Ministerio de Comercio Exterior COMEX

AUDITORIA INTERNA

Estudio de la Seguridad de la información sobre la plataforma tecnológica principal de COMEX, mediante la contratación externa de Auditores especialistas.

AUD-INF-ENV-0004-2019

Noviembre, 2019

TABLA DE CONTENIDOS

25 de noviembre de 2019

1. INTRODUCCIÓN

Las tecnologías de información (TI) constituyen una de las principales herramientas de trabajo que apoyan la gestión de COMEX, en la toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance.

Actualmente cuenta con varios sistemas: el Archivo digital institucional, ADI, un sistema de Administración de Correspondencia, SADCOR, el Sistema de Excelencia Operacional, OPPEX y otros sistemas, en la plataforma Sharepoint, los cuales contienen toda la información relevante que ingresa y la que se genera en la organización, por lo que es de gran importancia conocer, si los mismos cumplen con requerimientos de seguridad adecuados.

El Manual de Auditoría Interna, MARPAI, emitido por la CGR en el año 2018, menciona, la importancia de que el equipo de Auditoría tenga conocimientos suficientes de los riesgos y controles claves en tecnología de la información, conocimiento obtenido mediante especialistas internos o externos, siempre y cuando se trate de personal calificado, que no tenga impedimentos que afecten su independencia y objetividad.

La Unidad de Tecnología de Información considerando la migración del trabajo manual a electrónico, debe cumplir con una serie de estándares que aseguren la confiabilidad y resguardo de la información.

En el mes de setiembre 2019 con el aval del Viceministro, se tramitó una solicitud de servicios para la contratación de servicios de auditoría, para el desarrollo de esta Auditoría, aplicando los procedimientos de contratación por excepción a los procedimientos ordinarios, regulados en el artículo 139, inciso p) que dice:

> "Artículo 139.-**Objetos de naturaleza o circunstancia concurrente incompatibles con el concurso**. La Administración, podrá contratar de forma directa los siguientes bienes o servicios que, por su naturaleza o circunstancias concurrentes, no puede o no conviene adquirirse por medio de un concurso, así como los que habilite la Contraloría General de la República… inciso p) **Asesoría a Auditorías Internas**: La Auditoría Interna y los órganos de control podrán contratar servicios profesionales especiales para sus investigaciones, cuando la confidencialidad o agilidad así lo amerite."

La contratación directa N° 2019 CD-00077-000770000 "Servicio de Auditoría Externa sobre la seguridad informática", recayó en la empresa Deloitte & Touche, la cual cumplió suficientemente con el cartel de dicha contratación.

2. OBJETIVOS DEL SERVICIO DE AUDITORÍA

2.1 Objetivo general

La contratación de la Auditoría pretende conocer el estado general de la plataforma tecnológica con el fin de identificar oportunidades de mejora relacionadas con la confidencialidad, integridad y/o disponibilidad de la información de la organización."

2.2 Objetivos específicos:

- ✓ Identificar las vulnerabilidades relacionadas con la seguridad informática, que puedan ser aprovechados por atacantes externos e internos y pongan en riesgo la información institucional.

- ✓ Obtener información que sirva para conocer la razonabilidad de los controles establecidos sobre la plataforma tecnológica de COMEX.

- ✓ Dar recomendaciones focalizadas en las mejores prácticas, de conformidad con los estándares internacionales, en temas de gestión de la seguridad informática.

3. ALCANCE Y PERIODO DEL SERVICIO DE AUDITORIA

El estudio se realizó entre el mes de octubre y noviembre 2019 y abarcó:

- ✓ Revisiones en sitios web, realizadas externamente.
- ✓ Revisiones internas en equipos pertenecientes a la red internos.
- ✓ La revisión del proceso de gestión de accesos de red y en las aplicaciones utilizadas para la gestión documental empresarial y las configuraciones de la suite de servicios de Office 365.

3.4 Fuentes de criterio.

Para las evaluaciones se aplicó la metodología NIST 800-115

3.5 Metodología.

La realización del estudio fue contratada externamente y se solicitó a la empresa considerar, lo establecido en el Manual de Auditoría Interna MARPAI, emitido por la Contraloría General de la República en el año 2018 y se siguieran las fases:

Fase I Planeación
Fase II Examen
Fase III Comunicación de resultados

4. COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DEL SERVICIO.

El 04 de noviembre se remitieron al Departamento de Informática 4 informes preliminares, correspondientes a:

- ✓ Pruebas de intrusión red interna.
- ✓ Pruebas de intrusión red externa.
- ✓ Análisis del proceso de gestión de accesos de red y aplicaciones.
- ✓ Análisis de configuraciones de seguridad G.

Los resultados preliminares del estudio fueron presentados el 11 de noviembre por los Auditores de Deloitte, al Señor Minor Salazar, Jefe a.i. del Departamento de Informática, al señor Alfonso Chaves, funcionario del Departamento de Informática a cargo de los servidores institucionales, la señora Mariela Rojas, Oficial Mayor y Directora Administrativa y a la señora Marielos Gómez, Secretaría Técnica del CISED, quiénes manifestaron su conformidad con los resultados del estudio y las recomendaciones vertidas en el mismo.

5. CONCLUSIÓN GENERAL

Basados en el alcance del estudio, así como en las pruebas de auditoría realizadas, los resultados del estudio fueron razonables.

No obstante, se determinaron oportunidades de mejora relacionados con:

- ✓ El acceso no autorizado desde la infraestructura externa.
- ✓ El acceso no autorizado a sistemas críticos de la red interna.
- ✓ El proceso de gestión de accesos de red y en las aplicaciones de gestión documental.
- ✓ La configuración de seguridad de los equipos.

Tabla I Resultados de la evaluación de criterios para el servicio

#	COMPONENTE EVALUADO	RESULTADO DE LA EVALUACIÓN
1	Resultados Generales de las pruebas externas	Cumple parcialmente
2	Resultados Generales de las pruebas internas	Cumple parcialmente
3	Resultados Generales de las pruebas de configuración de seguridad.	No Cumple
4	Resultados Generales de la revisión de procesos y gestión de accesos	Cumple parcialmente

Fuente: Elaboración propia a partir de los resultados del informe presentado por la empresa Deloitte, sobre los resultados de las pruebas de auditoría desarrolladas.

6. RESULTADOS

6.1 Aspectos que fortalecen el Sistema de Control Interno

- ✓ La compra de un servidor que ingreso a la institución a finales de octubre, viene a contribuir a implementar las recomendaciones del informe, al poder migrar algunos de los sistemas que actualmente están almacenados en servidores, que se encuentran en estado de obsolescencia.

- ✓ Actualmente está en proceso de contratación el mantenimiento para la herramienta OPPEX, desarrollada en Share Point y al servidor Active Directory el mantenimiento lógico, en el cual, se mantienen todos los usuarios de acceso a la red, la seguridad de usuarios y otras aplicaciones de COMEX.

- ✓ Para el mes de diciembre se contrató el desarrollo y la migración de las herramientas SADCORD, ACCD, el SAT y SISPAD.

- ✓ Se incluyó en el plan de compras para el año 2020 la compra de un servidor físico para trasladar el Active Directory, debido a que el actual no tiene garantía ni servicio de soporte técnico.

6.2 Aspectos susceptibles de mejora

Anexo se remite el informe ejecutivo emitido por la empresa Deloitte, que incluye los resultados generales de las pruebas realizadas en cada una de las fases de análisis de la seguridad. Asimismo, se anexa un informe completo para cada una de las fases indicando las vulnerabilidades encontradas en cada una de las pruebas. Cada informe incluye los objetivos, el alcance, la metodología, las herramientas utilizadas, introducción y leyenda para describir los atributos de las observaciones, la calificación de riesgo, los resultados de las pruebas, un detalle de las vulnerabilidades, las conclusiones y en algunos casos un glosario de términos.

Los informes que se anexan son los siguientes:

1. Anexo No. 1 Informe Ejecutivo Análisis de Seguridad COMEX
2. Anexo No. 2 Informe de Pruebas de Penetración Red Externa
3. Anexo No. 3 Informe de Pruebas de Penetración Red Interna
4. Anexo No. 4 Informe de Revisión de Procesos, COMEX
5. Anexo No. 5 Informe de Políticas de Conformidad Suite Microsoft COMEX

7. RECOMENDACIONES

6.3 Al Viceministro de Comercio Exterior,

Girar las instrucciones a quien corresponda, a efecto de:

6.3.1 Someter al conocimiento y valoración del Comité Asesor de Tecnologías de información, CATI, ampliado con un representante de las áreas sustantivas cada uno de los informes emitidos por Deloitte.

6.3.2 Elaborar un plan de implementación de las recomendaciones emitidas en cada uno de los informes, incluyendo un cronograma de actividades, indicando plazos y responsables de su ejecución.

6.3.3 Justificar en forma escrita y suficientemente aquellas recomendaciones que no se van a implementar o su implementación será parcial, con respecto a lo recomendado en el informe.

6.3.4 Valorar si el incidente analizado en este estudio, relacionado con el acceso a información privada de funcionarios de COMEX, específicamente la carpeta "Mis Documentos", requiere de alguna acción por parte de la administración, de conformidad con lo establecido en el artículo 102, incisos a), b) y c) de la Ley General de la Administración Pública, o bien, de conformidad con el código de ética institucional.