UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

AUDITORÍA DE LA SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA PRIVADA COSTARRICENSE

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar al grado y título de **Maestría Profesional en Auditoría de Tecnologías de Información.**

SUSTENTANTE:

Roy Hernaldo Chavarría Barquero

Ciudad Universitaria Rodrigo Facio, Costa Rica

Abril 2018

DEDICATORIA

A Jesucristo, mi Señor y Salvador.

A mi amigo fiel, el Espíritu Santo y a mi Padre Celestial, al cual rindo mis logros dándole toda la gloria y honra, gracias por Tu infinita misericordia, Tu gran amor y Tu fidelidad, por guiarme en todo momento, por no soltarme en los momentos de debilidad y darme las fuerzas para no desfallecer.

A mis padres, Jesús Chavarría y Luvi Barquero, a quienes amo con todo mi corazón y son ejemplo para mi vida del esfuerzo y perseverancia. Gracias por la ayuda y motivación de que se pueden lograr las cosas cuando uno se las propone.

A mis hermanos y hermanas, quienes son inspiración para mi vida y me hacen ser mejor cada día.

AGRADECIMIENTOS

A Dios, por darme las fuerzas y sabiduría para salir adelante cada día.

A mi familia, por todo el apoyo que me brindan día a día.

A Rebeca, por su comprensión en todo este proceso y por motivarme a realizar cosas con excelencia.

A mis compañeros de la maestría en Auditoría de Tecnologías de Información, que me brindaron su apoyo y me enseñaron mucho durante todo este proceso. Sé que más que un aprendizaje, obtengo amistades muy especiales.

A Marco V. Gámez Acuña, por su valiosa y profesional ayuda, y por guiarme en este camino.

A Gino Ramírez y a los profesores de la Universidad de Costa Rica, por su valioso aporte y exigencia en mi formación profesional.

A Pablo Betrano y Juan Miranda, quienes me brindaron su colaboración para que este proyecto fuera exitoso.

Gracias a todos por su ayuda, apoyo y enseñanzas, guardan un lugar valioso en mi corazón; nuevamente, gracias.

HOJA DE APROBACIÓN

"Este Trabajo Final de Investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información".

_____

M.Sc Gino Ramírez Solís

Profesor - Coordinador

_____

M.Sc. Marco V. Gámez Acuña

Tutor

_____

Pablo Betrano Machado

Lector

_____

M.Sc. Ridiguer Artavia Barboza

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Roy Hernaldo Chavarría Barquero

Sustentante

TABLA DE CONTENIDO

RESUMEN

Este proyecto tiene como objetivo evaluar la seguridad de la información relacionada con el proceso de administración de nóminas realizado por la organización auditada, mediante buenas prácticas de seguridad de la información.

Para ello se realizó un programa de trabajo, en el cual se detallaron las diferentes actividades a evaluar, agrupándose en tres etapas, donde la primera de ellas consistió en determinar el alcance de la iniciativa de aseguramiento, seguido por el entendimiento de los habilitadores, establecimiento de criterios de evaluación y la aplicación de las evaluaciones, por último, se comunicaron los resultados obtenidos de las evaluaciones aplicadas.

En la realización de las diferentes tareas que se ejecutaron, se crearon papeles de trabajo para facilitar el análisis de la información y respaldo de auditoría, las plantillas de estos papeles de trabajo se encuentran detalladas en el capítulo 4. Estas plantillas son de fácil comprensión y aplicación, además se introducen con una breve explicación de la finalidad de cada una de ellas.

Una vez recolectada la información por medio de las plantillas, se procedió a una etapa de análisis, con el fin de detectar posibles debilidades en los controles de la seguridad de la información. Cada brecha encontrada como resultado del análisis se documentó como un hallazgo de auditoría, donde se muestra el criterio con el que se realizó la evaluación, el estado actual del control y el riesgo resultante si se materializa el evento descrito. Además, se realizó una serie de recomendaciones con el fin de mitigar el riesgo encontrado. Todo esto se documentó en el informe final de la auditoría.

Por último, se brindan las conclusiones del trabajo realizado, así como las recomendaciones para las personas competentes, según los resultados del estudio aplicado, con el fin de reforzar la seguridad de la información en la compañía.

ABSTRACT

The objective of this project is to assess the security of information related to the payroll administration process carried out by the audited organization, through good information security practices.

To this end, a work program was carried out detailing the different activities to be evaluated, grouped into three stages, where the first step was to determine the scope of the assurance initiative, followed by the understanding of the enablers, establishment of criteria for evaluation and application of the evaluations, finally, the results obtained from the evaluations applied were communicated.

To the different tasks executed to complete this project, I created work papers to facilitate the analysis of the information and audit support, the templates of these work papers are in chapter 4. These templates are easy to understand and application, they are introduced with a brief explanation of the purpose of each of them.

Once it information was collected through the templates, an analysis stage was carried out in order to detect possible weaknesses in information security controls. Each gap found in the analysis, it was documented as an audit finding, showing the criteria with which the evaluation was conducted, the status of the control and the resulting risk if the described event materializes. In addition, a series of recommendations were made to mitigate the risk found. All this information was documented in the final report of the audit.

Finally, the conclusions of the work carried out are provided, as well as the recommendations to the competent people according to the results of the applied study, in order to reinforce the security of the information in the company.

CAPÍTULO 1 - Introducción

Objetivos

Objetivo general

Realizar una auditoría de la seguridad de la información en una empresa del sector privado costarricense, con el fin de determinar la suficiencia de las actividades de control ejecutadas para preservar la confidencialidad, integridad y disponibilidad de la información.

Objetivos específicos

1. Determinar los principales riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información.
2. Evaluar lo adecuado del proceso interno actual para administrar la seguridad de la información de la empresa y datos del Sistema de Administración de Nóminas.
3. Aplicar las técnicas y normativas asociadas con el tema tratado, que permitan determinar la suficiencia de la seguridad de la información y emitir recomendaciones de los aspectos encontrados sujetos a mejora.

Alcance y limitaciones del proyecto

El proyecto se desarrolla en el periodo que abarca de diciembre 2017 a abril de 2018, para el análisis de actividades e información se contempla lo generado o actuado en relación con el proceso de “Administración de Nóminas” para el período comprendido entre enero y diciembre del 2017. No serán analizadas las

bases de datos provenientes de otros servicios o sistemas propios de la empresa que no tengan relación con el Sistema de Administración de Nóminas.

Considerando que la empresa no cuenta con un marco de seguridad propio, su accionar en materia de seguridad de la información se valora contra los criterios expuestos en el documento “COBIT 5 para la seguridad de la información”, específicamente en su sección II “Uso de habilitadores de COBIT 5 para implementar la seguridad de la información en la práctica, capítulo 2 “Catalizador: Principios, Políticas y Marcos de Referencia”, que es referente a las Políticas de Seguridad de la Información, el cual toma en cuenta los principios de COBIT 5. Como parte de los procesos de COBIT 5 para ser utilizados como base para formar parte de los criterios de evaluación en esta auditoría, se utiliza el proceso DSS05 “Gestionar los Servicios de Seguridad”. Además, se toman en cuenta los aspectos básicos de la norma ISO 27001 “Gestión de la Seguridad de la Información”, así como prácticas documentadas o no que realiza la empresa para su gestión del proceso evaluado, entre ellas:

- RRH-PO-01 Políticas Internas.
- STT RRH-PO-06 Políticas de privacidad y tratamiento de datos personal STT Regional.
- SIF-PO-02 Política para uso tecnológico (seguridad de la información).

Justificación

Este trabajo es de gran importancia para la empresa, puesto que al concluirse le permitirá conocer los aspectos que se pueden mejorar para obtener una seguridad razonable de la información que maneja en la base de datos auditada y brindar un mejor servicio a sus clientes.

La sociedad costarricense también se verá beneficiada con una empresa más madura en el tratamiento de los datos de sus clientes, lo cual incrementará el nivel de confianza en el servicio brindado, además de cumplir con normativa del país en materia de protección de datos personales.

Metodología

Clasificación de la investigación

Tipo de Método

Según su profundidad u objeto, se puede catalogar como descriptiva (Barrantes, 2009), ya que describe una condición encontrada, que se valora contra unos criterios normativos establecidos que rigen el tema evaluado tanto a nivel interno como externo (ámbito costarricense) y de ahí se emiten aspectos de mejora, si así se determina.

Desde su alcance temporal se considera como una investigación transversal o sincrónica (Barrantes, 2009), ya que se realiza en un momento dado (diciembre 2017 hasta abril 2018) y los datos o situaciones analizadas también pertenecen a un periodo dado (enero-diciembre de 2017).

Tipo de investigación

Este trabajo es una investigación aplicada, por cuanto se aplica el conocimiento adquirido durante la maestría a un caso real en una organización costarricense, con la finalidad de detectar aspectos sujetos a mejora en el control interno del lugar donde se aplica. El estudio realizado no pretende aportar un conocimiento teórico nuevo al campo de la auditoría, sino atacar potenciales problemas generadores de riesgo en el tema evaluado, que en este caso es la seguridad de la información en una empresa privada costarricense.

Tipo de enfoque

Respecto a su enfoque o medición, se considera cualitativa, ya que se describirán situaciones ordinarias de la institución evaluada sin cuantificar o manipular datos numéricos específicos, más que los que se observan o responden a instrumentos cualitativos. Tiene lugar en el campo y no en un laboratorio, con situaciones naturales y libertad de acción de los observados.

Fuentes de información

Existen dos tipos de fuentes básicas que todo proyecto debe tener: primarias y secundarias, éstas se describen seguidamente:

Fuentes primarias

Las fuentes primarias proporcionan datos de primera mano, pues se trata de documentos que contienen datos propios de la empresa donde se desarrolla el proyecto y de personas que realizan las actividades a evaluar.

Fuentes secundarias

La información de fuentes secundarias se obtendrá por medio de información suministrada en sitios de Internet tales como: leyes, reglamentos, jurisprudencia, que sustentarán los criterios y las actividades de control interno a evaluar.

También se consideran fuentes secundarias el COBIT 5 y la ISO 27001, si bien son mejores prácticas aceptadas mundialmente, no son propias de la empresa a evaluar.

Técnicas e instrumentos para la recolección de información

Para esta investigación se emplean una serie de métodos o instrumentos distintos para recopilar información, entre ellos: observación, el análisis de documentación de la empresa y recolección de datos recopilados con los papeles de trabajo diseñados y aplicados.

La observación

Se observará al personal involucrado en el proceso de administración de nóminas y al personal encargado de la gestión de TI, con el fin de obtener información de interés relativa al proceso realizado y para determinar la suficiencia y cumplimiento de los controles implantados para la seguridad de la información.

Análisis de contenido

Se realiza un análisis de los documentos propios de la empresa, para obtener un amplio conocimiento de las políticas y procesos que se ejecutan en la organización; así como las fuentes secundarias de información citadas anteriormente, con el fin de determinar si las políticas de la compañía se alinean con las mejores prácticas existentes.

Entrevistas

Se entrevista al personal encargado de la gestión de TI, al coordinador del departamento de TI y a usuarios respecto a su percepción de la gestión de TI y cualquier otro personal de interés; para obtener un mejor entendimiento de los procesos realizados por la compañía.

Plantillas de trabajo

Se elaboran papeles de trabajo para evaluar o describir condiciones encontradas, listas de verificación, cuadros, resúmenes de información recopilada, resultados de pruebas, hojas de recolección de hallazgos, etc.

Detalle de la metodología

El plan de auditoría se realiza conforme a los lineamientos establecidos en el procedimiento “GES-PR-02 Procedimiento de Auditoría Interna. V2” de la organización, en el cual indica lo que deben contener las auditorías:

Plan de auditoría

Aquí se describen las actividades que se llevan a cabo en la auditoría. Como se indicó en el apartado anterior, la planificación se desarrollará de acuerdo con el formulario propio de la compañía “GES-FO-04 Plan de auditoría V2”, el cual debe contener:

- Objetivo
- Alcance

- Norma de Referencia
- Auditados y Auditores
- Fecha y horario de la Auditoría
- Cronograma de Auditoría: fecha, hora, proceso, numerales aplicables, criterios de la auditoría, Auditado y Auditor.

Además, en esta etapa se pueden desarrollar listas de verificación si así se estima conveniente, para las diferentes actividades a auditar, en un formato similar al que se presenta en el “GES-FO-09 Listas de verificación”.

Ejecución de la auditoría

La actividad de ejecución se debe realizar conforme al programa elaborado en la etapa de planificación. Las actividades dispuestas se ejecutan en forma ordenada, lo cual conlleva a realizar pruebas, evaluar controles y recolectar la evidencia necesaria mediante la utilización de técnicas y prácticas de auditoría para determinar, justificar y presentar apropiadamente los hallazgos de auditoría, con sus atributos de criterio, condición, causa y efecto. Todos los hallazgos deben ser claramente documentados, referenciando los documentos, materiales, registros y cualquier otro aspecto revisado.

En la ejecución se aplican todos los papeles de trabajo diseñados en la etapa de planificación y cualquier otro requerido de acuerdo con los hallazgos encontrados, esto siguiendo el debido proceso tanto de la ejecución como en la recolección de la evidencia.

Informe

Con base en las observaciones y hallazgos encontrados, se debe elaborar el “GES-FO-08 Informe de Auditoría”. Dentro de este informe, se deben incluir los hallazgos, conclusiones y recomendaciones.

CAPÍTULO 2 - Perspectivas teóricas

Estado de la cuestión en Costa Rica

La información es de gran valor para las organizaciones, sin importar el tipo de actividad a la que se dedique, sea una institución pública o privada, la información se ha convertido en su activo más valioso y alguien puede estar interesado por obtenerla. Por esta razón, es que las compañías han realizado esfuerzos para protegerla de terceros y mantenerla disponible, confiable e íntegra.

En Costa Rica se han realizado esfuerzos para responder ante incidentes relativos a la seguridad de la información.

Desde el año 2012, se realizó la publicación oficial de la creación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT), que entre sus objetivos se encuentran el promover una cultura nacional de seguridad cibernética e informática, así como proponer guías para la evaluación de los programas interinstitucionales en materia de seguridad de tecnologías de la información y comunicación.

Pese a que existen esfuerzos en el país, el CSIRT se ha quedado corto, ya que muchos especialistas en seguridad de la información manifiestan que el CSIRT no ha avanzado como ellos han querido.

Las instituciones, por su lado, han tomado la iniciativa por sus propios medios de asegurar su información, algunas con éxito, pero otras han tenido incidentes que los han afectado, como el caso de Deloitte, donde su correo electrónico corporativo fue atacado por un hacker que comprometió la confidencialidad y planes de algunos de sus clientes. Los 244 000 correos de sus empleados fueron almacenados por el hacker, que obtuvo acceso de administrador que le otorgaba acceso sin restricciones. Algunos de los correos que fueron comprometidos, contenían adjuntos con detalles de seguridad y datos sensibles de sus clientes.

Las empresas tienen presente que pueden ser atacadas externamente en cualquier momento, pero no todo ataque ocurre fuera de la organización. Muchas veces, los empleados acceden a datos a los cuales no deberían hacerlo, lo que puede causar fuga de la información. De acuerdo con la revista IT Now, (Boris,

2017) señala que un informe elaborado por Forcepoint, sobre el Estado de la seguridad cibernética, muestra que “Las fugas de información causadas por empleados de las organizaciones suele tener un costo promedio de US$5 millones”. (párr. 1)

Existen diferentes normas y marcos que ayudan a las organizaciones a establecer controles adecuados para asegurar la información, entre ellos se encuentra COBIT, con sus principios, políticas y marcos de referencia con respecto a la seguridad de la información en la empresa. Por otro lado, se encuentra la familia de normas ISO 27000, que establece un sistema de gestión de seguridad de la información y a nivel nacional, la Contraloría General de la República publicó, en el 2007, las Normas Técnicas para la gestión y control de las tecnologías de información.

Historia de la empresa

Grupo STT se especializa en funcionar como un agente catalizador, que se encarga de enlazar diversas oportunidades de empleo, que ofrecen sus clientes de renombre, con el talento humano de quienes aspiran por un trabajo digno, retador y gratificante, que les permita magnificar su potencial.

La empresa evaluada se dedica a la tercerización de procesos. Esta compañía es de capital costarricense y se encuentra en todo el continente americano, teniendo sus orígenes en año 1999.

A través de quince años de arduo trabajo, STT ha logrado posicionarse como una de las organizaciones más importantes en los diferentes mercados donde tiene operaciones, promoviendo la calidad en el servicio y el trabajo, a través de gente de talento, lo que ha permitido su expansión.

Manteniendo siempre una exitosa relación con empresas y marcas renombradas y emergentes, nacionales e internacionales, Grupo STT asegura que sus cimientos se basan en la búsqueda de nuevas oportunidades y una proyección más amplia hacia el mercado.

La estrecha relación y excelencia en el servicio que brinda a sus clientes, tanto nacionales como internacionales, son los que respaldan las bases de la compañía y amplía la proyección en el mercado.

Las oficinas centrales están ubicadas en San José, Costa Rica, 100 metros oeste de la estación de Bomberos de Tibás.

Visión

"Posicionarnos como aliados de preferencia de nuestros clientes, agregando valor a sus procesos e innovando servicios". (Quienes somos, párr.3)

Misión

"Satisfacer las necesidades de nuestros clientes, por medio de procesos en una constante búsqueda del mejoramiento continuo". (Quienes somos, párr.2)

Valores

Grupo STT indica que la compañía cuenta con tres valores distintivos, los cuales son:

- ✓ Servicio**.**
  - o "Vocación de servicio para atender las necesidades de nuestros clientes tanto internos como externos".

- ✓ Talento.
  - o "Reconocer la necesidad de un trabajo desafiante brindando oportunidades de desarrollar el talento potencial".

- ✓ Trabajo.
  - o "Creemos en la sinergia. Es un compromiso de ser eficaces y eficientes trabajando juntos".

Servicios

La compañía cuenta con una variedad de servicios que ofrece a las empresas para el crecimiento económico de las mismas, estos servicios son:

HRO (Sub contratación de personal)

Se realiza la contratación de personal de acuerdo con la solicitud del cliente. La empresa prestataria (STT Group) asume toda la responsabilidad laboral y administrativa. La empresa usuaria de este servicio dirige la inducción, supervisa y asigna materiales, dicta políticas, etc.

STT Group asigna un supervisor en el sitio, según lo amerite la operación.

RPO (Reclutamiento y selección de personal)

Consiste en la equiparación de currículos con perfiles, entrevista estructurada, aplicación de pruebas psicométricas, pruebas psicomotoras, de percepción y habilidad, pruebas de conocimiento del trabajo, chequeo de referencias y entrevista por el cliente.

PPO (Administración de Nómina)

STT se encarga de la administración de nómina, es decir, hace el proceso de preparación, pago y contabilización de nómina en los periodos y modalidades acordadas, de acuerdo con las obligaciones obrero y patrón.

Los sistemas de información permiten agilizar el procesamiento de los datos, reportes históricos de ingresos y salidas, lo que permite que se adapten a los requerimientos de cada cliente.

BPO (Administración de Procesos)

A diferencia del HRO, en este servicio, STT brinda todas las herramientas de trabajo, incluyendo infraestructura, recurso humano y todo lo que implique llevar a cabo el proceso con excelencia.

GAO (Outsourcing de servicios generales administrativos)

Gracias al talento que se cuenta en la compañía y las aplicaciones propias de STT, se logran brindar servicios contables y auditoría fiscal a sus clientes.

Normativa asociada

Grupo STT tiene clara la importancia de mantener segura la información de la organización, por esa razón, ha desarrollado la “Política para uso tecnológico (Seguridad de la información)”.

El objetivo del documento es establecer las políticas de la seguridad de la información de tecnologías, que deben de conocer y cumplir todos los colaboradores de la organización. Entre estas políticas se incluyen:

- Políticas para el uso adecuado de las tecnologías de información.
- Propiedad de información.
- Políticas de contraseñas.
- Políticas de Internet y correo electrónico.
- Seguridad y Almacenamiento
- Políticas para el uso de software.
- Políticas para compra y uso de equipo de cómputo.
- Política de respaldo de la información por parte de Proveedores de Sistemas Informáticos.

Estas políticas o reglas buscan proteger la información, al personal, a la empresa y buscan propiciar un aumento de la seguridad y aprovechamiento de la tecnología, la cual contribuye a aumentar la eficiencia en el trabajo y garantiza la continuidad de las operaciones en la institución por medio de la tecnología.

La Política para uso tecnológico puede ser localizada en la organización como “SIF-PO-02 Política uso tecnológico (Seguridad de la información)”, en su versión 01, la cual rige a partir del 09 de agosto de 2016.

Esta política se complementará con este trabajo de investigación al buscar una alineación con COBIT 5 basado específicamente en el proceso DSS05

Gestionar los servicios de seguridad, el cual se centra en administrar los servicios de Seguridad. (ISACA, 2012b)

COBIT 5 es un marco que presenta un enfoque integral y orientado al negocio para el gobierno y la gestión de TI. Este marco fue publicado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés), en el año 2012 y se considera una guía para los profesionales de tecnologías de información, además, se encuentra alineado con la norma ISO 27001[1] que contiene las mejores prácticas relativas a la seguridad de la información.

Por otro lado, cabe mencionar que en STT es importante la seguridad, privacidad y confidencialidad de la información personal de clientes y colaboradores, por tal razón cuentan con una política que está alineada con la Ley 8968 denominada Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Asamblea Legislativa, 2011), con el fin de garantizar a cualquier persona el adecuado tratamiento de sus datos personales.

Estudio preliminar

Como ya se indicó anteriormente, Grupo STT se ha comprometido a asegurar sus sistemas de información por medio de políticas:

- RRH-PO-01 Políticas Internas.
- STT RRH-PO-06 Políticas de privacidad y tratamiento de datos personal STT Regional.
- SIF-PO-02 Política para uso tecnológico (seguridad de la información).

No obstante, algunos de sus colaboradores indican que no conocen bien sobre qué tratan estas políticas.

[1] ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Fue publicada el 15 de octubre de 2005 y revisada el 25 de septiembre de 2013. Es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información.

Pese a los esfuerzos de la compañía, hay aspectos por mejorar dentro de sus políticas internas y controles, ya que en su mayor parte se refieren a reglas de conducta (uso apropiado), descuidando así otras áreas de interés y la manera cómo se administran los servicios de seguridad relacionados con TI.

Para la compañía, su fuente principal de negocio se centra en el servicio de administración de nóminas, por lo que consideran importante realizar una auditoría de TI relacionada con este proceso, ya que nunca se ha realizado una auditoría de seguridad del sistema de información, lo que hace pensar al nivel directivo de la compañía, si están en un nivel de riesgo aceptable o deben mejorar sus controles establecidos.

CAPÍTULO 3 - Desarrollo del tema de investigación

Actividades del proyecto

Tal como se planteó en la metodología, la investigación abarca tres grandes etapas: Planificación, Ejecución e Informe de Auditoría; las cuales son descritas a continuación:

Etapa 1 - Planificación

La etapa de planificación inicia con un estudio preliminar que tiene como objetivo un mejor entendimiento de la naturaleza de la empresa, así como conocer las necesidades y el ambiente de control donde se desarrolla la auditoría.

Producto de la anterior investigación, se determina la oportunidad y posibilidad real de llevar a cabo el trabajo con el alcance y en el tiempo establecido, así como los recursos requeridos.

Una vez determinada la viabilidad de cumplir con los objetivos del proyecto y de la empresa, se prepara el programa de ejecución del trabajo, para que una vez aprobado se comiencen a determinar las áreas de riesgo, diseñar las herramientas para poder atender de extremo a extremo todo el programa de ejecución, diseñar el mapa de riesgos, diseñar las pruebas, los cuestionarios, las guías de entrevista y todas las plantillas de trabajo para evidenciar su ejecución.

Programa de auditoría del proyecto.

Según se establece en Grupo STT, se debe elaborar el programa para la actividad de planificación, en el que se definan los procedimientos de auditoría que se requieren aplicar para cumplir con los objetivos correspondientes a esta actividad; así como el objetivo, naturaleza, alcance, oportunidad, plazo y sus responsables. (STT, 2015)

Dicho lo anterior, se describe a continuación el programa para ejecutar la auditoría de seguridad de la información:

Proceso a Auditar	Administración de nóminas		
Responsable:	Roy Hernaldo Chavarría Barquero		
Aprobado por			
	M.Sc. Marco V. Gámez Acuña	**Firma**	**Fecha**
	M.Sc. Gino Ramírez Solís	**Firma**	**Fecha**
Plazo de ejecución	De enero a abril de 2018		

I. Objetivos de la auditoría

Determinar la suficiencia de las actividades de control ejecutadas para preservar la confidencialidad, integridad y disponibilidad de la información.

II. Naturaleza

La presente auditoría se realiza dada la necesidad de Grupo STT de verificar y reforzar sus medidas para asegurar la seguridad de la información en la compañía.

III. Alcance

El proyecto se desarrolla en el periodo que abarca de diciembre 2017 a abril de 2018, para el análisis de actividades e información se contempla lo generado o actuado por el proceso de “Administración de nóminas” en el período de enero 2017 a diciembre 2017.

IV. Procedimientos de trabajo

Procedimientos a ejecutar			
ID	Detalle	Ref. PT	Tiempo estimado
A	Determinar el alcance de la iniciativa de aseguramiento		
A.1	Determinar las partes interesadas en relación con la seguridad de la información y el rol de cada una de éstas.	PT-AUD-01	8 enero – 10 enero de 2018
A.2	Determinar los objetivos de aseguramiento para la seguridad de la información basados en la evaluación del entorno (contexto interno y externo) y del riesgo relevante y las oportunidades relacionadas.	PT-AUD-02	11 enero – 15 enero de 2018
A.3	Determinar los habilitadores y la(s) instancia(s) de los habilitadores en el alcance de la seguridad de la información.	PT-AUD-03	16 enero -19 enero 2018
B	Entender los habilitadores, establecer criterios de evaluación y realizar la evaluación		
B.1	Acordar con las partes interesadas según su rol las métricas y los criterios para los objetivos empresariales y los objetivos relacionados con TI.	PT-AUD-04	22 enero – 24 enero de 2018
B.2	Obtener la comprensión del proceso de seguridad de la información, establecer los criterios de evaluación adecuados y evaluarlos.	PT-AUD-05	25 enero – 29 enero de 2018
B.3	Conseguir una comprensión de los principios, políticas y marcos de referencia para la seguridad de la información y evaluarlos a la luz de los criterios establecidos previamente.	PT-AUD-06	30 enero – 2 febrero de 2018
B.4	Obtener la comprensión de la estructura de la organización y evaluarla a la luz de los criterios establecidos previamente.	PT-AUD-07	5 febrero – 8 febrero de 2018
B.5	Comprender la cultura, ética y comportamiento relacionado con la seguridad de la información y evaluarlos a la luz de los criterios establecidos previamente.	PT-AUD-08	9 febrero – 12 febrero de 2018
B.6	Obtener una comprensión de los elementos de información incluidos en el alcance y	PT-AUD-09	13 febrero – 16 febrero de 2018

	evaluarlos a la luz de los criterios establecidos previamente.		
B.7	Obtener una comprensión de los servicios, infraestructura y aplicaciones relacionados con el proceso de administración de nóminas y evaluarlos a la luz de los criterios establecidos previamente.	PT-AUD-10	19 febrero – 22 febrero de 2018
C	Comunicar los resultados		
C.1	Documentar las excepciones y brechas.	Análisis de resultados	27 febrero – 28 febrero de 2018
C.2	Comunicar el trabajo realizado y los hallazgos.	Comunicación de los resultados	02 abril de 2018

Etapa 2 – Examen o ejecución

La etapa de ejecución del proceso se realizó una vez aprobado el programa de auditoría del proyecto indicado en la sección anterior, en el cual se describen las tareas a desarrollar y los tiempos de inicio y finalización de la ejecución de cada una de ellas.

Esta ejecución se realizó agrupando en tres grandes fases las diferentes actividades a realizar, a saber:

Determinar el alcance de la iniciativa de aseguramiento.

Para realizar la determinación del alcance de la iniciativa de aseguramiento, se dividió el proceso en sub-fases, en las cuales se realizaron tareas específicas que se muestran a continuación:

- Determinar las partes interesadas en relación con la seguridad de la información y el rol de cada una de éstas

La determinación de las partes interesadas se realizó por medio de un entendimiento de la estructura organizacional de la empresa, para ello, se solicitó el organigrama vigente y por medio de una entrevista con el Gerente de Tecnologías de Información, se documentó el rol y descripción de las funciones de

cada una de las partes interesadas en la seguridad de la información del proceso nóminas, en el formulario “Determinación de las partes interesadas”.

- Determinar los objetivos de aseguramiento para la seguridad de la información

Mediante la recopilación y análisis de la información de la estructura organizacional de la compañía, se logró la determinación de los objetivos de aseguramiento de la seguridad de la información del proceso de nóminas, los cuales se documentaron en la Matriz RACI señalada en el punto 4.3 de este documento y utilizando de base las prácticas claves señaladas por COBIT 5 “DSS05 - Gestionar los Servicios de Seguridad”.

- Determinar los habilitadores para el alcance de la seguridad de la información

El desarrollo de esta tarea se basó en lo que indica COBIT 5 “DSS05 - Gestionar los Servicios de Seguridad”, en donde se establecen los puntos más relevantes a considerar al momento de determinar los habilitadores para el alcance de la seguridad de la información.

Según lo define y estable COBIT 5, los habilitadores son los factores que influyen en el cumplimiento de las metas específicas; para efectos de este trabajo sería la seguridad de la información. COBIT 5 en su proceso “DSS05 - Gestionar los Servicios de Seguridad” describe cinco habilitadores claves para la seguridad en los servicios de TI, éstos son:

- **Principios, políticas y marcos de referencia**: Se refiere a las políticas y principios establecidos en la organización para asegurar que la información sea utilizada solo por personal autorizado, además, de los marcos de referencia que se utilizan para el establecimiento de ésta.
- **Estructura organizacional**: Define cuál es la estructura de la organización que está comprometida con el aseguramiento de la seguridad de la información.

- **Cultura, ética y comportamiento:** Establece los lineamientos a seguir dentro de la organización para asegurar que la información sea utilizada de manera correcta.
- **Servicios, infraestructura y aplicaciones**: Se refiere a los servicios y aplicaciones que soportan la seguridad de la información del proceso a auditar, así como la infraestructura que soporta estos servicios.
- **Personas, habilidades y competencias**: Está relacionado con las personas que son necesarias para cumplir las metas establecidas por la organización.

Para el desarrollo de este punto, se utilizaron los formularios definidos en el punto 4.4 de este documento “Habilitadores del alcance de la seguridad de la información”.

Entender los habilitadores, establecer criterios de evaluación y realizar la evaluación.

Para la adecuada realización de este proceso, se elaboraron diferentes formularios, con los cuales se obtuvo una mejor comprensión de las actividades definidas en cada habilitador evaluado.

Esos formularios se encuentran en la sección 4 de este documento, específicamente del punto 4.5 al 4.10, en los que se incluyen listas de verificación aplicadas en la realización de este trabajo. Si bien, este trabajo es basado en COBIT 5, las preguntas de verificación de los cuestionarios se reforzaron utilizando los principios señalados en la norma ISO 27001 “Gestión de la Seguridad de la Información”.

Una vez analizadas las respuestas de los formularios, se inicia con la documentación de los resultados.

Etapa 3 – Comunicación de los resultados

Por un requerimiento de confidencialidad acordado con la empresa, previo al inicio de este trabajo de investigación, y de acuerdo con lo establecido en los términos para su realización desde el inicio del curso Práctica Profesional I, no resulta factible incluir en este apartado los resultados logrados o hallazgos determinados; los cuales fueron ampliamente detallados en el informe N.° 01-2018 entregado a las autoridades de Grupo STT, según consta en la siguiente nota y fueron expuestos a esas instancias según consta en la siguiente acta N.° ACT-AUD-01.

Lo anterior no obsta para mencionar que se determinaron una serie de condiciones relevantes que la empresa auditada dio por aceptadas y se comprometió a iniciar a la mayor brevedad las tareas necesarias para fortalecer las estructuras de control que garanticen la seguridad de la información del proceso de nómina; las cuales se mencionan en términos generales en el capítulo 5.

23 de marzo de 2018

Pablo Betrano Machado, Coordinador de TI
Grupo STT
Presente

Estimado señor:

Producto del acuerdo previo entre la empresa Grupo STT y el Sr. Roy Chavarría Barquero, relativo al Trabajo Final de Graduación de la Maestría Profesional en Auditoría de Tecnologías de Información, se hace la entrega del informe final de auditoría N.**°01-2018,** el cual, es resultado de la práctica profesional desarrollada como parte del programa de la maestría.

El trabajo final de graduación, consistió en la realización de una auditoria de la seguridad de información en una empresa privada costarricense. Dentro de los objetivos principales se encontraban los siguientes:

- Determinar los principales riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información.

- Evaluar lo adecuado del proceso interno actual para administrar la seguridad de la información de la empresa y datos del Sistema de Administración de Nóminas.

- Aplicar las técnicas y normativas asociadas al tema tratado, que permitan determinar la suficiencia de la seguridad de la información y emitir recomendaciones de los aspectos encontrados sujetos a mejora.

Se agradece su atención y la colaboración brindada en todo el proceso realizado.

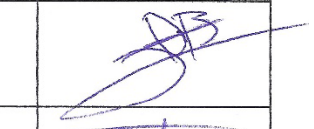
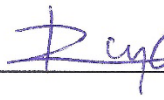
Roy Chavarría Barquero
Sustentante

Pablo Betrano Machado
Coordinador de TI, Grupo STT.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS **TRABAJO FINAL DE GRADUACIÓN**	**ACT-AUD-01**
	Versión: 01

ACTA DE CONFERENCIA DEL INFORME DE AUDITORIA

El día **23 de marzo de 2018,** en las oficinas de Grupo STT de Costa Rica, Tibás, se realizó la conferencia del "Informe de auditoría sobre la seguridad de la información", correspondiente a la actividad realizada del Trabajo Final de Graduación de la Maestría Profesional en Auditoría de Tecnologías de Información, los abajo firmantes manifiestan haber participado en dicha conferencia estando en acuerdo con los temas tratados

PARTICIPANTE	PUESTO	FIRMA
Fabricio Díaz Bolaños	Soporte Técnico	
Pablo Betrano Machado	Coordinador IT	
Roy Chavarría Barquero	Auditor.	

Etapa 4 – Evidencia de la auditoría

Para la toma de la evidencia se utilizaron diferentes técnicas de auditoría entre ellas se encuentran:

- **Plantillas de trabajo**: Se realizaron diferentes formularios con el fin de recopilar información y evaluar condiciones específicas. Las plantillas utilizadas se pueden encontrar en el capítulo IV de este documento.
- **Análisis de contenido**: Se efectuó un análisis de la documentación propia de la compañía, como lo son las políticas y procedimientos relacionados con la seguridad de la información del proceso de nóminas.
- **La observación**: Del personal involucrado en el proceso de administración de nóminas y el personal encargado de la gestión de TI en la compañía.
- **Entrevistas**: Aplicadas al coordinador de TI y a usuarios involucrados en el proceso de nóminas.

La evidencia de auditoría no consta en este trabajo por aspectos de confidencialidad mencionados en el apartado anterior. Tal evidencia forma parte del expediente entregado a Grupo STT como parte de los resultados de la auditoría.

Etapa 5 – Documentación de la auditoría

Al ser una auditoría de seguridad de la información, la compañía solicitó mantener la confidencialidad de la información resultante de este trabajo, ya que se trata de información sensible para la organización. Por esta razón, no se adjunta a este documento lo relativo al proceso aplicado, el cual se realizó con las plantillas indicadas en el capítulo IV de este documento.

Etapa 6 – Calidad en la auditoría

El desarrollo de este proceso de auditoría se elaboró bajo los siguientes principios de calidad:

- **Ética**: Los principios de ética establecidos por el Instituto de Auditores Internos de Costa Rica fueron la base para el desarrollo de este trabajo.

- **Supervisión**: La participación del tutor del proyecto fue un aporte muy valioso para la elaboración de este trabajo, quién supervisó en todo momento las etapas de la auditoría.
- **Mejores prácticas**: Este trabajo fue elaborado con las mejores prácticas existentes relativas a la seguridad de la información, entre las cuales se encuentra COBIT 5 elaborado por ISACA, el cual sirvió de guía en este proyecto.

CAPÍTULO 4 - Plantillas de hojas o papeles de trabajo

El desarrollo de este proyecto permitió desarrollar un conjunto de herramientas o insumos necesarios que pueden ser utilizados por la compañía en la elaboración de futuras auditorías de seguridad de la información. Por esa razón se detallan seguidamente los documentos utilizados en el proceso ejecutado.

Determinación de las partes interesadas

La siguiente plantilla fue utilizada para identificar los roles o actores interesados en la seguridad de la información del proceso auditado, en éste se indicó cuál es el rol existente y una descripción de sus funciones.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

Referencia

Versión: 01

Partes interesadas	
Rol/Estructura	**Descripción**
Corporativo	
Director General Ejecutivo (CEO)	
Director General Financiero (CFO)	
Coordinador de TI	
Ejecutivos de cuenta	
Coordinador CSC	
Coordinadores de Talento Humano	
Clientes	
Auditoría	

Matriz RACI

El objetivo de este papel de trabajo es determinar las responsabilidades de los diferentes actores que intervienen en las prácticas claves del proceso de seguridad de la información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

Referencia

Versión: 01

Matriz RACI

Prácticas claves del proceso	Corporativo	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Coordinador de TI	Ejecutivos de Cuenta	Coordinador CSC	Coordinadores de Talento Humano	Auditoría
Proteger contra software malicioso	I	I	C	A	I	R	R	C
Gestionar la seguridad de la red y conexiones	I	A	C	R		I		C
Gestionar la seguridad de los puestos de usuario final	I	A		R		I	I	C
Gestionar la identidad del usuario y acceso lógico	I			A		R	I	C
Gestionar el acceso físico a los activos de TI	I	A		R		I		C
Gestionar documentos sensibles y dispositivos de salida	I	A		R	I	C	C	C
Supervisar la infraestructura para detectar eventos relacionados con la seguridad	I	A		R		C	I	C

Significado de los tipos de responsabilidad:

R (Responsable de ejecutar): Es el responsable de realizar la tarea.

A (Responsable de rendir cuentas): En inglés se identifica como "*Accountable*". Es el responsable de asegurar que la tarea se realice y el que debe rendir cuentas sobre su ejecución. Solo puede existir un rendidor de cuentas por tarea.

C (Consultado): Es quién posee alguna información necesaria para poder realizar la tarea con éxito.

I (Informado): Es el que debe ser informado sobre el avance y resultados de la ejecución de la tarea.

Habilitadores del alcance de la seguridad de la información

Los habilitadores son utilizados para obtener una comprensión más clara del alcance de la auditoría. Basados en las mejores prácticas de COBIT 5, se cuentan con cinco habilitadores[2], a continuación, se muestran las plantillas utilizadas en la ejecución de cada uno de ellos:

Habilitador 1: Principios, políticas y marcos

El objetivo de este habilitador es obtener entendimiento y documentar los principios, políticas y marcos de referencia utilizados en la organización para la seguridad de la información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

Referencia

Versión: 01

1. Principios, Políticas y Marcos			
No.	**Nombre del principio, política o marco**	**Versión**	**Ubicación**
1			
2			
3			
Etc.			

Habilitador 2: Estructura organizacional

El objetivo de este papel de trabajo es comprender y documentar los roles y funciones de los actores involucrados en el proceso de seguridad de la información.

[2] COBIT 5 cuenta con un total de siete habilitadores, pero para el proceso DSS05 “Gestionar los servicios de seguridad” solo aplican cinco de ellos.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

2. Estructura organizacional		
No.	**Rol/Estructura**	**Descripción de funciones**
1		
2		
3		
Etc.		

Habilitador 3: Cultura, ética y comportamiento

Este habilitador tiene como objetivo entender la cultura, la ética y el comportamiento de los colaboradores dentro de la organización, para ello se utilizó la siguiente plantilla para documentar las diferentes políticas y procedimientos establecidos que competen a los temas relacionados con este habilitador:

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

3. Cultura, Ética y Comportamiento		
No.	**Nombre de la política o procedimiento**	**Referencia**
1		
2		
3		
5		
Etc.		

Habilitador 4: Servicios, infraestructura y aplicaciones

Esta plantilla fue utilizada para documentar los diferentes servicios brindados por el área de TI, la infraestructura de la organización y las diferentes aplicaciones que se utilizan para brindar una adecuada seguridad de la información del proceso auditado.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

4. Servicios, Infraestructura y Aplicaciones		
Servicios		**Versión**
1		
2		
Etc.		
Infraestructura		
1		
2		
Etc.		
Aplicaciones		
1		
2		
Etc.		

Habilitador 5: Personas, habilidades y competencias

La siguiente plantilla tiene como finalidad documentar las diferentes habilidades y competencias de las personas involucradas con la administración de la seguridad de la información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

5. Personas, habilidades y competencias: Administración de la seguridad	
Rol	**Habilidades y competencias**
Anotar el nombre del rol a describir	Describir las habilidades y competencias del rol indicado

Métricas

La siguiente plantilla es utilizada para documentar las diferentes métricas que deben cumplirse para garantizar una razonable disponibilidad, confiabilidad e integridad de la información.

Métricas		
Objetivo	**Métrica**	**Meta de cumplimiento (mínimo)**
Protección de activos	- Proporción de incidentes significativos frente a los incidentes totales	
Cumplimiento con leyes y regulaciones externas	- Costo del incumplimiento regulatorio - Incumplimientos a acuerdos contractuales con clientes	
Continuidad y disponibilidad del servicio	- Tiempo de interrupciones del servicio contra el tiempo en funcionamiento - Porcentaje de quejas en función de disponibilidad del servicio	
Cumplimiento de políticas internas	- Porcentaje de partes interesadas que entienden las políticas - Porcentaje de políticas respaldadas por normas o mejores prácticas de trabajo	
Cumplimiento y apoyo de TI al negocio para que cumpla de leyes y regulaciones externas	- Número de incumplimientos de TI informados al corporativo o que afectan la reputación pública - Evaluación a proveedores de servicios de TI	
Gestión del riesgo relacionado con TI	- Números de incidentes significativos relacionados con TI no identificados en la evaluación de riesgos	
Seguridad de la información, procesamiento de infraestructura y aplicaciones	- Tiempo para otorgar, cambiar y eliminar privilegios de acceso, en comparación con los niveles de servicio acordados - Frecuencia de evaluación de la seguridad contra las últimas normas y directrices	

Comprensión y evaluación del proceso de seguridad de la información

Para realizar la compresión y evaluación del proceso de seguridad, se aplicaron diferentes plantillas las cuales se muestran a continuación:

Practicas claves del proceso

Con esta plantilla se identificaron las prácticas claves de la seguridad de la información, para cada una de estas prácticas, se elaboró una lista de chequeo para facilitar su evaluación.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

Practicas claves del proceso			
No.	**Práctica**	**Propósito**	**Referencia**
1	Proteger contra software malicioso	Mantener medidas preventivas y correctivas para proteger los sistemas de información y tecnología de cualquier software malicioso como virus, gusanos, spam, entre otros.	Proteger contra software malicioso
2	Gestionar la seguridad de la red y conexiones	Utilizar medidas de seguridad y procedimientos de gestión de la seguridad, para proteger la información desde cualquier modo de conexión.	Gestionar la seguridad de la red y conexiones
3	Gestionar la seguridad de los puestos de usuario final	Asegurar que los puestos de usuario final son seguros para procesar, almacenar o transmitir información.	Gestionar la seguridad de los puestos de usuario final
4	Gestionar la identidad del usuario y acceso lógico	Asegurar que los usuarios tengan derechos de accesos a la información de acuerdo con su perfil de trabajo.	Gestionar la identidad del usuario y acceso lógico
5	Gestionar el acceso físico a los activos de TI	Establecer procedimientos para conceder, limitar o revocar accesos a las diferentes áreas físicas de las instalaciones, de acuerdo con las necesidades del negocio.	Gestionar el acceso físico a los activos de TI
6	Gestionar documentos sensibles y dispositivos de salida	Establecer prácticas de gestión de documentos e inventario de activos de TI, para salvaguardar la documentación sensible, activos especiales o credenciales de seguridad (token), entre otros.	Gestionar documentos sensibles y dispositivos de salida

7	Supervisar la infraestructura para detectar eventos relacionados con la seguridad	Supervisar la infraestructura para detectar accesos no autorizados y asegurar la adecuada gestión de incidentes.	Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Proteger contra software malicioso

Esta plantilla tiene como objetivo verificar los diferentes controles de seguridad de la información relativos a la protección contra software malicioso.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**CHK-AUD-SIF-01**
	Versión: 01

Lista de chequeo para evaluación de controles contra software malicioso					
Objetivo: Evaluar los controles de seguridad de la información relativos a la protección contra software malicioso					
Auditor:		**Proceso:** COBIT 5, DSS05 Gestionar Servicios de Seguridad **Práctica:** DSS05.01 Proteger contra software malicioso			
No.	**Verificación**	**Cumplimiento**			**Comentarios u observaciones**
		Sí	**No**	**Parcial**	
1	¿Existe una política de prevención contra software malicioso?				
2	¿Existe un programa de concienciación a los colaboradores sobre las implicaciones de un software malicioso y cómo proceder frente a éstos?				
3	¿Se envían boletines informativos y/o notificaciones en a la organización con alertas de software malicioso?				
4	¿Se encuentran definidas las responsabilidades de los colaboradores sobre la prevención frente al software malicioso?				
5	¿Se encuentran los equipos de cómputo con software instalado y activado para la protección de software malicioso?				

6	¿Se actualizan las definiciones de software malicioso periódicamente?				
7	¿Se realiza la actualización de las definiciones contra software malicioso de forma automática?				
8	¿Se distribuyen las actualizaciones de las definiciones contra software malicioso de forma centralizada?				
9	¿Se distribuye la instalación del programa contra software malicioso de forma centralizada?				
10	¿Se administra de forma centralizada el programa de prevención contra software malicioso?				
11	¿Se realizan evaluaciones periódicas de la información sobre nuevas amenazas?				
12	¿Se realiza un filtrado del tráfico entrante para protegerse de información no solicitada?				
13	¿Existen capacitaciones periódicas al personal sobre el software malicioso?				
14	¿Existen capacitaciones sobre el uso adecuado del correo electrónico, internet e instalación de software no autorizado?				
15	¿Existe un listado oficial documentado del software autorizado por la organización?				
16	¿Se verifica periódicamente el software instalado en los equipos?				
17	¿Se verifica periódicamente los datos guardados en los equipos de los usuarios?				
18	¿Se verifica la presencia de virus en archivos descargados de internet?				
19	¿Se cuenta con filtrado de virus y spam en el correo electrónico?				

Gestionar la seguridad de la red y conexiones

La siguiente lista de verificación fue aplicada con el fin de evaluar los controles de seguridad de la información relativos a la protección de la red y las conexiones, tanto internas como externas, realizadas en la organización.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	**CHK-AUD-SIF-02**
	Versión: 01

Lista de chequeo para evaluación de controles de seguridad de la red y conexiones

Objetivo: Evaluar los controles de seguridad de la información relativos a la protección de la seguridad de la red y conexiones a la red.

Auditor:	**Proceso:** COBIT 5, DSS05 Gestionar Servicios de Seguridad **Práctica:** DSS05.02 Gestionar la seguridad de la red y conexiones

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Existe una política de seguridad de la conectividad, basada en los requerimientos del negocio y análisis de riesgos?				
2	¿Está restringido el acceso a la red de la organización sólo a dispositivos autorizados?				
3	¿Se encuentra la información restringida por dispositivos o usuarios?				
4	¿Se encuentra la red inalámbrica segmentada para acceso de invitados y acceso interno?				
5	¿Se encuentra la red de la organización segmentada por áreas de negocio?				
6	¿Se cuenta con cortafuegos (firewall) y/o software para detección de intrusiones?				
7	¿Existe un reglamento o política para controlar el tráfico de la red entrante o saliente?				
8	¿Se tienen establecidos y se aplican los protocolos de seguridad para las conexiones de red?				

9	¿Se restringe la configuración de la tarjeta de red en los equipos de los usuarios?				
10	¿Existe un monitoreo de la red para detectar cualquier anomalía en el tráfico de red?				
11	¿Se tiene definido un procedimiento y las responsabilidades para la gestión de accesos remotos a servidores y/o dispositivos de red (firewall, swich, routers, etc.)?				
12	¿Se cuenta con un esquema de red documentado donde se muestren los enlaces de datos, internet y red local?				
13	¿Se realizan pruebas periódicas de penetración para determinar la adecuada protección de la red?				
14	¿Se realizan evaluaciones periódicas de seguridad al software de nóminas para determinar la protección de la información?				

Gestionar la seguridad de los puestos de usuario final

La plantilla siguiente se aplicó para determinar que los controles de seguridad de la información relativos a los puestos de usuario final, sean suficientes para garantizar la confidencialidad, integridad y disponibilidad de la información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

CHK-AUD-SIF-03

Versión: 01

Lista de chequeo para evaluación de la seguridad de los puestos del usuario final

Objetivo: Evaluar los controles de seguridad de la información relativos a la gestión de la seguridad de los puestos de usuario final.

Auditor:

Proceso: COBIT 5, DSS05 Gestionar Servicios de Seguridad

Práctica: DSS05.03 Gestionar la seguridad de los puestos de usuario final

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Existe una política de seguridad para el uso de los dispositivos de usuario final?				
2	¿Se restringen las opciones de configuración del sistema operativo para solo ser accedidas por el administrador?				
3	¿Se cuenta con bloqueos de usuario por intentos fallidos de contraseña?				
4	¿Se bloquean automáticamente los dispositivos al no ser utilizados por el usuario en un tiempo determinado?				
5	¿Se encuentra cifrada la información almacenada de acuerdo con su criticidad?				
6	¿Se restringe el acceso a la información almacenada por roles o usuarios?				
7	¿Se restringe el acceso a la información almacenada por IP?				
8	¿Se administra el acceso y el control remoto de las estaciones de los usuarios finales?				
9	¿Se cuenta con una plataforma de administración de los dispositivos móviles que permita el bloqueo, ubicación y/o formateo del éstos?				
10	¿Existe una clave o pin establecida para ingresar en los dispositivos móviles?				

11	¿Se cuenta con un procedimiento para la eliminación de información almacenada en dispositivos de usuario?				
12	¿Existe un procedimiento para el desecho de dispositivos de usuario de forma segura que garantice que la información haya sido eliminada completamente?				
13	¿Se registra la eliminación de los medios de almacenamiento como prueba de auditoría?				
14	¿Existe un procedimiento para la gestión de dispositivos de almacenamiento externo?				
15	¿Se encuentran definidos los permisos para la conexión de dispositivos de almacenamiento externo?				
16	¿Se registran en una bitácora las conexiones de dispositivos externos de almacenamiento?				

Gestionar la identidad del usuario y acceso lógico

Esta lista de verificación se aplicó para evaluar los controles de seguridad de la información relativos con la gestión de la identidad del usuario y el acceso lógico de éstos.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

CHK-AUD-SIF-04

Versión: 01

Lista de chequeo para evaluación de controles de identidad y acceso lógico

Objetivo: Evaluar los controles de seguridad de la información relativos a la gestión de la identidad del usuario y acceso lógico a los sistemas.

Auditor:

Proceso: COBIT 5, DSS05 Gestionar Servicios de Seguridad

Práctica: DSS05.04 Gestionar la identidad del usuario y acceso lógico

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Se establecen los permisos de acceso de los usuarios al sistema de acuerdo con sus funciones?				
2	¿Se alinean los permisos de acceso a los roles y responsabilidades, basándose en el principio de menor privilegio?				
3	¿Se cuenta con autenticación de acceso a los activos de información?				
4	¿Existe un documento con el procedimiento de solicitud y aprobación de cambios en los derechos de acceso?				
5	¿Se administra todos los cambios de permisos de acceso (creación, modificación y/o eliminación) mediante una solicitud formal?				
6	¿Se encuentran definidos los usuarios que pueden solicitar la modificación de permisos de acceso?				
7	¿Existen niveles de aprobación para las solicitudes de cambios en los permisos de acceso?				
8	¿Se registran todos los cambios en los permisos en los usuarios para revisiones posteriores?				
9	¿Se realizan revisiones periódicas de las cuentas de usuario y los accesos relacionados?				
10	¿Se mantiene un registro de auditoría de acceso a la información clasificada como altamente sensible?				

11	¿Se identifican en el sistema las actividades de procesamiento de información realizadas por los usuarios?				
12	¿Existen usuarios genéricos o compartidos por más de una persona?				
13	¿Se tiene definido quién administra y controla los accesos a usuarios y roles?				
14	¿Se cuenta con bloqueo temporal de los accesos de usuario cuando este se encuentra de vacaciones, incapacidades y/o permisos temporales?				
15	¿Se asignan accesos temporales a usuarios externos o personal en pasantía, limitados solo para las actividades que realizan?				
16	¿Se cuenta con un registro donde se identifiquen los usuarios con los respectivos privilegios asignados a las diferentes aplicaciones en la organización?				

Gestionar el acceso físico a los activos de TI

La siguiente plantilla se aplicó para determinar la suficiencia de los controles establecidos en la organización con respecto al acceso físico a los activos de tecnología de la información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

CHK-AUD-SIF-05

Versión: 01

Lista de chequeo para evaluación de controles de acceso físico a los activos

Objetivo: Evaluar los controles de seguridad de la información relativos a la gestión del acceso físico a los activos de TI en la organización.

Auditor:	**Proceso:** COBIT 5, DSS05 Gestionar Servicios de Seguridad **Práctica:** DSS05.05 Gestionar el acceso físico a los activos de TI

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Se controla el ingreso adecuado a los cuartos de redes y servidores?				
2	¿Se realizan peticiones formales de acceso a las áreas de redes y servidores?				
3	¿Se encuentra establecido un responsable para autorizar las peticiones de acceso a las áreas de TI?				
4	¿Se registran y supervisan los accesos a las áreas de TI?				
5	¿Se registra la hora de ingreso, hora de salida y función a realizar por la persona que ingresa a TI?				
6	¿Se registran los visitantes, proveedores y/o contratistas con fecha y hora de entrada y salida del área de TI?				
7	¿Se mantiene en todo momento una identificación visible por parte del personal?				
8	¿Se instruye al personal para que los visitantes sean acompañados en todo momento mientras están en el sitio?				
9	¿Se realizan capacitaciones de concienciación al personal sobre la seguridad física?				
10	¿Se conoce el procedimiento a seguir por parte del personal, en caso de ver una persona no acompañada y desconocida que no lleva identificación?				

11	¿Se restringe el acceso a las diferentes ubicaciones en la organización mediante restricciones perimetrales tales como dispositivos de seguridad para acceso en puertas interiores y exteriores?				
12	¿Se cuenta con grabación de circuito cerrado en las áreas de TI y de negocio?				
13	¿Se cuenta con alarmas o notificaciones en caso de acceso no autorizado en las diferentes ubicaciones en la organización?				
14	¿Se instruye al personal para no prestar o ceder su acceso a otros usuarios y visitantes?				
15	¿Se cuenta con roles o niveles de acceso de acuerdo con las necesidades del negocio?				
16	¿Existe un procedimiento para eliminar el acceso físico a los usuarios?				

Gestionar documentos sensibles y dispositivos de salida

El fin de la aplicación de esta plantilla es la evaluación de los diferentes controles de seguridad a los documentos sensibles y dispositivos de salida sensibles, como por ejemplo tarjetas de acceso a bancos, llaves o "*token"* de seguridad para accesos a sistemas, dispositivos de almacenamiento externo con información sensible, entre otros.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

CHK-AUD-SIF-06

Versión: 01

Lista de chequeo para evaluación de controles de documentos y dispositivos sensibles

Objetivo: Evaluar los controles de seguridad de la información relativos a la gestión de documentos sensibles y dispositivos de salida.

Auditor:	**Proceso:** COBIT 5, DSS05 Gestionar Servicios de Seguridad **Práctica:** DSS05.06 Gestionar documentos sensibles y dispositivos de salida

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Existe un procedimiento para controlar la recepción, uso y/o destrucción de formularios especiales y/o dispositivos de salida hacia dentro y fuera de la organización?				
2	¿Se cuenta con un inventario de documentos sensibles?				
3	¿Se asignan privilegios de acceso a los documentos sensibles basados en el principio del menor privilegio?				
4	¿Se restringe el acceso a los documentos sensibles desde fuera de la organización?				
5	¿Existe un registro de los accesos que han tenido los documentos sensibles?				
6	¿Se designa un responsable de los documentos sensibles?				
7	¿Existe un inventario de activos de TI documentado?				
8	¿Se mantiene un registro de los dispositivos asignados a cada usuario?				
9	¿Se identifica cuáles son los dispositivos sensibles o especiales?				
10	¿Se establecen las responsabilidades para el uso de los dispositivos asignados a los usuarios?				
11	¿Se controla la salida de dispositivos sensibles o especiales fuera de la organización?				

12	¿Existen salvaguardas físicas apropiadas para el acceso a documentos físicos sensibles y/o dispositivos sensibles?				
13	¿Existen trituradoras de papel para la destrucción de documentos físicos sensibles o confidenciales?				
14	¿Existe un procedimiento para la destrucción de dispositivos sensibles o especiales?				
15	¿Se establece el adecuado borrado de la información de los dispositivos sensibles antes de reciclarlos o destruirlos?				
16	¿Se elimina la información sensible que contengan los dispositivos de TI antes de enviarlos a reparación?				

Supervisar la infraestructura para detectar eventos relacionados con la seguridad

La siguiente plantilla fue aplicada en la organización para determinar la suficiencia de los controles establecidos para detectar eventos que comprometan la seguridad de la infraestructura.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

CHK-AUD-SIF-07

Versión: 01

Lista de chequeo para evaluación de controles de supervisión la infraestructura

Objetivo: Evaluar los controles de seguridad de la información relativos a la supervisión de la infraestructura para detectar eventos relacionados con la seguridad en el proceso de administración de nóminas.

Auditor:	**Proceso:** COBIT 5, DSS05 Gestionar Servicios de Seguridad
	Práctica: DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Se utilizan herramientas para detectar posibles intrusiones en la infraestructura?				
2	¿Se guardan los registros de eventos relacionados con la seguridad de la información, reportados por las herramientas?				
3	¿Se revisan regularmente los registros de eventos para detectar posibles incidentes?				
4	¿Se comunica a los interesados la naturaleza y características de los posibles incidentes relacionados con la seguridad?				
5	¿Se establece y comunica a los interesados el impacto de los posibles incidentes para determinar una respuesta acorde?				
6	¿Se ingresan tiquetes de incidentes de seguridad en el momento que se detectan potenciales incidentes?				
7	¿Existe un proceso documentado para la recopilación de evidencia forense del posible incidente?				
8	¿Conoce el personal los requisitos para la recolección de la evidencia?				

Comprensión y evaluación de los principios, políticas y marcos

Se realizó una comprensión y evaluación de los principios políticas y marcos de referencia con que cuenta la compañía. Esta evaluación se efectuó esencialmente bajo las mejores prácticas indicadas por COBIT 5 para la seguridad de la información, en la sección II titulada “Uso de habilitadores de COBIT 5 para implementar la seguridad de la información en la práctica”, específicamente en su capítulo 2 llamado “Catalizador: Principios, Políticas y Marcos de Referencia”, el cual es especializado en los principios, políticas y marcos de referencia para la seguridad de la información.

Para esta evaluación se aplicaron dos plantillas las cuales se detallan a continuación:

Evaluación de los principios, políticas y marcos

Esta plantilla se utilizó para evaluar aspectos generales que deben contener los principios y políticas existentes, basados en las mejores prácticas de COBIT 5.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FINAL DE GRADUACIÓN

Referencia

Versión: 01

Evaluación de los Principios, Políticas y Marcos

Objetivo: Evaluar los principios, políticas y marcos existentes en la organización relativos a la seguridad de la información con base en las mejores prácticas.

Auditor:	**Criterio:** COBIT 5 para la seguridad de la información, Sección II "Uso de habilitadores de COBIT 5 para implementar la seguridad de la información en la práctica, Capítulo 2 "Catalizador: Principios, Políticas y Marcos de Referencia" COBIT 5, DSS05 Gestionar Servicios de Seguridad

Nombre de la política, principio o marco	Versión	Ubicación

No.	Verificación	Cumplimiento		Comentarios u observaciones
		Sí	No	
1	¿Se establece el alcance de la política y excepciones?			
2	¿Se cuenta con fecha en que rige la política?			
3	¿Existe una fecha de vencimiento o próxima revisión de la política?			
4	¿Existe la fecha de la última actualización o revisión del documento?			
5	¿Se encuentra el documento disponible para los interesados?			
6	¿Se puede navegar fácilmente por el documento?			
7	¿Existe una estructura lógica en el documento?			
8	¿Se establecen las consecuencias de su incumplimiento?			
9	¿Se indican las áreas a las que aplica la política?			
10	¿Se cumple con alguna regulación o requerimiento legal?			

Aspectos específicos por evaluar en las políticas

Una vez evaluadas las generalidades en las políticas, se aplicó esta plantilla, donde se consideraron los siguientes aspectos: controles de acceso, respuestas ante incidentes de seguridad, gestión de activos, reglas de conducta, gestión de proveedores y gestión de riesgos.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

Aspectos específicos por evaluar en las políticas relativos con la seguridad de la información				
No.	**Verificación**	**Cumplimiento**		**Comentarios u observaciones**
		Sí	**No**	
1	**Control de acceso**	**Propósito:** Proporcionar un adecuado acceso a las partes interesadas		
1.1	¿Se permite el acceso de emergencia a los sistemas y su revocación en el tiempo oportuno?			
1.2	¿Se establece una segregación de funciones?			
1.3	¿Se incluye el aprovisionamiento de acceso físico y lógico?			
2	**Respuestas a incidentes de seguridad**	**Propósito**: Recuperar de manera oportuna las actividades del negocio		
2.1	¿Existe la definición de incidente de seguridad de información?			
2.2	¿Se establece el procedimiento para manejar los incidentes?			
2.3	¿Se incluyen los requisitos para conformar el equipo de respuesta a incidentes, con roles y responsabilidades?			
2.4	¿Se cuenta con los requisitos para la creación de un plan probado de respuesta a incidentes, con sus objetivos, procedimientos y directrices?			
2.5	¿Se incluye el proceso para documentar y cerrar los incidentes?			
2.6	¿Se incluye el análisis de impacto en el negocio (BIA)?			

2.7	¿Se establecen los requisitos para la recuperación de los sistemas críticos?			
3	**Gestión de activos**	**Propósito**: Garantizar el adecuado manejo de los activos		
3.1	¿Se establece la propiedad de la información?			
3.2	¿Se establece la adecuada utilización de los recursos?			
3.3	¿Se encuentra el ciclo de vida de los activos establecido?			
3.4	¿Se establecen las medidas de protección de activos?			
4	**Reglas de conducta**	**Propósito**: Delimitar el uso y comportamiento apropiado		
4.1	¿Se establece la privacidad de la información?			
4.2	¿Se define el uso adecuado de los sistemas?			
4.3	¿Se incluye el uso adecuado de internet, correo y mensajería instantánea?			
4.4	¿Se incluye el uso de acceso remoto?			
4.5	¿Se establece el uso de redes sociales?			
5	**Gestión de proveedores**	**Propósito**: Gestionar el adecuado servicio de los proveedores		
5.1	¿Se establecen los términos y condiciones referentes a la seguridad que deben cumplir los proveedores?			
5.2	¿Se establecen las evaluaciones a proveedores?			
5.3	¿Se establecen los procedimientos para la verificación de la seguridad para adquisiciones y/o desarrollos?			
6	**Gestión de riesgos**			
6.1	¿Se establece el alcance de la gestión de riesgos?			
6.2	¿Se establecen los roles y responsabilidades?			
6.3	¿Se define la metodología a utilizar?			
6.4	¿Se establecen las técnicas y herramientas a utilizar?			

Comprensión y evaluación de la estructura organizacional

La finalidad de la siguiente plantilla es evaluar la estructura de la organización de acuerdo con las mejores prácticas.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

Estructura de la organización

Objetivo: Comprender y evaluar la estructura de la organización de acuerdo con las mejores prácticas

Auditor:	**Criterio:** COBIT 5, DSS05 Gestionar Servicios de Seguridad

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Está formalmente establecida la estructura organizativa?				
2	¿Tiene la estructura organizativa un mandato claro y documentado?				
3	¿Se evalúa regularmente el desempeño de la estructura organizativa y sus miembros por asesores externos?				
4	¿Existe un procedimiento de escalaciones?				
5	¿Están definidos los niveles de autoridad y son respetados?				

Comprensión y evaluación de la cultura, ética y comportamiento

La siguiente lista de verificación fue aplicada con el fin de evaluar la cultura, ética y comportamiento dentro de la organización.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

Cultura, ética y comportamiento					
Objetivo: Comprender y evaluar la cultura, ética y comportamiento relacionado con la seguridad de la información					
Auditor:		**Criterio:** COBIT 5, DSS05 Gestionar Servicios de Seguridad			
No.	**Verificación**	**Cumplimiento**			**Comentarios u observaciones**
		Sí	**No**	**Parcial**	
1	¿Se establecen las conductas y/o comportamientos de los colaboradores?				
2	¿Se cumplen los comportamientos establecidos?				
3	¿Existen capacitaciones periódicas sobre la seguridad de la información?				
4	¿Se realizan comunicados sobre ética, cultura organizativa y/o comportamiento?				
5	¿Existe un programa de incentivos a los colaboradores que cumplen los lineamientos establecidos?				

Comprensión y evaluación de los elementos de información

La siguiente plantilla sirve para evaluar la información generada en el proceso evaluado de seguridad de la información.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

Elementos de información

Objetivo: Comprender y evaluar los elementos de información generados en el proceso de seguridad de la información del proceso a evaluar.

Auditor:	**Criterio:** COBIT 5, DSS05 Gestionar Servicios de Seguridad

No.	Verificación	Cumplimiento			Comentarios u observaciones
		Sí	No	Parcial	
1	¿Existe un procedimiento documentado del proceso de nóminas?				
2	¿Se identifican en el procedimiento las partes interesadas en el proceso de nóminas?				
3	¿Se tienen definidos los servicios y aplicaciones de TI que soportan el proceso de nóminas?				
4	¿Existen métricas para comprobar la exactitud de la información generada?				
5	¿Se encuentra disponible la información cuando es requerida por alguna parte interesada?				

Comprensión y evaluación de los servicios, infraestructura y aplicaciones

La siguiente plantilla sirve para comprender los objetivos del servicio brindado y evaluarlos de acuerdo con las métricas establecidas por la organización.

UNIVERSIDAD DE COSTA RICA | PROGRAMA DE POSGRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS TRABAJO FINAL DE GRADUACIÓN	Referencia
	Versión: 01

Servicios, infraestructura y aplicaciones					
Objetivo: Comprender y evaluar la efectividad de los objetivos de servicios, infraestructura y aplicaciones de acuerdo con las métricas establecidas por la organización del servicio analizado					
Auditor:		**Criterio:** COBIT 5, DSS05 Gestionar Servicios de Seguridad			
No.	**Verificación**	**Cumplimiento**			**Comentarios u observaciones**
		Sí	**No**	**Parcial**	
1	¿Existe un documento del servicio brindado por TI para soportar la administración de nóminas?				
2	¿Se encuentra disponible para los interesados el documento con la especificación del servicio brindado?				
3	¿Se establece la calidad de los entregables del servicio?				
4	¿Se entrega el servicio en el tiempo pactado?				
5	¿Se cumple con las métricas establecidas para el servicio brindado?				
6	¿Se establece un acuerdo de nivel operativo (OLA) en el servicio brindado por TI?				
7	¿Se establece un acuerdo de nivel de servicio (SLA) con los proveedores de servicios tecnológicos?				

CAPÍTULO 5 - Análisis de resultados

Una vez aplicadas las plantillas mostradas en el capítulo 4 de este documento, se procedió a realizar un análisis de la información recolectada, con el fin de identificar los hallazgos resultantes de la auditoría.

El análisis se realizó en diferentes etapas, iniciando con el entendimiento del negocio y determinando las partes interesadas en el tema auditado. Seguidamente se procedió a evaluar los diferentes procesos de la seguridad de la información. Esta tarea se realizó con las prácticas claves de COBIT 5 mencionadas en el proceso DSS05 “Gestionar los servicios de seguridad”, utilizando las plantillas indicadas en el punto 4.6.1 del capítulo anterior, en donde se analizó:

- El grado de protección contra el software malicioso.
- La gestión de la seguridad de la red y las conexiones.
- La gestión de la seguridad de los puestos de usuario final.
- La identidad del usuario y el acceso lógico.
- Los accesos físicos a los activos de TI.
- Los documentos sensibles y dispositivos de salida.
- La supervisión de la infraestructura para detectar eventos relacionados con la seguridad.

Adicional a estos puntos analizados, se evaluaron las políticas existentes con respecto a la seguridad de la información de acuerdo con las mejores prácticas de COBIT 5, así como la estructura organizativa, la cultura, ética y los servicios de infraestructura que soportan el proceso auditado.

Como resultado del análisis, se encontraron algunas debilidades las cuales fueron expuestas en forma detallada a la administración del Grupo STT, pero que seguidamente se mencionan en forma general por aspectos de confidencialidad ya explicados anteriormente.

Con respecto a las políticas de seguridad que debe tener la organización, algunas políticas básicas no existen en la compañía, mientras que las existentes

son políticas débiles, lo que permite que haya falta de claridad en los roles y responsabilidades al momento de ocurrir un incidente de seguridad.

También se determinaron algunas debilidades en procedimientos y controles, como por ejemplo la falta de revisiones periódicas a los accesos asignados tanto a los sistemas como a la información almacenada. Esto puede llegar a permitir que se manipule información confidencial, sensible y relevante por parte de personas que ya no deberían tener estos privilegios.

Por otro lado, en la organización no se realizan pruebas periódicas sobre la seguridad de la infraestructura y los sistemas, con el fin de determinar su adecuada protección.

Hay poca información para los colaboradores sobre posibles amenazas de software malicioso y capacitaciones sobre la seguridad de la información, lo que puede causar que, sin dolo, un colaborador abra una brecha en la seguridad que perjudique los procesos y documentación de la organización.

En el estudio se detectó que el área de Talento Humano no le informa al Departamento de TI en el menor tiempo posible los movimientos o salidas del personal, para que éste pueda modificar los accesos oportunamente y evitar que sean utilizados por personas no autorizadas.

A pesar de la existencia de algunas deficiencias detectadas en el análisis realizado, se logró determinar que en la compañía se tiene un grado razonable respecto a la seguridad de la información. Estas deficiencias serán mostradas detalladamente como hallazgos de auditoría en el informe final.

En cada hallazgo se mostrará la situación actual encontrada, la causa del por qué sucede la desviación encontrada, el efecto que podría tener si se materializa la situación detectada y por último el criterio de la norma o marco de referencia aplicable donde se indica cómo debe ser.

Finalmente, se realiza una recomendación a la persona competente, para tomar las acciones necesarias con el fin de solucionar en el corto plazo cada hallazgo detectado.

CAPÍTULO 6 - Conclusiones y recomendaciones

Conclusiones y recomendaciones del estudio aplicado

Seguidamente, se muestran las principales conclusiones y recomendaciones de la auditoría aplicada, dada la solicitud de la compañía en mantener la confidencialidad, se expresan en una forma general.

Conclusiones

Con el estudio realizado, se evaluó lo adecuado del proceso interno actual para administrar la seguridad de la información de la empresa y los datos del sistema de Administración de Nóminas, por medio de la aplicación de diferentes técnicas de auditoría, además, se determinaron los principales riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información.

Gracias al trabajo efectuado, se logró determinar la suficiencia de la seguridad de la información en la compañía y se emitieron las recomendaciones correspondientes a los aspectos encontrados sujetos a mejora, con el objetivo de reforzar los puntos débiles detectados y así soportar los requerimientos del negocio.

Es importante que, a corto, la alta dirección, así como los diferentes roles responsables de velar por la seguridad de la información, tomen las medidas necesarias que contribuyan a mitigar las situaciones descritas en el Informe Final dado a la organización, con el fin de establecer una adecuada seguridad de la información.

Recomendaciones

Se recomienda a la alta dirección, adoptar un marco de referencia o norma para la seguridad de la información, para reforzar la seguridad de la información en la compañía. Además, se le recomienda establecer una política de la seguridad de la información la cual se debe alinear con los requerimientos del negocio y establecer roles y responsabilidades que deben cumplir todos los involucrados en el proceso, así como, la creación de las políticas básicas que solicitan las mejores

prácticas como lo son COBIT 5 o ISO 27001. Estas políticas deben someterse a revisiones periódicas con el fin de mantenerlas actualizadas.

Se le sugiere al coordinador de Talento Humano, formular un programa de concienciación para los colaboradores con respecto al tema de seguridad de la información, así como coordinar con el área de TI para que le facilite la información que se debe de enviar en las alertas sobre posibles amenazas de software malicioso que puedan afectar la a compañía. Por otra parte, informar al área de TI cualquier movimiento o salida de personal en el menor tiempo posible, para que TI pueda modificar los accesos oportunamente.

Al coordinador de TI, se recomienda reforzar las debilidades detectadas en los controles que soportan la seguridad de la información, así como realizar diferentes pruebas internas periódicamente con el fin de determinar que se brinda una adecuada seguridad de la infraestructura en la organización.

Es importante que se tomen las medidas necesarias para mitigar los hallazgos detectados en un corto plazo y así asegurar una adecuada seguridad de la información.

Conclusiones del proyecto aplicado

La utilización del marco de referencia de COBIT 5 de ISACA, es sin duda el pilar de este proyecto aplicado, gracias a este marco, se logró realizar una auditoría de la seguridad de la información siguiendo las mejores prácticas.

Este trabajo beneficia a la empresa donde se ejecutó por medio de las recomendaciones brindadas que refuerzan la seguridad de la información y también, por medio de las plantillas elaboradas en la aplicación del estudio, las cuales pueden ser utilizadas para futuras auditorías en la compañía e inclusive por todo aquel profesional que quiera utilizarlas en el desarrollo de futuros estudios de auditoría de esta naturaleza.

Gracias al desarrollo de este proyecto, en lo personal, he reforzado los conocimientos teóricos vistos durante toda la carrera de Auditoría en Tecnologías de Información, lo que crea en mí, un mejor profesional que realizará su rol de auditor en forma competente y ética.

Recomendaciones resultantes del desarrollo del trabajo final de graduación.

Es importante que las empresas cuenten con un marco de referencia o norma para tratar la seguridad de la información, por lo que la primera recomendación es para que las organizaciones adopten un marco de referencia que les brinde las mejores prácticas para mejorar el desempeño de TI y seguridad de la información. Entre estos se encuentra COBIT 5 y la ISO 27000, por lo que la compañía debe evaluar cuál se ajusta más a su enfoque del negocio.

Los profesionales de auditoría de Tecnologías de Información deben aportar recomendaciones viables y esto se logra gracias al conocimiento de las mejores prácticas. Como parte del desarrollo profesional, existen certificaciones para los auditores, donde se refuerza el conocimiento en auditoría de las Tecnologías de la Información, por lo que se recomienda, de ser posible, alcanzar estas certificaciones, ya que, gracias a esto, proyectos como el desarrollado se pueden realizar de manera correcta.

No queda de más recomendar a todos los expertos de auditoría realizar este tipo de evaluaciones con los más altos grados de ética y profesionalismo, con el fin de brindar un valor agregado a sus organizaciones y beneficiar a la sociedad en general.

CAPÍTULO 7 - Bibliografía

Asamblea Legislativa. (05 de setiembre de 2011). Ley N.º 8968. *Ley de protección de la persona*. San José, Costa Rica.

Barrantes, E. R. (2009). *La investigación: un camino al conocimiento.* San José, Costa Rica: UNED. Recuperado el 17 de octubre de 2017, de https://www.uned.ac.cr/academica/images/ceced/docs/Investigacion_camino_conocimiento.pdf

Boris, R. (29 de setiembre de 2017). *US$5 millones en promedio le costaría una fuga de información*. Recuperado el 01 de octubre de 2017, de IT Now: https://revistaitnow.com/us5-millones-promedio-le-costaria-una-fuga-informacion/

CGR. (2014). *Normas Generales de Auditoría para l Sector Público.* San José: Contraloría General de la República de Costa Rica. Recuperado el 30 de Setiembre de 2017, de www.cgr.go.cr

Gómez López, R. (2004a). *Evolución científica y metodológica de la economía*. Recuperado el 25 de Setiembre de 2017, de Eumed.net: http://www.eumed.net/cursecon/libreria/rgl-evol/2.4.1.htm

Gómez López, R. (2004b). *Evolución científica y metodológia de la economía*. Recuperado el 25 de Setiembre de 2017, de Edumed.net: http://www.edumed.net/cursecon/libreria/rgl-evol/2.4.2.htm

Hernández Sampieri, R. (2007). *Metodología de la Investigacion.* México: McGraw Hill.

ISACA. (2012a). *Cobit 5 para la seguridad de la información.* Estados Unidos: ISACA.

ISACA. (2012b). *Un marco de Negocio para el Gobierno y Gestión de las TI de la Empresa.* Estados Unidos: ISACA.

ISO27000. (2012). *SGSI*. Recuperado el 5 de Noviembre de 2017, de Iso27000.es: http://www.iso27000.es/sgsi.html

Martínez López, A. (noviembre de 2010). *¿Qué es, y para qué nos sirve el Método científico?* Recuperado el 25 de Setiembre de 2017, de Blogspot.com: http://cientificmethodkids.blogspot.com/

STT, G. (2015). *GES-PR-02 Procedimiento de Auditoría Interna. V2.* San José.