Tabla 1 Hallazgos de Auditoría

3 CONCLUSIONES

Dentro de la auditoría realizada al Sistema de Gestión de Seguridad de la Información de ABC S.A. realizada entre el 18 y 21 de mayo de 2015, no se encontraron no conformidades mayores, se encontraron 4 conformidades menores y 13 oportunidades de mejora.

Como observación general debe decirse que debido al estado inicial del SGSI, el 59% de los controles de la norma se encuentran en estado de implementación dentro de lo establecido por ABC S.A en su plan de tratamiento de Riesgos, en esta auditoría inicial no se catalogan como no conformidades pero debe tenerse en cuenta que en futuras auditorías al sistema se espera que el nivel de madurez de dichos controles ya haya aumentado.

FIN DEL INFORME