“EVALUACIÓN DE LA CAPACIDAD DE DETECCIÓN Y RESPUESTA A RIESGOS DE CIBERSEGURIDAD, CASO DE LA EMPRESA SISC”

Trabajo de Investigación presentado

para optar al Grado Académico de

Magister en Auditoría

Presentado por:

Sr. Mendoza Silva, Luis Fernando

Sr. Vega Gallegos, Giancarlo Roberto

Asesor: Profesor Alejandro Magdits Gutiérrez

2019

Resumen ejecutivo

Es un tema de preocupación actual la constante y creciente amenaza de ciberataques que ponen en serio riesgo la información y los sistemas de negocio de las empresas. De modo que se hace indispensable que la alta dirección de la empresa Servicios Integrales de Servicios Compartidos (SISC) conozca cuál es el nivel de capacidad alcanzado por la gestión de la ciberseguridad y, además, conocer qué medidas debe implementar para mejorar su capacidad de gestionar eventos que puedan afectar la normal operación en la empresa.

El presente trabajo de investigación tuvo por objetivos diagnosticar el nivel de capacidad en la gestión de la ciberseguridad de la empresa, identificar las brechas para diseñar y proponer los controles claves para fortalecer la ciberseguridad y, por último, elaborar y proponer la hoja de ruta de implementación de los controles clave. Asimismo, se limitó el alcance a los aspectos relacionados a la detección y respuesta de eventos relacionados a la ciberseguridad.

De otro lado, cabe señalar que el trabajo ha sido dividido en cinco capítulos. El primero de ellos es la introducción, que describe el contexto actual de la ciberseguridad y los retos que este mismo presenta. El segundo capítulo delimita con mayor detalle el problema materia de la investigación como la incapacidad de la empresa para detectar y responder a un evento de ciberseguridad. En el tercer capítulo, se describe el marco de referencia en ciberseguridad del National Institute of Standards and Technology de Estados Unidos (NIST) (2018), que se ha usado como el principal marco de referencia. Asimismo, se describe la norma ISO/IEC 33020-2015 (International Standard Organization 2015) como referente para la evaluación de capacidad actual de los procesos y la guía COBIT 5 para riesgos (ISACA 2013), que es utilizada para la gestión y el control de riesgos asociados a la tecnología de la información. Ambos documentos serán tomados como complementos referenciales para este trabajo de investigación. Más adelante, en el cuarto capítulo, se describe la metodología usada, que comprende el priorizar y delimitar las áreas de negocio dentro de un rango de alcance, identificar los activos de información involucrados, efectuar el análisis de capacidad actual de los procesos, ejecutar una evaluación de riesgos, determinar y priorizar las brechas encontradas y desarrollar la hoja de ruta de implementación de las mejoras. Luego, en el quinto capítulo, se muestran los resultados de la investigación, que corresponden a la evaluación de capacidad de los procesos investigados y el análisis de riesgos dentro del contexto de la ciberseguridad; asimismo, se presentan los controles recomendados para superar las brechas de capacidad identificadas.

Finalmente, no es menos importante mencionar que el presente trabajo supuso un reto por el hecho de aplicar una metodología relativamente nueva dentro del fenómeno –también nuevo- de la ciberseguridad y cómo se le entiende en el marco del uso de la tecnología de la información en el mundo actual.

Índice

Índice de tablas

Índice de gráficos

Índice de anexos

Capítulo I. Introducción

La ciberseguridad es una parte de la seguridad de la información que se enfoca en la protección de los activos de información al direccionar las amenazas a la información que se procesa, almacena y transporta a través de los sistemas de información que trabajan sobre la Internet (ISACA 2017).

Hoy en día, la ciberseguridad está tomando protagonismo debido al incremento de ataques que se produce en el mundo virtual. Estos ataques no solo continúan incrementándose, sino que cambian constantemente sus procedimientos de acción. Así, se han convertido en un potencial peligro para las empresas que reciben sus irrupciones. Un escenario como este trae nuevos retos a las organizaciones, algo que no es ajeno para la empresa Servicios Integrales de Servicios Compartidos (SISC), pues, si bien no ha sufrido aún ataques cibernéticos que hayan afectado sus operaciones, no es improbable que pueda ocurrir algo parecido en el futuro próximo.

De este modo, surgen preguntas e inquietudes en los ejecutivos sobre cuán segura se encuentra la empresa de no sufrir un ciberataque; y, de ocurrir, cuál sería su capacidad de respuesta. SISC depende de los sistemas de información para la entrega de sus servicios; asimismo, hace uso intensivo de Internet para comunicarse con sus proveedores y clientes, dar soporte remoto o entregar sus servicios a sus clientes. Por esto, es preciso que la empresa cuente con los controles necesarios que la protejan de ataques cibernéticos.

El presente trabajo busca efectuar el diagnóstico de la situación actual de la empresa en relación con la ciberseguridad. De este modo, se pretende identificar las brechas y culminar con el desarrollo del plan de implementación de las mejoras a efectuar en la empresa. Para este propósito, nos basaremos en la versión 1.1 del marco de referencia para la mejora de la Infraestructura Crítica en Ciberseguridad del National Institute of Standards and Technology de Estados Unidos (NIST) (2018).

Capitulo II. Planteamiento del problema

1. Antecedentes

Para empezar, se debe mencionar el ciberataque ocurrido el 12 de mayo del 2017, que fue originado por la diseminación del virus llamado Wannacry, que comprendió un ciberataque de escala mundial y dimensión nunca antes vista, pues afectó a instituciones y empresas en más de 70 países. El virus suponía un fragmento de software que secuestraba los archivos de una computadora para, posteriormente, pedir un pago antes de restaurar los archivos cifrados.

El mencionado ataque, aunque no produjo daños a la información contenida en los sistemas de información de la empresa SISC, sí la llevó a aplicar la medida reactiva y extrema de aislarse de Internet, lo que significó tener que paralizar parcialmente sus operaciones por dos días. Asimismo, reveló diversos problemas técnicos, por ejemplo, el no haberse aplicado un parche de seguridad sobre los sistemas informáticos, que estaba disponible desde mediados de marzo; también, el no disponer de procesos automatizados que facilitaran un despliegue rápido de dicho parche; y la existencia de sistemas operativos en desuso vulnerables a este tipo de ataque cibernético.

Lo ocurrido confirma lo que importantes foros y especialistas han revelado:

- Ocho de cada 10 vulneraciones se detectan dentro de las 24 horas (estadísticas del Gobierno del Reino Unido reveladas en la revista Auditor Interno) (Mccollum 2016)
- Los delitos cibernéticos a nivel global aumentaron progresivamente. En el 2016, llegaron al segundo lugar, frente al cuarto que ocuparon en el 2014 (PWC México 2016).

2. Planteamiento del problema

2.1 Ambiente externo

Similarmente a los riesgos financieros y de reputación, los riesgos de ciberseguridad afectan la línea base de una compañía. Estos pueden elevar los costos e impactar en los ingresos, además, pueden dañar la habilidad de una organización para innovar, para ganar y mantener a sus clientes (Shackelford, Martell & Craig 2015: 307).

Los gobiernos, las empresas y los individuos están constantemente incrementando su preocupación acerca de la seguridad en los sistemas de cómputo en la red, y tal preocupación está justificada. La prensa reporta ataques exitosos que crecen con más frecuencia, entre ellos, el hurto de contraseñas de los consumidores, las brechas a gran escala de la información personal de los clientes corporativos, los ataques distribuidos de denegación de servicio sobre páginas web, el ciberespionaje dirigido a documentos clasificados, y los ataques sobre las infraestructuras críticas. Consecuentemente, las gerencias están invirtiendo en medios tecnológicos. No obstante, las soluciones tecnológicas son de menos utilidad si no están desplegadas de manera completa y correcta o si las prácticas operativas permiten a los atacantes evadirlas (Mulligan & Schneider 2011:70).

La probabilidad de brechas en la seguridad de los datos de negocio se está incrementando con un 60% de organizaciones que sufrieron más de un incidente de seguridad en el 2015. Para direccionar esta amenaza, el 48% de las organizaciones incrementaron sus inversiones en tecnologías de seguridad y un 78% desarrollaron un plan de respuesta a estas amenazas (Dedeke 2017:47). Así, las empresas de *retail*, información, fabricación, finanzas y seguros, consistentemente poseen el mayor riesgo y el mayor costo por evento de ciberseguridad (Romanosky 2016: 122).

De este modo, resulta importante y necesario contar con un plan de respuesta para mitigar el riesgo de que una brecha tenga un impacto sustancial en la empresa. No tenerlo ocasiona que no haya una clara definición de los participantes y sus responsabilidades en la ejecución de este plan (Sobowale 2017:35). Como se sabe, la información factual relacionada con los incidentes reportados indica que aquellos sufridos por las empresas son, en general, de carácter aleatorio, tanto en términos de ocurrencia como en su naturaleza. Claro está que las empresas no están libres de ser afectadas por los incidentes de seguridad de la información (Armin, Parinaz, Yang & Mingyan 2016: 26).

Se debe tomar en cuenta que los posibles infractores desarrollan nuevas habilidades y estrategias continuamente para realizar ciberataques. Por ello, es muy importante aprender de las experiencias propias y compartir para conseguir apoyo mutuo (EY 2017: 9). En especial, porque se sabe que la confianza mostrada por las empresas para resistir a ciberataques es ilusoria y de corta duración ante la magnitud el crecimiento de los riesgos y amenazas relacionadas con el mayor conocimiento de los cibercriminales sobre la explotación de las debilidades humanas del personal (EY 2017: 22).

Hoy en día los ciberataques son difíciles de ocultar, y es importante que las organizaciones puedan coordinar y dirigir las comunicaciones antes de que sean los medios de comunicación tradicionales y los de comunicación social quienes se hagan cargo (EY 2017: 34). Finalmente, vale mencionar que, de acuerdo con el Global Risk Report (World Economic Forum 2018), los ciberataques se ubican como el tercer riesgo a nivel mundial con mayor probabilidad de ocurrir.

Podemos, entonces, resumir los problemas relacionados con el ambiente externo de la siguiente manera:

- Las empresas cada vez tienen mayor necesidad por incrementar su presencia en Internet, tanto para poder realizar negocios, como para relacionarse con sus clientes. Una presencia más desplegada en Internet las expone al riesgo de sufrir ciberataques, que pueden ser o no expresamente dirigidos a ellas. En cualquier caso, los ciberataques aprovecharán las vulnerabilidades para poder introducirse en la red de las empresas y ocasionar daños sobre los sistemas de información que afectarán a la información de la empresa.
- Los riesgos y amenazas asociados a ciberataques están continuamente evolucionando.
- Al aumentar la sofisticación de los ciberataques, ninguna empresa debe sentirse segura de que no será afectada por un ciberataque.
- La empresa SISC ha aumentado su presencia en Internet, por lo cual su nivel de riesgo a sufrir ciberataques se ha incrementado.

2.2 Ambiente interno

La pérdida de los servicios de operación de la infraestructura de tecnología de la información brindados al cliente más importante de SISC a mediados del año 2013, trajo como consecuencia que la Gerencia de tecnologías y sistemas de negocio de SISC deba redimensionar su organización. De este modo, debóe reducir sus capacidades en la gestión de la seguridad de la información (en personal se pasó de tres a un solo recurso), tanto para los servicios entregados a clientes externos como para su gestión interna. La reducción de capacidades en seguridad de la información se vio reflejada con la reducción de personal y en la sobrecarga de funciones a otro personal.

Por otro lado, la organización de Tecnología y Sistemas de Negocio ha privilegiado manejarse bajo un enfoque que gestiona la tecnología, en contraposición con un enfoque de gestión de servicios soportado en los procesos. Asimismo, en los últimos cinco años, no se han realizado

inversiones en nuevas soluciones de seguridad, y se ha mantenido únicamente la renovación de los productos de seguridad ya existentes.

En materia de seguridad de la información en la empresa SISC, existe un enfoque centrado en adquirir y operar las plataformas de seguridad que protejan los activos de información, de allí que la gestión se ha centrado en la operación técnica de las soluciones de seguridad. Sin embargo, esto último ha revelado no ser suficiente para poder detectar y responder un ataque que provenga del ciberespacio, como fue evidenciado ante los hechos ocurridos en los ciberataques del 12 de mayo del 2017 (Ransomware WannaCry) y, posteriormente, el del 27 de junio del 2017 (Ransomware Petya). El ciberataque del 12 de mayo reveló que no se habían aplicado los parches de seguridad sobre el sistema de operativo de Windows, a pesar de que estos se habían revelado y publicado dos meses atrás por la empresa propietaria del software.

Con relación al rol de la gerencia sobre los cambios internos en su estructura, se conoce que enfrenta un dilema por no considerar los aspectos sensibles al cambio, los cuales involucran un rediseño de la organización, así como mantener los controles establecidos dentro del área de Tecnologías y Sistemas de Negocio, que se ha visto seriamente afectada por la pérdida de recursos. La gerencia ha reasignado funciones y responsabilidades sin haber realizado una adecuada evaluación del personal con potencial, adaptación al cambio y con la disposición de aprender rápidamente, con el propósito de asegurar, de este modo, el logro de sus objetivos. (Hernández, Gallarzo & Espinoza 2011).

Asimismo, la gerencia es responsable de la conducción de la organización y, tomando en cuenta los cambios internos señalados, la dirección no está ejerciendo plenamente sus roles, principalmente el de administrador, arquitecto y humano. La organización carece de una estructura óptima que responda a las necesidades tanto del cliente interno como externo, por ello, la asignación de recursos no está alineada al logro de objetivos. (Lazzati 2016). La seguridad cibernética es una responsabilidad compartida en una organización, los altos directivos deben apoyar todo esfuerzo que se realice y los empleados deben aprender a mantenerse alejado de los problemas, como, por ejemplo, evitar abrir correos electrónicos sospechosos (EY 2017: 9)

Finalmente, las empresas necesitan cambiar la forma en la que piensan sobre la ciberseguridad. Dicho de otro modo, necesitan concentrarse en otros aspectos además de la prevención, y empezar a desarrollar estrategias que enfaticen la detección y la respuesta (Mccollum 2016:11).

Podemos, entonces, resumir los problemas relacionados con el ambiente interno de la manera siguiente:

- Poca conciencia y falta de apoyo de la alta gerencia para alcanzar una resilencia efectiva a los ciberataques.
- Los temas de ciberseguridad o seguridad de la información no son abordados en los comités de gerencia. A esto se suma la falta de reportes con información relacionada.
- Limitaciones presupuestarias para incrementar la efectividad de la operación de la seguridad de la información.
- Se ha debilitado al equipo de seguridad de la información, con lo cual se han distendido los controles asociados a la ciberseguridad.
- Falta de recursos calificados, pues no se ha previsto la formación y especialización en tópicos de ciberseguridad, ni se han adquirido estas competencias contratando personal especializado.
- No se están tomando las previsiones y acciones necesarias para controlar efectivamente los riesgos asociados a los ciberataques.
- En los asuntos de ciberseguridad, se centra la acción en la gestión técnica de herramientas de seguridad en contraposición a una gestión de procesos centrada en la detección y respuesta a los incidentes de ciberseguridad.

3. Objetivos

3.1. Objetivo general

El objetivo de esta investigación es identificar las brechas en materia de ciberseguridad que están relacionadas con la detección y respuesta a los eventos de ciberseguridad en la empresa SISC. De este modo, se busca determinar los controles necesarios para cerrar las brechas existentes y proponer el plan de implementación de dichos controles. Como marco de referencia, se utilizará la versión 1.1 del marco desarrollado por el National Institute of Standards and Technology de Estados Unidos (NIST): Framework for Improving Critical Infrastructure Cybersecurity (NIST 2018).

3.2. Objetivos específicos

- Recabar la información necesaria para evaluar el nivel de capacidad en la gestión de la ciberseguridad de la organización.
- Diagnosticar las brechas existentes en los procesos de detección y respuesta de incidentes de ciberseguridad en la empresa y así determinar el nivel de capacidad de ciberseguridad en los procesos indicados. Con este fin, se utilizará el marco de referencia de ciberseguridad del NIST (2018).
- Analizar los escenarios de riesgos específicos relacionados a la ciberseguridad.
- Diseñar y proponer los controles clave de gestión para fortalecer la ciberseguridad en referencia a las brechas identificadas en el diagnóstico ejecutado.
- Elaborar y proponer la hoja de ruta para implementar los controles clave que permitan superar las brechas encontradas si se considera el nivel de deficiencia de los procesos evaluados.

4. Preguntas de investigación

- ¿Qué elementos se deben considerar para ejecutar la planificación de la evaluación de capacidad en la gestión de la ciberseguridad en la empresa?
- ¿Cuáles son los principales riesgos de ciberseguridad en la empresa?
- ¿Cuál es la actual capacidad de detección y respuesta de la empresa ante un ciberataque a los sistemas de información?
- ¿Cuál es el nivel de capacidad en ciberseguridad que la empresa debe tener al aplicar el marco de referencia de ciberseguridad del NIST?
- ¿Cuáles son los controles claves que debe implementar la empresa para fortalecer su gestión de riesgos en ciberseguridad?

5. Justificación

El presente tema de investigación se encuentra justificado como se señala a continuación:

- Mejorar el nivel de entendimiento de la gerencia sobre la ciberseguridad y su relevancia en el negocio.
- En relación a los procesos a investigar, «las funciones de detectar y responder combinadas, posibilitan monitorear y responder proactivamente, respectivamente» (Dedeke 2017:49).

- Según una encuesta global de Ernst and Young (2017), el 86% de las organizaciones señala que su función de seguridad cibernética no satisface plenamente sus necesidades. En el caso del Perú, esa cifra se eleva al 90% (Gestión 2017).
- Luis Moreno, presidente del Banco Interamericano de Desarrollo, nos dice que una enorme mayoría de los países latinoamericanos y del Caribe están aún poco preparados para contrarrestar la amenaza del cibercrimen (Banco Interamericano de Desarrollo 2016: XI).
- El Marco de ciberseguridad del NIST provee un procedimiento para mapear las mejores prácticas de ciberseguridad, determinar el completo estado de las prácticas de gestión de riesgo en ciberseguridad de la organización y estructurar una hoja de ruta para que las organizaciones mitiguen estos riesgos (Shackelford, Martell & Craig 2015: 308).
- Permitir a la gerencia contar con una hoja de ruta que le servirá para implementar los controles en ciberseguridad que se precisen.

6. Limitaciones

- La evaluación se hará a las sedes administrativas que ocupa SISC en Lima y a su personal en estas sedes.
- La evaluación se hará a las líneas de negocio que tienen más exposición a riesgos en ciberseguridad.
- La evaluación solo incluirá los aspectos relacionados a la operación de la empresa evaluada.
- La evaluación se hará únicamente a la infraestructura de tecnologías de la información bajo gestión de la empresa.

7. Delimitaciones

- El período del estudio es de 6 meses.
- Se evaluarán solo los procesos de tecnologías de la información relacionados con la ciberseguridad en los aspectos relacionados a la detección y respuesta.

Capítulo III. Marco conceptual

1. Marco teórico

La presente investigación se desarrollará apoyándose en los siguientes marcos y estándares:

- El Marco de referencia para la mejora de la infraestructura crítica de ciberseguridad (NIST 2018) para la definición de actividades de los procesos de gestión de la ciberseguridad, materia de la presente investigación.
- El documento de Implementación del marco de ciberseguridad del NIST (ISACA 2014), que describe los pasos para una evaluación en ciberseguridad y el Programa de auditoría/aseguramiento del marco de ciberseguridad (ISACA 2016), que provee una hoja Excel desarrollada para cada subcategoría del marco de referencia de ciberseguridad del NIST y que, asimismo, permite evaluar la efectividad de los controles en la organización.
- El Estándar ISO 33020: 2015, Evaluación de procesos (International Standard Organization 2015) para medir el nivel de capacidad de los procesos evaluados.
- Los principios de COBIT 5 para riesgos (ISACA 2013), para definir los escenarios de riesgos relacionados a la ciberseguridad.

A continuación, se detallan los marcos y estándares indicados.

1.1. Marco de referencia para la mejora de la infraestructura crítica de ciberseguridad del NIST

Un tema importante para la presente investigación es seleccionar el marco de referencia en ciberseguridad, el cual nos debe entregar los aspectos que se deben evaluar para los procesos de detección y respuesta que forman parte de esta investigación. Así, el Marco de referencia para la mejora de la infraestructura crítica de ciberseguridad, versión 1.1 (NIST 2018) es un enfoque que busca gestionar los riesgos de ciberseguridad, y se compone de tres partes: el núcleo del marco de referencia, los niveles de implementación del marco de referencia y los perfiles del marco de referencia. Para la investigación, se utilizarán el núcleo y los perfiles del marco de referencia, pues estos permitirán establecer el mapa de ruta de las mejoras a implementar.

El uso del marco de referencia del NIST se sustenta en lo indicado a continuación:

- El marco actúa como la piedra angular para ayudar a las organizaciones en el cumplimiento de los requerimientos de ciberseguridad. Por ser adaptable, su uso se puede aplicar a todo tipo de industria (Scofield 2016: 25).
- «La flexibilidad del marco permite un enfoque para direccionar los riegos de ciberseguridad más allá de la organización, industria o país» (Shackelford, Martell & Craig 2015: 336).
- El marco entrega un lenguaje común a las empresas, para que estas puedan evaluar su situación actual en ciberseguridad, definir su estado objetivo, priorizar las oportunidades de mejoras y evaluar su progreso hacia el estado objetivo. Para esto, se establecen mecanismos de comunicación entre los interesados internos y externos acerca de los riesgos en ciberseguridad (Shackelford, Martell & Craig 2015:330).
- El marco es flexible y neutral a la tecnología, por lo que puede ser usado en organizaciones de cualquier tamaño, especialidad o grado de exposición al ciberriesgo. Asimismo, las organizaciones pueden usar el marco para evaluar su programa de ciberseguridad existente o para diseñar e implementar uno, así como para establecer metas en ciberseguridad (Shen 2014: 3).
- El marco es un punto de referencia para los objetivos de las evaluaciones de los programas de ciberseguridad de las organizaciones y para identificar potenciales brechas en dichos programas (Shen 2014: 6).
- Según Gartner, para el 2020 más del 50% de empresas privadas y públicas en los Estados Unidos usarán el marco de referencia de ciberseguridad del NIST (Tenable network security, inc 2016:1495).

Para los objetivos de la presente investigación, se utilizarán los contenidos del marco relacionados con los procesos de detección y respuesta. Los contenidos del marco nos describen las características de estos dos procesos que se evaluarán. En el anexo 1, se mostrará mayor detalle sobre el marco.

1.1.1. Implementación y programa de auditoría/aseguramiento del marco de ciberseguridad del NIST

Debido al incremento del volumen y sofisticación de los ciberataques, la Information Systems Audit and Control Association (ISACA) desarrolló un programa de aseguramiento y auditoría basado en el marco de referencia de ciberseguridad del NIST para proveer a las organizaciones

con una manera formal y repetible para evaluar los controles de ciberseguridad. Con este fin, se publican los documentos Implementando el marco de ciberseguridad del NIST (ISACA 2014) y el Programa de auditoría/aseguramiento de ciberseguridad (ISACA 2016).

El objetivo de una auditoría de ciberseguridad es evaluar la efectividad de los procesos, políticas, procedimientos, gobierno y otros controles de ciberseguridad. La revisión se enfoca en los estándares, lineamientos y procedimientos de ciberseguridad como también en la implementación de estos controles. Entonces, los pasos de auditoría elaborados por ISACA (2016) en el documento indicado se han desarrollado para cada subcategoría del marco de referencia de ciberseguridad del NIST. De este modo, permiten evaluar la efectividad de los controles en la organización. Por ejemplo, contiene una hoja de cálculo en Excel para un completo programa de auditoría/aseguramiento. Así, la presente investigación usará esta hoja de cálculo para la evaluación de los procesos de detección y respuesta. Mayor detalle sobre el programa se encuentra en el anexo 2.

1.2. ISO/IEC 33020:2015 Tecnología de la información -evaluación de procesos –marco de medición de procesos para evaluar la capacidad de los procesos

Para la presente investigación, se necesita un modelo de evaluación que nos permita medir el nivel de capacidad de los procesos de detección y respuesta en ciberseguridad descritos en el marco del NIST. Para este propósito, usaremos la norma ISO/IEC 33020: 2015 (International Standard Organization 2015), que es el estándar para la evaluación de la capacidad de los procesos como una característica del proceso. La evaluación de procesos es usada por una organización con el objetivo de determinar si existen y cuáles son las mejoras que deben ser incorporadas en el proceso analizado. En el anexo 3, se describe con mayor detalle sobre este estándar.

1.3. COBIT 5 para riesgos

Para la evaluación de riesgos en ciberseguridad se utilizará la versión 1.0 del documento COBIT 5 para riesgos (ISACA 2013). COBIT 5 para riesgos está construido sobre el marco de referencia de COBIT 5; asimismo, se enfoca en los riesgos y provee más detalle y una guía práctica para los profesionales del riesgo y otros interesados en todos los niveles de la empresa. Del mismo modo, COBIT 5 discute los riesgos relacionados con la tecnología de la información, de allí su adaptabilidad a la presente investigación.

De la publicación de COBIT 5 para riesgos, utilizaremos los denominados escenarios de riesgos genéricos que aplican a los aspectos relacionados a la ciberseguridad. Un escenario de riesgo de TI contiene una descripción de un evento relacionado a TI, que puede llevar a un evento de pérdida con impacto al negocio si este llegase a ocurrir. Para mayor detalle sobre COBIT 5 para riesgos, consultar el anexo 4.

2. Estado de la cuestión

De acuerdo con lo informado por el NIST, el marco de referencia de ciberseguridad estuvo en un proceso de actualización. Una propuesta de la nueva versión 1.1 fue anunciada el 10 de enero del 2017 y publicada para el comentario público. Finalmente, la versión final del marco de referencia 1.1 se publicó en abril del 2018. El marco de referencia actualizado (versión 1.1) es completamente compatible con la anterior versión 1.0. Para al presente estudio, nos basamos inicialmente en la versión 1.0 del marco de referencia de ciberseguridad del NIST (2014); sin embargo, a razón de que los cambios incorporados en la versión 1.1 no alteran el trabajo desarrollado, referenciaremos la versión del 2018 como la adoptada para el estudio.

ISACA, a través de Cybersecurity Nexus (CSX), promueve activamente todo aspecto relacionado con la ciberseguridad. Así, ha desarrollado publicaciones y herramientas que soportan la implementación y auditoría de los aspectos de ciberseguridad basados en el marco de referencia de ciberseguridad del NIST. La presente investigación hará uso de las herramientas desarrolladas como soporte a la evaluación de capacidad a desarrollar.

De acuerdo con Uudhila (2016), las instituciones deben ser proactivas en términos de adoptar medidas de ciberseguridad con el fin de gestionar tanto ataques de amplio espectro, como los dirigidos. Asimismo, Uudhila diseñó un estudio para usar el método de investigación cualitativa, desplegando un análisis en profundidad del comportamiento del personal de tecnologías de la información cuando gestiona los diferentes activos de información. Por otro lado, encuestas y entrevistas cara a cara fueron conducidas para entender los riesgos de ciberseguridad.

En el contexto de riesgos, Alvarado y Zumba (2015) indican que COBIT 5 para riesgos es el marco que permite que se logre un mejor entendimiento sobre el impacto de los riesgos de TI a

nivel de toda la institución. El principal motivo es que se trata de una guía de extremo a extremo para la forma de gestionar los mismos.

Como referencias que describen el problema actual en ciberseguridad tenemos lo siguiente:

- «Muchas firmas han empezado a invertir proactivamente en mejores prácticas de ciberseguridad para protegerse mejor por si mismos contra el incremento de ataques sofisticados, pero la siempre cambiante naturaleza del problema y elevado número de actores involucrados han convertido en un arte un estándar de ciberseguridad» (Shackelford, Martell & Craig 2015: 312).
- «Los tradicionales controles de seguridad en la red enfocados en el perímetro no son más efectivos, dado que ellos implican la idea de una red interna confiable» (Manos 2017:1)
- El presidente de la SEC, Jay Clayton, dijo que << "la ciberseguridad es critica a las operaciones de nuestros mercados y los riesgos son significativos y en muchos casos sistémicos. Debemos ser vigilantes, También debemos reconocer que, en ambos sectores, público y privado, habrá intrusiones, y que el componente clave de la gestión del ciberriesgo es la resiliencia y la recuperación>> (Newslife corp. 2017).

Asimismo, según el informe publicado por Deloitte (2016), se revela lo siguiente sobre Latinoamérica:

- Al ser la protección de información sensible una de las iniciativas prioritarias para las organizaciones en el 2016, se observa que esta prioridad responde al bajo nivel de madurez que existe en Latinoamérica para gestionar este riesgo.
- Cuatro de cada diez organizaciones no cuentan con capacidades, herramientas ni procedimientos específicos para responder a una brecha de seguridad. Por otra parte, solo una de cada cuatro organizaciones ha implementado tecnologías y procesos para responder de manera ordenada y rápida ante la ocurrencia de una brecha de seguridad.

3. Descripción del sector y la empresa

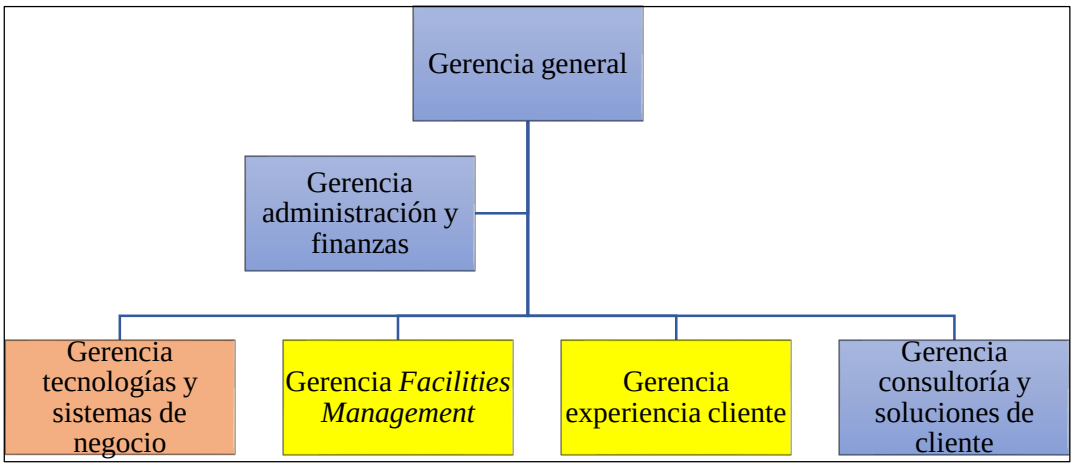
3.1. Giro del negocio

SISC es una empresa que da servicios integrales de soporte a la gestión a las diversas líneas de negocio de las empresas bajo un esquema de *outsourcing*. Así, presta servicios profesionales administrativos y de operación con los siguientes objetivos:

- Permitir que sus clientes concentren sus esfuerzos en las actividades que le generan mayor valor a su negocio.
- Proveer servicios con calidad, bajo acuerdos claros y competitivos.
- Incrementar la eficiencia operacional y generar economías de escala a través de la optimización de procesos, logro de sinergias, eficiencias y procesos *e-business*.
- Ofrecer la alternativa de cambiar costos fijos por variables en función del volumen de operaciones y del nivel de servicio prestado.

Su visión es ser la empresa líder en la prestación de servicios de soluciones de negocio a nivel nacional e internacional, reconocida por contribuir al crecimiento sostenido y rentable de sus clientes. Para ello, su misión es constituirse como una empresa internacional especializada en brindar servicio de soluciones de negocio confiables, eficientes y oportunas para permitir a sus clientes enfocarse en las actividades que les generen mayor valor. Asimismo, sus valores lo constituyen la credibilidad, respeto, imparcialidad, innovación y la confianza. Su estructura se muestra en el gráfico 1.

Gráfico 1. Estructura organizativa de SISC



Fuente: Elaboración propia, 2018.

La Gerencia de tecnologías y sistemas de negocio brinda servicios internos y externos en el desarrollo de sistemas de negocio y en la gestión de la infraestructura tecnológica de los sistemas de información a todas las otras líneas de la empresa. En esta gerencia, se ubica el oficial de seguridad como responsable de la seguridad de la información. Por otro lado, los dispositivos de seguridad son gestionados por el área de Infraestructura Tecnológica.

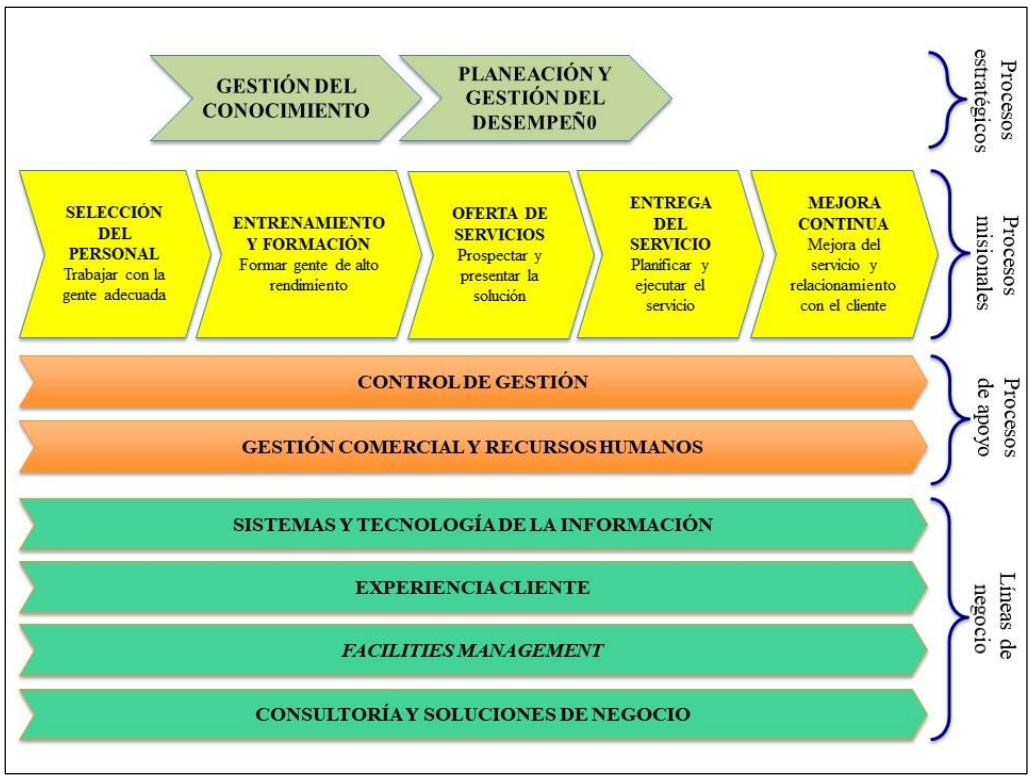
Las principales áreas dentro de SISC que dependen de los sistemas de información para la entrega de los servicios a sus clientes externos son las gerencias de Experiencia Cliente y *Facilities Management*. En conjunto, se puede decir que los objetivos estratégicos de SISC son los siguientes:

- En el foco cliente, satisfacer y fidelizar a sus clientes y posicionarse como proveedor de servicios empresariales.
- En el foco procesos, incrementar su calidad y eficiencia operacional y desarrollar soluciones creativas para las necesidades de los clientes.
- En el foco personal, desarrollar un capital humano, integrado, fidelizado y capacitado. Asimismo, fortalecer la cultura de servicio orientada al cliente y fomentar una cultura de creatividad e innovación.
- En el foco financiero, el crecimiento de ingresos manteniendo la rentabilidad de la empresa.

3.2. La cadena de valor

La cadena de valor se muestra en el gráfico 2, allí se pueden ver todos los elementos que la componen.

Gráfico 2. La cadena de valor de SISC



Fuente: Elaboración propia, 2018.

a. Procesos misionales

Son los procesos que generan los servicios, por lo tanto, ejecutan la misión de SISC. Involucra a diferentes áreas del servicio y tienen impacto en el cliente creando valor para este. Además, suponen las actividades esenciales del servicio, su razón de ser. En ese sentido, contiene los siguientes procesos:

- Selección de personal: realiza el reclutamiento de personal mediante una exhaustiva selección.
- Entrenamiento y formación: se realizan y ejecutan planes de capacitación a corto y largo plazo según las necesidades de las líneas de negocio. Busca que el personal se mantenga en constante cambio, actualizado y a la vanguardia para soportar el servicio que se entrega.
- Ofertar servicios: propone nuevas soluciones a los clientes, producto de investigación e innovación realizada por las áreas internas. Este proceso involucra prospectar, presentar la solución, armar la propuesta comercial de servicios, exponer y plantear los beneficios, negociar y cerrar la oferta de servicio.
- Entrega del servicio: se encarga de realizar el servicio.
- Mejora continua: busca mejorar el servicio entregado al cliente. Se revisan todos los componentes que intervienen en el servicio, su desempeño y los resultados alcanzados según los acuerdos de niveles de servicio.

b. Procesos estratégicos

Proporciona las directrices a todos los demás procesos. Así, contiene actividades asociadas a las prioridades estratégicas de la empresa. Sus actividades se disponen alrededor de la mejora de la gestión y el control, definir la estrategia y asimilar y planear el cambio organizacional.

c. Procesos de apoyo

Son aquellos que mantienen la operación en correcto funcionamiento dando apoyo a los procesos fundamentales que realiza un servicio.

3.3.Líneas de negocio

SISC tiene las siguientes líneas de negocio:

- Experiencia cliente: servicios integrales de venta y posventa, gestión de cartera de deuda.
- *Facilities management*: definición de necesidades inmobiliarias hasta la adaptación y mantenimiento de las instalaciones.
- Tecnología y sistemas de negocio: desarrollo y mantenimiento de aplicaciones de negocio, implementación de proyectos y servicios de operación de infraestructura tecnológica.
- Consultoría y soluciones de negocio: diseño e implementación de mejoras a los procesos de negocio.

3.4 Relaciones con clientes y proveedores

Los servicios que entrega la empresa SISC tienen dos niveles de intermediación: uno de ellos con los clientes y otro con los proveedores. A nivel de clientes, las características del servicio comprenden lo siguiente:

- Destacar personal para trabajar en las sedes del cliente
- Acceder remotamente a los sistemas de información del cliente
- Intercambiar información vía correo electrónico o por otros medios
- Dar acceso al cliente a los sistemas de negocio de la empresa

De otro lado, los controles del cliente suelen ser los siguientes:

- Acuerdos de confidencialidad
- Accesos autorizados y registrados para acceder a sus aplicaciones
- Auditorías anuales realizados a la Gerencia de tecnología y sistemas de negocio

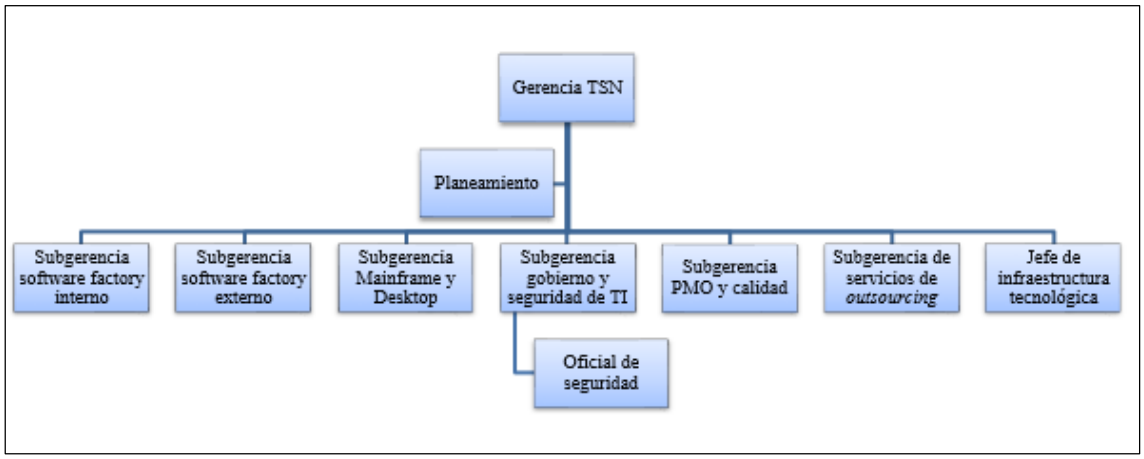
Finalmente, a nivel de proveedores, las características de la relación comprenden lo siguiente:

- Alojar a personal del proveedor en las oficinas de la empresa
- Dar acceso a los sistemas de información de la empresa a los proveedores

3.5 La seguridad de la información en la empresa

La gerencia de tecnología y sistemas de negocios está organizada como se muestra en el gráfico 3.

Gráfico 3. Organización de la gerencia de tecnología y sistemas de negocio



Fuente: Elaboración propia, 2018.

Las funciones relacionadas con la seguridad de la información se desarrollan en la empresa SISC como se indican a continuación:

- El oficial de seguridad es responsable de definir los lineamientos relacionados a la seguridad de la información.
- Los especialistas técnicos de redes y comunicaciones, dentro de sus funciones, también operan los dispositivos de seguridad perimetral.
- La operación de la solución de antivirus está tercerizada.
- La gestión de cuentas está tercerizada.

3.6 Exposición a los ciberriesgos

A efectos de delimitar la investigación, se procedió a efectuar una evaluación interna de las líneas de negocio de la empresa, para medir su nivel de exposición a los ciberriesgos. De este modo, los siguientes factores fueron evaluados:

- El uso de Internet; en qué medida el personal accede a las páginas de Internet por razones de trabajo.
- El uso de correo para comunicación externa a la empresa; en qué medida los usuarios cursan y reciben correos hacia entidades diferentes a la empresa.
- El nivel de automatización de las tareas; en qué medida el área hace uso de aplicaciones informáticas para soportar sus procesos y actividades.
- Las transacciones a través de la web; en qué medida el área usa aplicaciones en la web.

- El uso de proveedores; en qué medida el área depende de los proveedores.

Asimismo, se usó la escala de medida siguiente:

- (0), no aplica el factor.
- (1), bajo uso
- (2), uso medio
- (3), uso intensivo

Los resultados se muestran en la tabla 1.

Tabla 1. Exposición de las líneas de negocio a los ciberriesgos

Factor	**Experiencia cliente**	***Facilities Management***	**Tecnología y sistemas de negocio**	**Procesos de negocio**
Uso de Internet	1	1	3	2
Uso de correo para comunicación externa a la empresa	3	3	2	2
Nivel de automatización de las tareas (uso de aplicaciones)	3	3	1	0
Transacciones a través de la web	3	3	1	0
Uso de proveedores	2	3	2	0
Total	**12**	**13**	**9**	**4**

Fuente: Elaboración propia, 2018.

De los resultados, delimitaremos el alcance de la investigación a las líneas de negocio de Experiencia cliente y *Facilities Management*.

Capítulo IV. Metodología

1. Tipo de investigación

Por la naturaleza de la información que se va a recoger para responder al problema planteado, la presente investigación se encuentra dentro del enfoque cualitativo. Asimismo, debido a la naturaleza de sus objetivos, la presente investigación es del tipo exploratoria, porque examina un tema poco estudiado en el ámbito local y explicativa por qué se busca encontrar las causas del problema.

2. Caso de estudio

El presente trabajo adopta la forma de un caso de estudio, que es un tipo de investigación cualitativa, que es útil y apropiada porque pone a prueba modelos teóricos diversos y reduce el campo amplio de la investigación. Así, el caso de estudio consiste en una generalización analítica y no estadística porque no se trata de extraer una muestra probabilística de una población, sino está enfocada en ilustrar, representar y generalizar teorías similares. Dicho de otro modo, se enfoca en la transferibilidad de una teoría a otros casos utilizando o examinando fenómenos contemporáneos o nuevos en un entorno real de caso único o múltiple. Además, cabe señalar que el caso de estudio en el diseño del caso cualitativo ha tenido un valor resaltante en el desarrollo de disciplinas de estudio de organizaciones, pues de ellas han surgido teorías de campo empresarial donde la validez y la fiabilidad de sus resultados han sido confiables (Yin 1994).

En la presente investigación, encontramos los cinco componentes de un caso de estudio descritos por Yin (1994):

- Las preguntas de investigación, detalladas en el capítulo II, Planteamiento del problema.
- Sus objetivos, detallados en el capítulo II, Planteamiento del problema.
- La unidad de análisis: la empresa SISC.
- La determinación de cómo los datos serán alineados a los objetivos.
- Los criterios para identificar los hallazgos, los marcos de referencia y estándares descritos en el capítulo III, Marco conceptual.

3. Nivel de investigación

El grado de profundidad para el presente trabajo de investigación es el siguiente:

- La evaluación se hará a los sistemas de negocio que muestran mayor nivel de exposición a un ciberataque. Entre estos, destacan Experiencia cliente y *Facilities Management.*
- Se evaluarán únicamente los procesos de detección y respuesta descritos en el marco de ciberseguridad del NIST debido a lo siguiente:

    - Las funciones de detectar y responder combinadas posibilitan monitorear y responder proactivamente respectivamente (Dedeke 2017: 49).
    - Según la encuesta desarrollada por RSA (2015), Índice de pobreza en ciberseguridad, las organizaciones continúan enfatizando la protección sobre la detección y respuesta a pesar del hecho de que las capacidades preventivas y de protección son incapaces de detener las más grandes ciberamenazas de hoy. RSA cree que la habilidad para detectar y responder a los ciberataques, antes de que ellos resulten en daños o pérdidas, es la más importante capacidad que las organizaciones deben desarrollar y refinar.
    - Hay una necesidad real de considerar un enfoque bien equilibrado hacia la prevención y detección, además de mecanismos de respuesta (Piper 2016: 37).

- Se estima realizar la evaluación del nivel de capacidad de los procesos de detección y respuesta -indicada por el marco de ciberseguridad del NIST- únicamente en el nivel 1 de capacidad. El motivo es que, de acuerdo con el estudio de RSA, las habilidades de detección, respuesta y recuperación están aún en fase incipiente en las empresas. De allí que la investigación incidirá en encontrar qué aspectos se cumplen dentro del nivel 1 de capacidad. Si la investigación encuentra en cumplimiento dentro del nivel 1(completamente alcanzado), se procederá a evaluar el siguiente nivel de capacidad (2).

4. Diseño de la investigación

La presente investigación está catalogada como investigación no experimental; como tal, se centra en evaluar un contexto en un punto del tiempo. Para este caso, consideramos como diseño apropiado el transversal o transeccional, porque el enfoque se hará sobre la exploración de un momento específico, aplicado a un problema de investigación relativamente nuevo como

lo es la ciberseguridad. En otras palabras, tomaremos una foto de cuál es el estado de la empresa en los aspectos de la ciberseguridad, para lo cual se abarcarán varios grupos de áreas y personas, e información relacionada.

5. Consideraciones

Para efectos de alinear términos del marco de medición de capacidad con el marco de ciberseguridad del NIST, se asumirá que el término función del marco del NIST se corresponde con el término proceso que se indica en la ISO/IEC 30020 (International Standard Organization 2015). Esta asunción se respalda en el hecho de que, en el marco de ciberseguridad del NIST, cada función está asociada a un conjunto de buenas prácticas o actividades que guardan relación entre sí. Por otro lado, la definición de proceso se relaciona a un conjunto de actividades relacionadas.

Los marcos o estándares descritos en el capítulo III justifican su uso en la presente investigación debido a los siguientes motivos:

- Para desarrollar el marco de referencia y ganar un entendimiento del panorama actual de la ciberseguridad, el NIST consultó a cientos de profesionales en seguridad en la industria. Así, llevó a cabo un número de sesiones de trabajo que reunió a muchos participantes del sector privado, y recibió numerosos comentarios al borrador del marco de referencia. Más de 3.000 individuos y organizaciones contribuyeron al marco de referencia (Shen 2014:3).
- El marco fue organizado para que se adapte a las cambiantes circunstancias y entornos, de modo que sus futuras versiones se puedan crear mientras evoluciona el panorama de la ciberseguridad (Shackelford, Martell & Craig 2015: 336).
- Con relación al marco para calificar el nivel de capacidad de los procesos a evaluar, se usará un estándar internacional vigente desde el año 2003 y que ha sido actualizado el año 2015, el cual es promovido y adoptado por ISACA (2012) en su publicación COBIT 5.
- Para el análisis de riesgos, usaremos las plantillas de riesgos presentadas en el documento de COBIT 5 para riesgos.

6. Pasos por ejecutar en la investigación

Los siguientes pasos describen cómo se ejecutará la investigación.

6.1. Orientar

Se identifica, para las líneas de negocio seleccionado, los sistemas y activos relacionados, los requerimientos regulatorios y todo enfoque de riesgos. Se identifica, además, las amenazas y vulnerabilidades de estos sistemas y activos.

6.2. Identificar el nivel de capacidad actual

Se evalúa el nivel de capacidad actual, indicando qué resultados por categoría y subcategoría, de acuerdo con el marco de referencia del NIST, están siendo actualmente alcanzados.

6.3. Conducir una evaluación de riesgos

Se analiza el entorno operacional con el fin de discernir la probabilidad de un evento de ciberseguridad y el impacto que el evento puede tener en la empresa. Además, se buscará incorporar riesgos emergentes y datos de amenazas y vulnerabilidades para facilitar un robusto entendimiento de la probabilidad e impacto de los eventos de ciberseguridad.

6.4. Identificar el nivel de capacidad objetivo

Se identifica un perfil objetivo, focalizado en la evaluación de las categorías y subcategorías del marco de referencia del NIST, que describa los resultados de ciberseguridad deseados de la empresa.

6.5. Identificar brechas y desarrollar el plan de acción

Se compara el perfil actual y el perfil objetivo para determinar las brechas. A continuación, se crea un plan de acción priorizado para direccionar aquellas brechas a fin de lograr los resultados del perfil objetivo. Finalmente, se determinan los recursos necesarios para direccionar las brechas.

7. Diagrama de la metodología a ejecutar

A continuación, se muestra, en la tabla 2, qué herramientas se usarán para cada paso por ejecutar en la investigación.

Tabla 2. Esquema de herramientas versus pasos a seguir en la evaluación

Paso a seguir	¿Qué se busca?	Herramienta para usar
1.Orientar	Identificar qué sistemas y activos están involucrados.	Inventario de aplicaciones, servidores, redes, etc.
2.Identificar el perfil actual	Evaluación de capacidad de ciberseguridad.	Marco ciberseguridad del NIST, Programa de auditoría/aseguramiento del marco de ciberseguridad de ISACA y el ISO 33020.
3.Conducir una evaluación de riesgos	Evaluar los riesgos en ciberseguridad.	COBIT 5 para riesgos.
4.Identificar el perfil objetivo	Identificar el TO BE en la empresa.	Marco ciberseguridad del NIST.
5.Identifica brechas y desarrollar el plan de acción	Identificar brechas y elaborar hoja de ruta de controles a implementar.	Hoja de ruta.

Fuente: Elaboración propia, 2018.

8. Técnicas por usar

Se describen, en las fases donde se necesita capturar datos o información, qué técnicas se van a usar.

8.1.Fase orientar

En esta fase se desarrollan las siguientes técnicas:

- Captura de registros asociado a los sistemas y activos de información involucrados.
- Análisis de contenido. Se revisa la información recolectada.

8.2.Fase identificar el perfil actual

En esta fase se desarrollan las siguientes técnicas:

- Cuestionarios. La investigación se apoya en el cuestionario desarrollado por ISACA (2016), que está basado en el marco de referencia del NIST. Se aplicarán estos cuestionarios para evaluar el nivel de capacidad de los procesos.
- Entrevistas. Se tendrán entrevistas usando los cuestionarios indicados en el párrafo anterior, las cuales se desarrollarán con las siguientes personas:

    - El jefe de infraestructura tecnológica
    - El oficial de seguridad
    - Especialistas técnicos de tecnologías de la información

Las entrevistas se desarrollarán en sesiones con participación de uno o más de los indicados.

- El resultado de esta fase será presentado al Comité Gerencial de Tecnología y Sistemas de Negocio para recoger sus observaciones.

8.3. Fase conducir una evaluación de riesgos

En esta fase se desarrollan las siguientes técnicas:

- Cuestionarios. La investigación se apoya en los escenarios desarrollados por ISACA (2013) en el marco de referencia de COBIT 5 para riesgos. Se aplicarán los escenarios de riesgo relacionados a ciberseguridad.
- Una sesión de tormenta de ideas. Para identificar los riesgos relacionados con ciberseguridad, se conforma un grupo multidisciplinario conformado por las siguientes personas:

    - El jefe de infraestructura tecnológica
    - El oficial de seguridad
    - Especialistas técnicos de tecnologías de la información
    - Usuario líder de la línea de negocio evaluada

Capítulo V. Análisis de resultados y hallazgos

1. Sistemas y activos involucrados

Línea de negocio: experiencia cliente.

Tabla 3. Sistemas críticos, línea experiencia cliente

Sistema crítico	Plataforma		Publicado en		Usado por			Número de usuarios		
	Propia	Tercerizada	Intranet	Internet	Personal	Proveedor	Cliente	<50	<100	>100
Web SIAC	X			X		X				X
VCDial	X		X		X					X
Robot	X		X		X					X

Fuente: Elaboración propia, 2018.

Activos:

- Servidores
- Equipos de comunicación
- Aplicaciones de negocio críticas (Web SIAC, VCDial, Robot)
- Software base (sistema operativo, base de datos)
- Equipos de cómputo del usuario final
- Dispositivos de almacenamiento externo (USB)
- Datos

Línea de negocio: *Facilities Management.*

Tabla 4. Sistemas críticos, línea *Facilities Management*

Sistema crítico	Plataforma		Publicado en		Usado por			Número de usuarios		
	Propia	Tercerizada	Intranet	Internet	Personal	Proveedor	Cliente	<50	<100	>100
EDI	X		X	X	X	X	X			X

Fuente: Elaboración propia, 2018.

Activos:

- Servidores
- Equipos de comunicación y redes
- Aplicación de negocio crítica, EDI
- Software base (sistema operativo, base de datos)
- Equipos de cómputo del usuario final
- Dispositivos de almacenamiento externo (USB)
- Datos

2. Evaluación del nivel de capacidad en ciberseguridad

Los resultados indican que, en el nivel 1 de capacidad, los procesos de detección y el de respuesta son parcialmente logrados en la empresa evaluada, esto es, existe alguna evidencia de un enfoque en la detección, en la repuesta y algún logro de los atributos definidos en ambos procesos. A la vista de los resultados alcanzados, los procesos de detección y de respuesta no están implementados o fallan en el cumplimiento de sus propósitos. Los resultados de los procesos de detección y de respuesta se muestran en la tabla 5 y 6.

Tabla 5. Resultados de capacidad en el nivel 1 del proceso de detección

Subproceso	Descripción	Madurez subproceso	Madurez del proceso
Anomalías y eventos	La actividad anómala se detecta oportunamente y se entiende el potencial impacto de los eventos.	Parcialmente alcanzado	Parcialmente alcanzado
Monitoreo continuo de la Seguridad	Los sistemas de información y los activos se monitorean en intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	Largamente alcanzado	
Procesos de detección	Los procesos y procedimientos de detección se mantienen y prueban para asegurar la oportuna y adecuada concientización en los eventos anómalos.	Parcialmente alcanzado	

Fuente: Elaboración propia, 2018.

Tabla 6. Resultados de capacidad en el nivel 1 del proceso de respuesta

Subproceso	Descripción	Madurez subproceso	Madurez del proceso
Planear la respuesta	Los procesos y procedimientos de respuesta son ejecutados y mantenidos para asegurar la oportuna respuesta a los eventos de ciberseguridad detectados.	Largamente alcanzado	Parcialmente alcanzado
Comunicaciones	Las actividades de respuesta son coordinadas con los interesados internos y externos según corresponda.	Parcialmente alcanzado	
Análisis	El análisis es realizado para asegurar adecuada respuesta y soporte a las actividades de recuperación.	Parcialmente alcanzado	
Mitigación	Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.	Largamente alcanzado	
Mejoras	Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta.	Parcialmente alcanzado	

Fuente: Elaboración propia, 2018.

Los resultados de la evaluación llamaron la atención a la gerencia, pues los resultados de los pasados eventos de eventos de ciberseguridad no habían afectado a la empresa. Por ello, se consideraba que había suficientes controles en ciberseguridad ante un ciberataque.

3. Evaluación de los riesgos

3.1. Lista de riesgos

Los riesgos identificados con relación a la ciberseguridad se muestran en la tabla 7.

Tabla 7. Lista de riesgos

Escenario	Riesgo
Experiencia y habilidad del personal de TI.	**1. Falta de personal técnico especializado en ciberseguridad**. La organización no cuenta con especialistas técnicos suficientes y/o capacitados en seguridad de la información, lo cual ocasiona que no se revisen los eventos de seguridad.

Escenario	Riesgo
Personal de operaciones	**2. Falta de la actualización del software base.** Los administradores de las plataformas no actualizan oportunamente los sistemas operativos u otro software base cuando el fabricante libera nuevas versiones o parches. Los hackers desarrollan malware que aprovecha las vulnerabilidades en el software base.
	3. Falta de procedimientos para el tratamiento de incidentes de ciberseguridad. No se cuenta con procedimientos que delineen los roles y actividades a ejecutar cuando se produzca un evento de seguridad.
Infraestructura de TI.	**4. Infraestructura en uso obsoleta**. Existen en uso plataformas que, por su obsolescencia, no permiten actualizaciones del software base.
Software	**5. Selección e implementación de software inseguro por costo**. Por ahorros económicos, se selecciona software de bajo costo con poca garantía de seguridad.
Proveedores	**6. Incumplimiento del proveedor a los lineamientos de seguridad**. El personal del proveedor no cumple los lineamientos de seguridad establecidos en el contrato de servicio y expone a la empresa a riesgos de ciberseguridad.
Malware	**7. Intrusión de malware sobre servidores operacionales críticos**. Un malware penetra la infraestructura de TI de la empresa e infecta los servidores críticos y la información contenida en ellos.
	8. Infección de PC/ laptops con malware. Un virus penetra la infraestructura de TI de la empresa e infecta los equipos de los usuarios (pc/laptop) y la información contenida en ellos.
	9. Robo de información por un ataque de *phishing*. Método usado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta.
	10. Extorsión por un ataque de ransomware. Software malicioso que, al infectar un equipo, le da al ciberdelincuente la capacidad de bloquear el equipo y encriptar los archivos. Así toma el control de la información y datos almacenados y coacciona al usuario a pagar un rescate.

Escenario	Riesgo
	11. Infección de dispositivos móviles. Se facilita el ataque por el uso de sistemas operativos antiguos, en los dispositivos móviles.
	12. Minado malicioso de monedas criptográficas. La producción de criptomonedas precisa de una gran capacidad informática. Los ciberdelincuentes, en su intento por producir criptomonedas, siembran malware que usa el poder de procesamiento de los equipos infectados.
Ataques lógicos	**13. Ataque de denegación de servicios**. Se produce cuando una cantidad considerable de sistemas atacan a un objetivo único y provoca la denegación de servicios de los usuarios legítimos del sistema afectado.
	14. Ataque sobre las páginas web. Un servidor conectado a Internet recibe ataques continuos.
Aplicación	**15. Malas prácticas de parte de los programadores en el desarrollo de las aplicaciones**. Riesgos de seguridad por errores en la programación debido a una inexistente o insuficiente validación de los datos de entrada de las aplicaciones web que son explotados por los atacantes cibernéticos.
Ingeniería de los Medios Sociales	**16. Uso no controlado de las redes sociales**. Las redes sociales pueden convertirse en la fuente para las fugas de información. Además, con un sistema de seguridad deficiente pueden afectar seriamente a la empresa.
Dispositivos móviles	**17. Uso de dispositivos y equipos propios por el personal**. Las aplicaciones instaladas en los dispositivos móviles pueden tener configuraciones de seguridad débiles, de modo que un hacker podría aprovecharlas.
	18. Uso de medios de almacenamiento externo (USB). El usuario activa programas contenidos en el USB en su equipo de escritorio de la oficina. De este modo, puede infectarlo con programas maliciosos
	19. Uso de equipos de la empresa fuera de las instalaciones. El equipo de la empresa usado fuera de las instalaciones por largo tiempo no mantiene actualizado el antivirus, eso lo expone al ataque de nuevo malware.

Fuente: Elaboración propia, 2018.

3.2.Impacto

Los criterios de impacto adoptados han sido tomados del informe publicado por Deloitte (2016), Debajo de la superficie de un ciberataque. Esos mismos criterios se muestran en la tabla 8.

Tabla 8. Matriz de impactos

Factor de impacto de un ciberataque	Línea de negocio	
	Experiencia cliente	**Facilities Management**
Investigación técnica	Aplica	Aplica
Notificación de brechas al cliente	No aplica	No aplica
Protección al cliente post brecha	No aplica	No aplica
Cumplimiento regulatorio	Aplica	No aplica
Relaciones públicas	No aplica	No aplica
Honorarios de abogados y del litigio	Aplica	No aplica
Mejoras en ciberseguridad	Aplica	No aplica
Incremento de las primas de los seguros	No aplica	No aplica
Incremento en el costo por aumentar la deuda	No aplica	No aplica
Impacto de la interrupción o destrucción operacional.	Aplica	Aplica
Pérdida de valor de las relaciones con el cliente	Aplica	Aplica
Valor de los ingresos perdidos en contratos	Aplica	Aplica
Devaluación del nombre comercial de la marca SISC.	Aplica	Aplica
Pérdida de la propiedad intelectual	No aplica	No aplica

Elaboración: Deloitte, 2016.

En la tabla 9, se muestran los rangos de impacto por cada impacto que aplica para las líneas de negocio a evaluar.

Tabla 9. Cuadro de rango de impactos

Factor impacto de un ciberataque	Rango de impacto				
	Insignificante (1)	**Menor (2)**	**Moderada (3)**	**Mayor (4)**	**Grave (5)**
A. Investigación técnica	No precisa de investigación.	Precisa de una revisión técnica de baja complejidad.	Precisa de una revisión técnica que involucra varias especialidades.	Precisa de una revisión técnica especializada con apoyo externo.	Precisa una amplia y compleja escala de investigación forense.
B. Cumplimiento regulatorio	El cumplimiento regulatorio es afectado de manera insignificante.	Infracción menor al cumplimiento	Los entes reguladores y legales solicitan información.	Los entes reguladores y legales aplican multas.	Los entes reguladores y legales aplican acciones legales.
C. Honorarios de abogados y del litigio	No se precisa de honoraros de abogados.	Solo precisa de consultas a los abogados.	Se precisa de una acción más activa de los abogados.	Se puede llegar a un acuerdo sin ir a juicio.	Hay necesidad de ir a un juicio.
D. Mejoras en ciberseguridad	No se precisa de cambios en la infraestructura o controles.	Precisa de pequeños cambios.	Precisa de medianos cambios.	Precisa de muchos cambios.	Se precisa de grandes cambios en la infraestructura y controles.
E. Impacto de la interrupción o destrucción operacional	T < 1 hora	1 hora < T < 2 horas	2 horas < T < 4 horas	4 horas < T < 1 día	T > 1 día
F. Pérdida de valor de las relaciones con el cliente	Relaciones afectadas de manera insignificante	Relaciones levemente afectadas	Relaciones medianamente afectadas.	Relaciones afectadas seriamente	Relaciones pérdidas con el cliente
G. Valor de los ingresos perdidos en contratos	Reducción ingresos del contrato < 5%	Reducción ingresos del contrato < 10%.	Reducción ingresos del contrato < 25%	Reducción ingresos del contrato < 100%	El contrato se cancela o no se renueva.
H. Devaluación del nombre comercial de la marca SISC.	Marca afectada de manera insignificante	Marca afectada de manera leve	Marca afectada medianamente	Marca afectada seriamente	Marca afectada enormemente

Fuente: Elaboración propia, 2018.

3.3.Probabilidad

Los valores de probabilidad a aplicar en la evaluación de riesgos se muestran en la tabla 10.

Tabla 10. Matriz de probabilidades

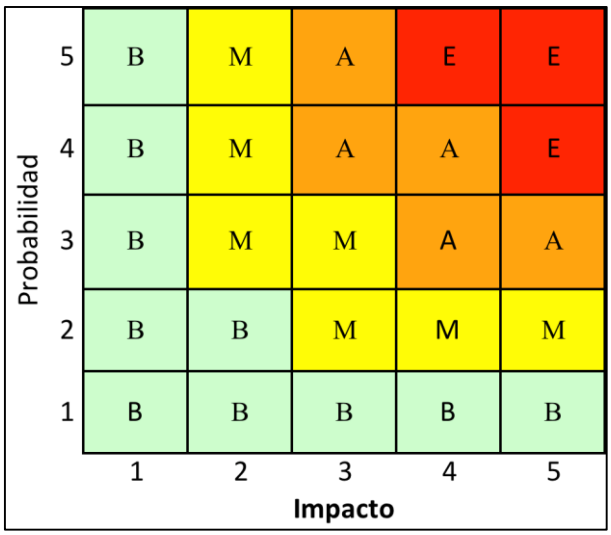
Rango probabilidad	Frecuencia	Probabilidad matemática	Valor
Rara	1 vez al año	< 10%	1
Improbable	1 vez cada 6 meses	10.1% - 20%	2
Moderada	1 vez cada trimestre	20.1% - 50%	3
Probable	1 vez cada bimestre	50.1% - 90%	4
Casi certeza	1 vez cada mes	> 90%	5

Fuente: Elaboración propia, 2018.

3.4.Matriz de severidad

De la combinación de impacto y probabilidad, se obtiene la matriz de severidad.

Gráfico 4. Matriz de severidad



Fuente: Elaboración propia, 2018.

E: extremo; A: alto; M: moderado; B: bajo

3.5.Análisis de riesgos

A continuación, se muestra los cuadros de resultados de severidad de los riesgos, para la línea de Experiencia Cliente y Facilities Management, en las tablas 11 y 12 respectivamente.

Tabla 11. Análisis de riesgos, Experiencia cliente

Categoría del riesgo	Riesgo	Impacto (*)								Prob.	Severidad
		A	B	C	D	E	F	G	H		
Experiencia y habilidad del personal de TI	1. Falta de personal técnico especializado en ciberseguridad					3				4	12
Personal de operaciones	2. Falta de la actualización del software base					4	4	4	4	4	16
	3. Falta de procedimientos para el tratamiento de incidentes de ciberseguridad					4				3	12
Infraestructura de TI	4.Infraestructura en uso obsoleta					4	4	4	4	4	16
Software	5. Selección e implementación de software inseguro por costo					4	3			4	16
Proveedores	6. Incumplimiento del proveedor a los lineamientos de seguridad					3				3	9
Malware	7. Intrusión de malware sobre servidores operacionales críticos	4	3	3	5	5	4	4	4	4	20
	8. Infección de laptops con malware	2	2	1	2	3	1	2	1	3	9
	9. Robo de información por un ataque de *phishing*	3	4	3	3	1	3	4	4	3	12
	10. Extorsión por un ataque de ransomware	5	4	3	4	5	4	3	4	3	15
	11. Infección de dispositivos móviles	2	2	2	3	3	2	1	2	4	12
	12. Minado malicioso de monedas criptográficas	2		2	2	3				2	6
Ataques lógicos	13. Ataque de denegación de servicios	4			3	4	2	2		3	12
	14. Ataque sobre las páginas web	3			4	4	3	2	3	4	16
Aplicación	15. Malas prácticas de parte de los programadores en el desarrollo de las aplicaciones				4	4		3		4	16
Ingeniería de los medios sociales	16. Uso no controlado de las redes sociales		3	3		4	4			2	8
Dispositivos móviles	17. Uso de dispositivos y equipos propios por el personal		2			4				1	4
	18. Uso de medios de almacenamiento externo (USB)					3				4	12
	19. Uso de equipos de la empresa fuera de las instalaciones					4				1	4

Fuente: Elaboración propia, 2018.

Tabla 12. Análisis de riesgos, *Facilities Management*

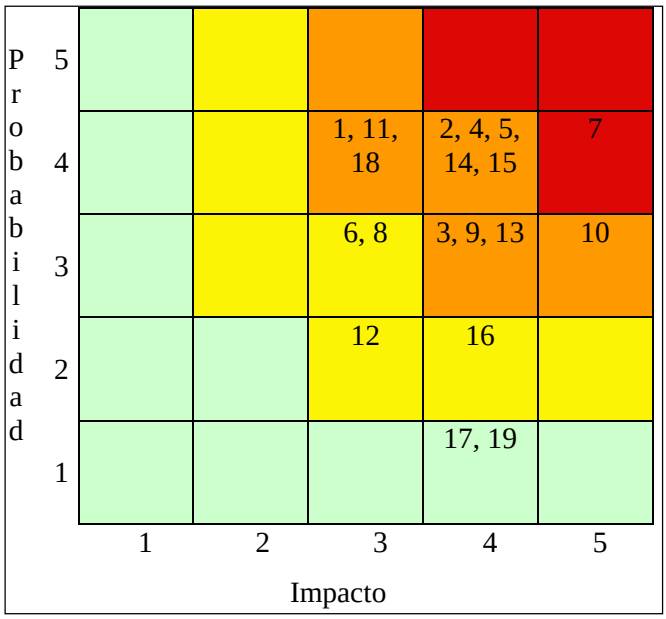
Categorías del riesgo	Riesgo	Impacto (*)					Prob.	Severidad
		A	E	F	G	H		
Experiencia y habilidad del personal de TI	1. Falta de personal técnico especializado en ciberseguridad		3				4	12
Personal de operaciones	2. Falta de la actualización del software base		4	4	4	4	2	8
	3. Falta de procedimientos para el tratamiento de incidentes de ciberseguridad		4				3	12
Infraestructura de TI	4. Infraestructura en uso obsoleta		4	4	4	4	2	8
Software	5. Selección e implementación de software inseguro por costo		4	3			2	8
Proveedores	6. Incumplimiento del proveedor a los lineamientos de seguridad		3				3	9
Malware	7. Intrusión de malware sobre servidores operacionales críticos	4	5	4	4	4	3	15
	8. Infección de laptops con malware	2	3	1	2	1	3	9
	9.Robo de información por un ataque de *phishing*	2	1	2	2	2	3	6
	10. Extorsión por un ataque de ransomware	5	5	4	3	4	2	10
	11. Infección de dispositivos móviles	2	3	2	1	2	3	9
	12. Minado malicioso de monedas criptográficas	2	3				2	6
Ataques lógicos	13. Ataque de denegación de servicios	4	4	2	2		2	8
	14. Ataque sobre las páginas web	3	4	3	2	3	2	8
Aplicación	15. Malas prácticas de parte de los programadores en el desarrollo de las aplicaciones		4		3		2	8
Ingeniería de los medios sociales	16. Uso no controlado de las redes sociales		4	4			1	4
Dispositivos móviles	17. Uso de dispositivos y equipos propios por el personal		4				1	4
	18. Uso de medios de almacenamiento externo (USB)		3				4	12
	19. Uso de equipos de la empresa fuera de las instalaciones		4				1	4

(*) Ver la tabla 9, columna factor impacto de un ciberataque.

Fuente: Elaboración propia, 2018.

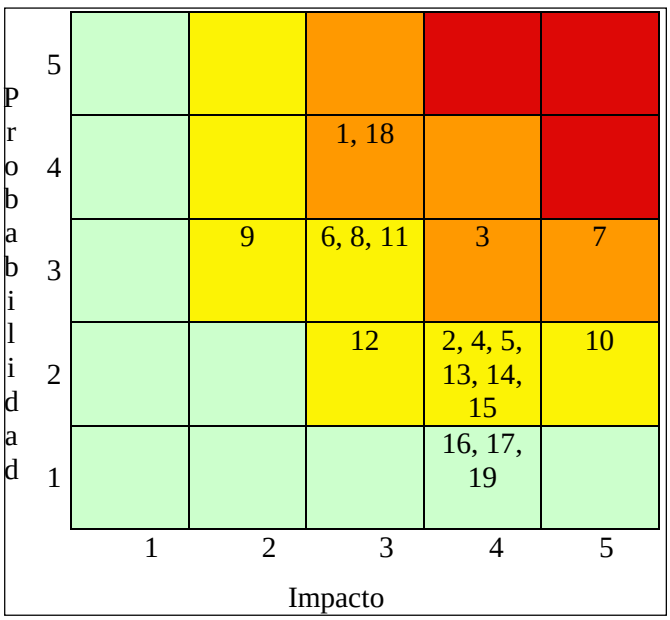
En los gráficos 5 y 6, se muestra cómo están agrupados los riesgos de acuerdo con su severidad para las líneas de Experiencia cliente y Facilities Management.

Gráfico 5. Severidad riesgos, Experiencia cliente



Fuente: Elaboración propia, 2018.

Gráfico 6. Severidad riesgos, *Facilities Management*



Fuente: Elaboración propia, 2018.

3.6. Comentarios de la gerencia

- Es importante realizar una gestión de los riesgos de ciberseguridad para seguir su evolución en el futuro.
- Los gestores de las líneas de negocio deben involucrarse en la gestión de riesgos de ciberseguridad y tratarla con la línea de negocio respectiva periódicamente.

4. Nivel de capacidad objetivo

El perfil objetivo de los procesos materia de la presente investigación, dentro del nivel 1 de capacidad, se muestra en la tabla 13.

Tabla 13. Perfil objetivo de los procesos de detección y respuesta

Proceso	Subproceso	Nivel actual (1)	Nivel objetivo (1)
Detección	Anomalías y eventos	Parcialmente alcanzado	Completamente alcanzado
	Monitoreo continuo de la seguridad	Largamente alcanzado	Completamente alcanzado
	Procesos de detección	Parcialmente alcanzado	Completamente alcanzado
Respuesta	Planear la respuesta	Largamente alcanzado	Completamente alcanzado
	Comunicaciones	Parcialmente alcanzado	Completamente alcanzado
	Análisis	Parcialmente alcanzado	Completamente alcanzado
	Mitigación	Largamente alcanzado	Completamente alcanzado
	Mejoras	Parcialmente alcanzado	Completamente alcanzado

Fuente: Elaboración propia, 2018.

El nivel de capacidad objetivo propuesto busca los siguientes objetivos:

- La empresa SISC pueda identificar oportunamente la ocurrencia de los eventos de ciberseguridad.
- La empresa SISC pueda tomar acciones apropiadas y planificadas con relación a los incidentes de ciberseguridad detectados.

5. Brechas identificadas y plan de acción

5.1.Brechas

5.1.1. Proceso detectar

Las brechas identificadas en relación al nivel objetivo definido (tabla 13) se describen a continuación:

Subproceso: anomalías y eventos.
Objetivo de control: la actividad anómala se detecta y se entiende el potencial impacto de los eventos.

Tabla 14. Brechas subproceso anomalías y eventos

Control	Brecha
Los eventos detectados son analizados para entender los objetivos y métodos de ataque.	No se cuenta con un procedimiento para el monitoreo de eventos anómalos en la red y en los sistemas gestionados por los dispositivos de seguridad.
	No se ejecuta el análisis de los eventos anómalos detectados.
Los impactos de los eventos son determinados.	No se evalúa el impacto de los eventos anómalos detectados.
Los umbrales de alerta a los incidentes están establecidos.	No existe un procedimiento formal para escalar los eventos detectados, ni se han definido los umbrales para activar las apropiadas respuestas.

Fuente: Elaboración propia, 2018.

Subproceso: monitoreo continuo de la seguridad.
Objetivo de control: los sistemas de información y los activos se monitorean para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.

Tabla 15. Brechas subproceso monitoreo continuo de la seguridad

Control	Brecha
La red es monitoreada para detectar potenciales eventos de ciberseguridad.	No se monitorea a nivel de aplicaciones publicadas en Internet.
Se monitorea la actividad de los proveedores de servicios externos para detectar potenciales eventos de ciberseguridad.	Los contratos con los proveedores no contemplan los controles necesarios para salvaguardar los riesgos en ciberseguridad.
El escaneo de vulnerabilidades es ejecutado.	Se ejecuta el escaneo de vulnerabilidades de una manera ocasional no como una práctica común.

Fuente: Elaboración propia, 2018.

Subproceso: procesos de detección.

Objetivo de control: los procesos y procedimientos de detección se mantienen y prueban para asegurar la concientización en los eventos anómalos.

Tabla 16. Brechas subproceso procesos de detección

Control	Brecha
Los roles y responsabilidades para la detección están bien definidos para asegurar la rendición de cuentas.	Las responsabilidades clave o posiciones específicas para la detección se han definido informalmente y ocasionalmente se cumplen.
La detección de actividades cumple con todos los requerimientos aplicables.	No se han documentado los requerimientos y regulaciones de seguridad que aplican en la organización.
Los procesos de detección son probados.	El proceso de detección no se prueba.
La información de la detección de eventos se comunica a las partes apropiadas.	Los eventos detectados se comunican ocasionalmente en las reuniones de gerencia.
Los procesos de detección se mejoran continuamente.	Existe evidencia ocasional de lecciones aprendidas y acciones para prevenir incidentes en el futuro.

Fuente: Elaboración propia, 2018.

5.1.2. Proceso responder

Subproceso: planear la respuesta.

Objetivos de control: los procesos y procedimientos de respuesta son ejecutados y mantenidos para asegurar la respuesta a los incidentes de ciberseguridad detectados.

Tabla 17. Brechas subproceso planear la respuesta

Control	Brecha
El plan de respuesta es ejecutado durante o después de un incidente.	No existen procedimientos formales de respuesta para los incidentes de ciberseguridad.

Fuente: Elaboración propia, 2018.

Subproceso: comunicaciones.

Objetivos de control: las actividades de respuesta son coordinadas con los interesados internos y externos.

Tabla 18. Brechas subproceso comunicaciones

Control	Brecha
El personal conoce sus roles y orden de operaciones cuando una respuesta es necesaria.	Los roles y responsabilidades no están formalmente definidos, para responder a los incidentes de ciberseguridad.
Los incidentes son reportados consistentemente con criterios establecidos.	Los reportes y canales de comunicación para los incidentes de están vagamente definidos.
	Los empleados están parcialmente entrenados para reportar los sospechosos incidentes de ciberseguridad.
La coordinación con los interesados ocurre consistentemente con planes de respuesta.	No existe un procedimiento formal para la comunicación con los interesados internos y externos durante y a continuación de un incidente de ciberseguridad.

Fuente: Elaboración propia, 2018.

Subproceso: análisis.

Objetivos de control: el análisis es realizado para asegurar efectiva respuesta y soporte a las actividades de recuperación.

Tabla 19. Brechas subproceso análisis

Control	Brecha
Las notificaciones de los sistemas de detección son investigados.	Las notificaciones de los sistemas de detección implementados no se investigan como una práctica común.
El impacto de los incidentes es entendido.	No se analizan y clasifican los incidentes en base a su potencial impacto.
Análisis forense son ejecutados.	No hay un proceso para ejecutar el análisis forense cuando se necesite.
Los incidentes son categorizados consistentemente con los planes de respuesta.	No se ha incluido la priorización de los incidentes que posibilite una rápida respuesta para incidentes o vulnerabilidades significativas.
Los procesos son establecidos para recibir, analizar y responder a las vulnerabilidades divulgadas desde fuentes internas y externas.	El procedimiento de gestión de incidentes no describe la recepción, análisis y respuesta a las vulnerabilidades divulgadas por fuentes internas o externas.

Fuente: Elaboración propia, 2018.

Subproceso: mitigación.

Objetivos de control: se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y resolver el incidente.

Tabla 20. Brechas subproceso mitigación

Control	Brecha
Los incidentes son mitigados.	No existe una estrategia para tratar con diferentes tipos de incidentes de ciberseguridad.
Las vulnerabilidades identificadas recientemente son mitigadas o documentadas como riesgos aceptados.	No se cuenta con una entidad externa, que nos informe permanentemente sobre amenazas y vulnerabilidades del entorno.

Fuente: Elaboración propia, 2018.

Subproceso: mejoras.

Objetivos de control: las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta.

Tabla 21. Brechas subproceso mejoras

Control	Brecha
Los planes de respuesta incorporan lecciones aprendidas.	Los resultados de los incidentes reales no han sido usados para actualizar los procedimientos de respuesta a incidentes de ciberseguridad.

Fuente: Elaboración propia, 2018.

5.2.Plan de acción

5.2.1. Controles recomendados

Los controles a recomendar se pueden clasificar en 3 áreas: proceso, técnico y personal.

- Proceso: define un control del tipo plan, procedimiento o actividad a desarrollar e implementar.
- Técnico: define un control de tipo tecnológico.
- Personal: define un control a aplicar sobre los individuos que componen la organización.

Los controles recomendados han sido extraídos de los documentos publicados por el Center for Internet Security (2018), CIS Controls; ISACA (2012), Cobit 5 Procesos Catalizadores; International Standard Organization (2012), NTP-ISO/IEC 27001, Sistemas de gestión de seguridad de la información; y el NIST (2018), Framework for Improving Critical Infraestructure Cybersecurity.

Los controles recomendados que permitirán que los procesos de detección y respuesta logren los niveles objetivo descritos en la tabla 13 se describen en la tabla 22. Esta última se asocia con el área y la fuente en la cual se podrá encontrar mayor información para su implementación.

Tabla 22. Controles recomendados

Ítem	Control	Área	Proceso NIST	Fuente
1	Desarrollar e implementar un procedimiento para la detección de los eventos anómalos. Debe comprender el análisis, evaluación de impacto y umbrales de alerta a los incidentes para el escalamiento; además, debe describir los roles y responsabilidades de manera que aseguren la rendición de cuentas.	Proceso	DAE / DPD	NIST 1.1
2	Desplegar un gestor de eventos y seguridad de la información (SIEM) o una herramienta analítica de registros propia.	Proceso	DAE	CIS 6.6
3	Incorporar cláusulas en los contratos con los proveedores de servicio con el propósito de a) notificar a la organización tan pronto como sea posible de cualquier evento de ciberseguridad sospechoso o conocido, y b) implementar los controles de seguridad equivalentes a o que excedan el nivel de seguridad requerido de la empresa.	Proceso	DMC	Cobit 5, APO07.06
4	Establecer un programa anual de pruebas de hackeo ético para detectar vulnerabilidades.	Proceso/ técnico	DMC	CIS 20.1
5	Desplegar el firewall de aplicaciones web para monitorear todo el tráfico que fluye a las aplicaciones publicadas en la Internet.	Técnico	DMC / Riesgo	CIS 18.10
6	Establecer la mejora continua en el proceso de detección.	Proceso	DPD	NIST 1.1
7	Documentar el apetito de riesgo de la empresa a los riesgos en ciberseguridad.	Proceso	DPD	NIST 1.1
8	Identificar y documentar todos los requerimientos contractuales, regulatorios y legales que son necesarios considerar para la detección de los eventos de ciberseguridad.	Proceso	DPD	ISO 27001, control A18.1.1
9	Establecer un programa de pruebas para asegurar que las actividades de detección cumplen con el procedimiento establecido.	Proceso	DPD	NIST 1.1
10	Establecer canales apropiados para el reporte de los eventos de ciberseguridad por los empleados de la empresa.	Proceso	DPD	ISO 27001, control A16.1.2
11	Informar mensualmente a la gerencia los eventos anómalos detectados.	Proceso	DPD	NIST 1.1

Ítem	Control	Área	Proceso NIST	Fuente
12	Establecer mecanismos para aprovechar el conocimiento obtenido de los incidentes de ciberseguridad. Así, se busca reducir la probabilidad e impacto de futuros incidentes.	Proceso	DPD / RMe	ISO 27001, control A16.1.6
13	Desarrollar e implementar el plan de continuidad del negocio.	Proceso	RPR	Cobit 5, DSS04.03
14	Documentar el procedimiento de respuesta a los incidentes de ciberseguridad. La idea es que los incidentes se categoricen, se evalúe su impacto y se priorice su atención. Asimismo, asignar los roles y responsabilidades para la respuesta a los incidentes.	Proceso	RPR / RM / RA / RC	CIS 19.1, CIS 19.2, CIS 19.8
15	Publicar información relacionada con la notificación de anomalías e incidentes de ciberseguridad.	Proceso	RC	CIS 19.6
16	Incluir los mecanismos de escalamiento jerárquico a los incidentes de ciberseguridad.	Proceso	RC	NIST 1.1
17	Diseñar estándares de uso en toda la organización para el reporte de los incidentes de ciberseguridad. Mantener información de contactos para reportar los incidentes de seguridad.	Proceso	RC / RM	CIS 19.4, CIS 19.5CIS 19.5
18	Implementar un programa anual de concientización en ciberseguridad.	Persona	RC / Riesgo	CIS 17.3
19	Desarrollar y aplicar un procedimiento para identificar, colectar, adquirir y preservar la información que pueda servir como evidencia en un análisis forense de ciberseguridad.	Proceso	RA	ISO 27001, control A16.1.7
20	Investigar las notificaciones de los mecanismos de detección; se debe llevar un control de su realización.	Proceso	RA	NIST 1.1
21	Establecer en el procedimiento, la recepción, análisis y respuesta a las vulnerabilidades divulgadas por fuentes internas y externas.	Proceso	RA/RM	NIST 1.1
22	Regularmente comparar los resultados de escaneos de vulnerabilidades seguidas para verificar que las vulnerabilidades han sido remediadas oportunamente.	Proceso	RM	CIS 3.6
23	Desarrollar estrategias para tratar con diferentes tipos de incidentes de ciberseguridad.	Proceso	RM	NIST 1.1
24	Planear y conducir ejercicios de respuesta a los incidentes para el personal involucrado en la respuesta a los incidentes.	Proceso	Re	CIS 19.7

Ítem	Control	Área	Proceso NIST	Fuente
25	Establecer prácticas de código seguro apropiadas al lenguaje de programación y a los entornos de desarrollo a ser usados.	Técnico	Riesgo	CIS 18.1
26	Priorizar las remediaciones a las vulnerabilidades descubiertas mediante la puntuación de los riesgos asociados.	Proceso	Riesgo	CIS 3.7

Fuente: Elaboración propia, 2018.

Los controles mostrados en la tabla 22, se muestran cuantificados por proceso y subproceso en la tabla 23.

Tabla 23. Controles por proceso y subproceso

Proceso NIST	Subproceso NIST	Control							
Detección	Anomalías y eventos	1	2						
	Monitoreo continuo de la seguridad	3	4	5					
	Procesos de detección	1	6	7	8	9	10	11	12
Respuesta	Planear la respuesta	13	14						
	Comunicaciones	14	15	16	17	18			
	Análisis	14	19	20	21				
	Mitigación	14	17	21	22	23			
	Mejoras	12	24						
Riesgos		5	18	25	26				

Fuente: Elaboración propia, 2018.

En la tabla 24, se presentan los controles propuestos asociados con los riesgos identificados a los que están direccionados. En esta tabla, se han marcado en color verde los riesgos qu se mitigarian, de amarillo los riesgos que parcialmente se mitigarían y en rojo los riesgos que no se mitigarían. Con relación a los riesgos que parcialmente se mitigarían, se especifica lo siguiente:

- Falta de personal técnico especializado en ciberseguridad. En una etapa posterior debe evaluarse la incorporación de un especialista técnico en ciberseguridad.
- Falta de la actualización del software base. Debe revisarse el proceso operativo de protección a efectos de verificar la efectividad del control para actualizar el software base.
- Selección e implementación de software inseguro por costo. Los controles propuestos deben evidenciar las falencias en el software y un control posterior debe asegurar que se tomen las acciones correctivas.

Tabla 24. Controles relacionados a los riesgos identificados

Ítem	Control	Riesgos																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Desarrollar e implementar un procedimiento para detectar los eventos anómalos.			X			X	X	X	X	X	X	X	X	X		X		X	X
2	Desplegar un gestor de eventos y seguridad de la información (SIEM) propio.	X		X			X	X	X	X	X	X	X	X	X		X		X	
3	Incorporar cláusulas en los contratos con los proveedores de servicio.						X													
4	Establecer un programa anual de pruebas de hackeo ético.	X	X			X										X				
5	Desplegar el firewall de aplicaciones web.	X													X	X				
6	Establecer la mejora continua en el proceso de detección.			X				X	X	X	X	X	X	X	X		X		X	X
7	Documentar el apetito de riesgo de la empresa a los riesgos en ciberseguridad.			X																
8	Identificar y documentar todos los requerimientos contractuales, regulatorios y legales necesarios a considerar para la detección de los eventos de ciberseguridad.			X																
9	Establecer un programa de pruebas para asegurar que la detección cumple el procedimiento establecido.			X				X	X	X	X	X	X	X	X				X	
10	Establecer canales apropiados para el reporte de los eventos de ciberseguridad.			X																
11	Informar mensualmente a la gerencia los eventos anómalos detectados.			X																
12	Establecer mecanismos para aprovechar el conocimiento obtenido de los incidentes de ciberseguridad. Así, se busca reducir la probabilidad e impacto de futuros incidentes.			X																
13	Desarrollar e implementar el plan de continuidad del negocio.			X																
14	Documentar el procedimiento de respuesta a los incidentes de ciberseguridad.			X				X	X	X	X	X	X	X	X				X	
15	Publicar información sobre la notificación de anomalías e incidentes.			X				X	X	X	X	X	X	X	X				X	
16	Incluir mecanismos de escalamiento jerárquico a los incidentes de ciberseguridad.			X				X	X	X	X	X	X	X	X				X	

Ítem	Control	Riesgos																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
17	Diseñar estándares de uso en toda la organización para el reporte de los incidentes de ciberseguridad. Mantener información de contactos para reportar los incidentes.			X				X	X	X	X	X	X	X	X				X	X
18	Implementar un programa anual de concientización en ciberseguridad.			X			X	X	X	X	X	X	X	X	X			X	X	X
19	Desarrollar y aplicar un procedimiento para identificar, colectar, adquirir y preservar la información que pueda servir como evidencia en un análisis forense.			X																
20	Investigar las notificaciones de los mecanismos de detección; se debe llevar un control de su realización.			X																
21	Establecer en el procedimiento, la recepción, análisis y respuesta a las vulnerabilidades divulgadas por fuentes internas y externas.			X				X	X	X	X	X	X	X	X				X	
22	Regularmente comparar los resultados de escaneos de vulnerabilidades seguidos para verificar que las vulnerabilidades han sido remediadas oportunamente.		X			X										X				
23	Desarrollar estrategias para tratar con diferentes tipos de incidentes de ciberseguridad.			X				X	X	X	X	X	X	X	X	X	X	X	X	X
24	Planear y conducir ejercicios de respuesta a los incidentes para el personal involucrado en la respuesta.			X																
25	Establecer prácticas de código seguro apropiadas al lenguaje de programación.														X	X				
26	Priorizar las remediaciones a las vulnerabilidades descubiertas con la puntuación de los riesgos asociados.			X																

Fuente: Elaboración propia, 2018.

Riesgo a mitigar

Riesgo a mitigar parcialmente

Riesgo a no mitigar

5.2.2. Hoja de ruta

- **Pasos previos**

Antes de iniciar la hoja de ruta de implementación, la organización debe organizar un equipo de proyecto que lleve a cabo la implementación de los controles que se proponen. Así, dados los recursos actuales, se propone incrementar un recurso adicional especializado en seguridad de la información para poder reforzar el equipo actual y llevar a cabo la implementación de los controles propuestos.

A continuación, en la tabla 25, se muestra una matriz RACI, que define las responsabilidades por asumir en el proyecto de implementación y mejora de los controles propuestos.

Tabla 25. Matriz RACI de implementación

Actividad	Gerencia	Oficial de seguridad	Especialista de seguridad (nuevo)	Especialistas técnicos	Proveedores
Desarrollo de los procesos y procedimientos.	I	A	R	C	I
Implementación de los procesos	I	A	R	R	R
Implementación de soluciones tecnológicas	I	A	R	R	R
Plan de concientización	C/I	A	R		
Plan de continuidad	C/I	A	R	R	R

Fuente: Elaboración propia, 2018

Donde:

R = ejecutor en la actividad.

A= responsable de la actividad.

C = consultado.

I = informado.

Los controles propuestos, serán implementados en 3 fases, que se detallan a continuación:

- **Fase 1**

Los controles a implementar tienen por finalidad fortalecer el proceso de detección, a efectos de que este proceso cumpla su propósito. Por ello, en la primera etapa, se determinarán cuáles son los requerimientos contractuales, regulatorios y legales que la empresa SISC debe cumplir.

Todo esto, sumado al apetito de riesgo que la empresa está dispuesta a asumir, servirá para el desarrollo formal e implementación del procedimiento de detección. En esta etapa, además, se buscará incrementar las capacidades de la empresa para detectar los eventos de ciberseguridad. Adicionalmente, se considera desarrollar e implementar un programa de concientización en ciberseguridad que aborde de manera permanente la formación a los empleados.

- **Fase 2**

Se evaluará el cumplimiento del procedimiento de detección y se desarrollará e implementará el procedimiento de respuesta a incidentes de ciberseguridad. Asimismo, se enfatizará en adoptar medios para la comunicación de incidentes.

- **Fase 3**

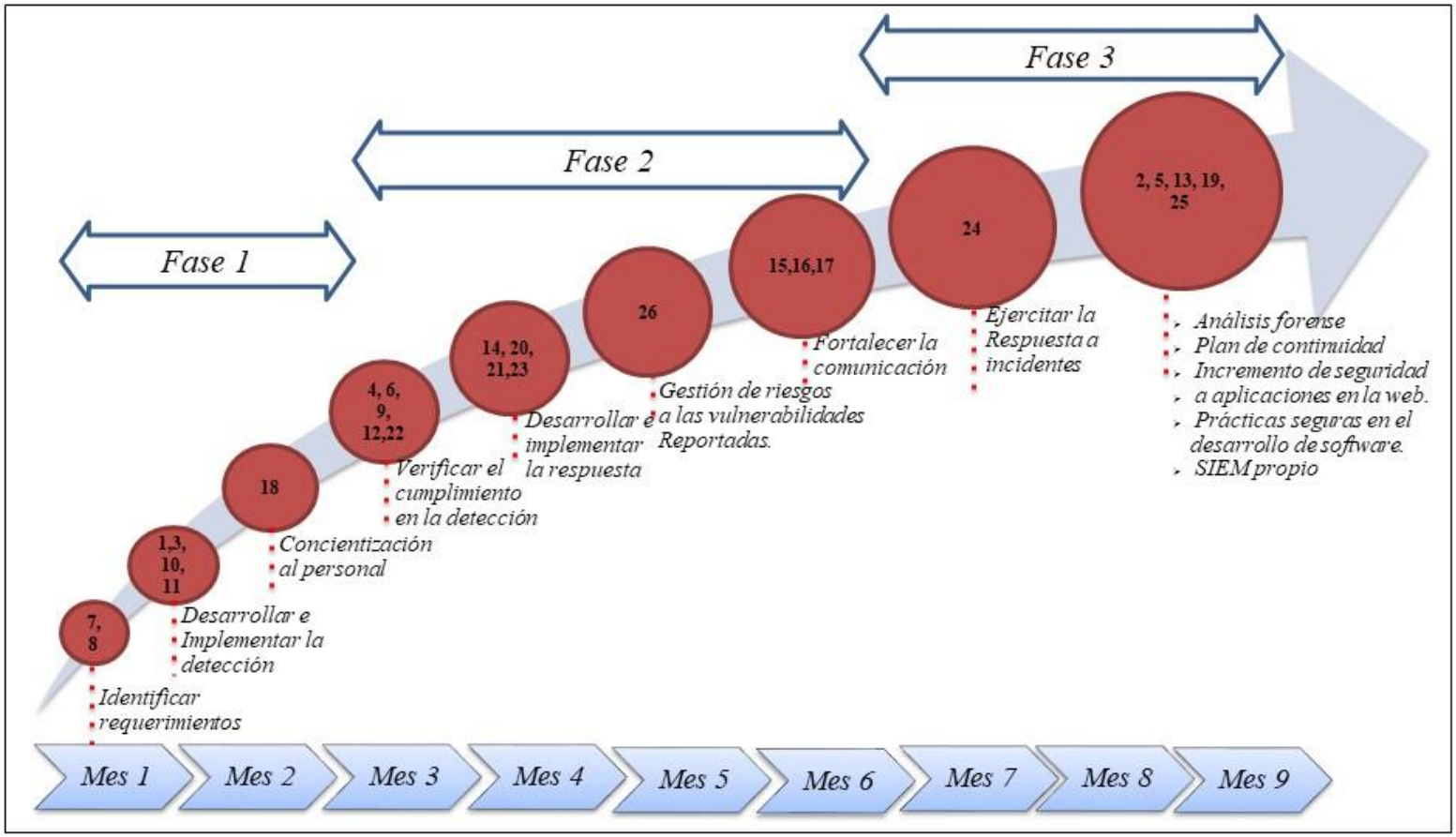
Se fortalece el proceso de respuesta implementando los ejercicios de respuesta a los incidentes con el personal involucrado. Asimismo, se desarrollará e implementará el plan de continuidad del negocio. También, se desarrollará e implementará el proceso de análisis forense para ciberseguridad. Finalmente, para reforzar aún más el proceso de detección, se propone que se adquiera e implemente usa solución de firewall para aplicaciones web.

Los períodos de implementación propuestos son los siguientes:

- Fase 1: dos meses (mes 1 al mes 2).
- Fase 2: cuatro meses (mes 3 al mes 6).
- Fase 3: tres meses (mes 7 al mes 9).

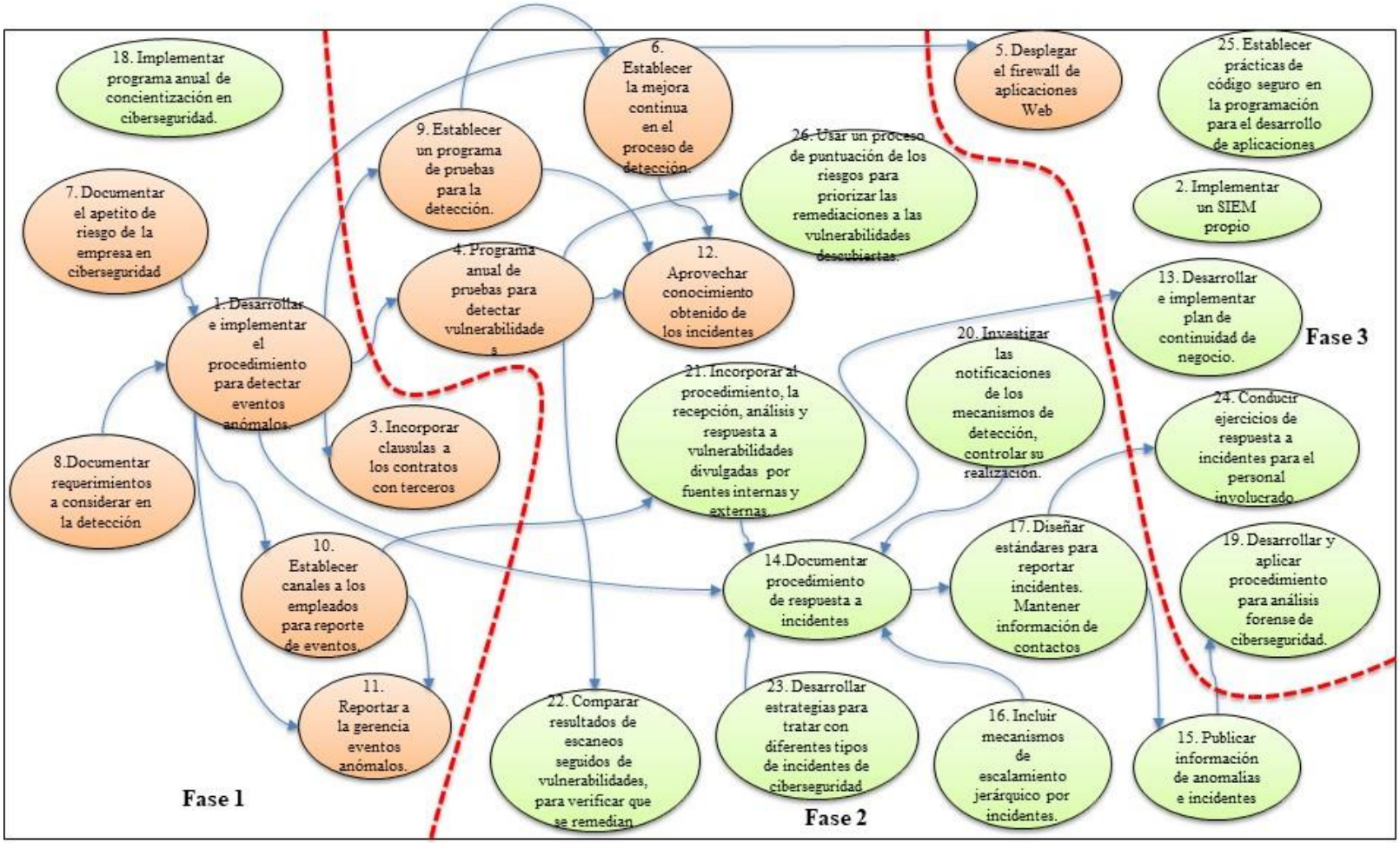
Las fases son consecutivas entre sí, esto significa que la propuesta es estimada para ser desarrollada en 9 meses. En el gráfico 7, se muestra la hoja de ruta, también, de manera resumida, los controles agrupados por cada fase y en el período de tiempo de implementación propuesto. Para un mayor nivel de detalle, observar el gráfico 8, en el que se muestran los controles propuestos y su relación en cada fase. Los controles resaltados en naranja corresponden al proceso de detectar y los resaltados en color verde corresponden al proceso de responder.

Gráfico 7. Hoja de ruta de implementación



Fuente: Elaboración propia, 2018.

Gráfico 8. Hoja de ruta de implementación detallada



Fuente: Elaboración propia, 2018.

Conclusiones

El presente trabajo de investigación servirá para que las empresas centradas en implementar soluciones tecnológicas como protección a ciberataques puedan desarrollar un enfoque de procesos que le permita mejorar sus capacidades para detectar y responder a eventos de ciberataques. Así, en el contexto de la empresa evaluada, este trabajo ha servido para que la gerencia mejore su nivel de entendimiento con respecto a los aspectos de ciberseguridad, que conozca a qué tipos de riesgo está expuesto, y que adopte una gestión en los riesgos de ciberseguridad.

Para ejecutar la planificación de la evaluación de capacidad en la gestión de la ciberseguridad, se debe considerar un marco de referencia en los procesos de ciberseguridad que sea aceptado como un importante referente en el tema. Además, se debe considerar un marco de medición que sea adecuado para medir la capacidad de los procesos. Del estudio realizado, podemos concluir que la versión 1.1 del Marco de referencia para la mejora de la infraestructura crítica en ciberseguridad, del National Institute of Standards and Technology (NIST 2018), es un modelo referente útil y válido, que se puede usar para realizar una evaluación de capacidad de los procesos de ciberseguridad en una empresa

Los principales riesgos de ciberseguridad encontrados en la empresa SISC son la intrusión de malware sobre los servidores operacionales críticos de la empresa, la falta de procedimientos para el tratamiento de incidentes de ciberseguridad, la falta de personal técnico especializado en ciberseguridad y el uso de medios de almacenamiento externo (USB).

Los resultados de la evaluación de capacidad realizada a los procesos de detección y de respuesta en ciberseguridad, en el nivel 1 (proceso ejecutado) de capacidad, nos revelan que ambos procesos en la empresa evaluada alcanzan su propósito parcialmente. Por ello, se encuentran en el nivel 0 de capacidad (proceso incompleto). Este resultado confirma que el enfoque actual de protegerse a través de la gestión técnica de herramientas de seguridad no es suficiente para detectar y responder a posibles incidentes de ciberseguridad. Así, el nivel de capacidad de ciberseguridad relacionado con los procesos de detección y de respuesta que la empresa SISC debe alcanzar -de acuerdo con el marco de referencia de ciberseguridad del NIST- es el nivel de proceso ejecutado (nivel 1). Por esto, deberá cumplir completamente los atributos definidos para cada proceso en el marco de referencia indicado.

Los controles clave que la empresa SISC debe implementar para lograr fortalecer su gestión de riesgos en ciberseguridad son un firewall de aplicaciones web para monitorear todo el tráfico que fluye hacia sus aplicaciones publicadas en la Internet, un programa anual de concientización en ciberseguridad. Asimismo, debe establecer prácticas de código seguro apropiadas al lenguaje de programación y a los entornos de desarrollo a ser usados. Finalmente, también debe priorizar las remediaciones a las vulnerabilidades descubiertas mediante la puntuación (severidad) de los riesgos asociados.

Por último, con relación a los objetivos planteados en el presente trabajo de investigación, se ha conseguido lograr lo siguiente:

- Obtener el nivel de capacidad de los procesos de detección y respuesta de eventos de ciberseguridad para la entidad materia de la investigación.
- Identificar las brechas en materia de ciberseguridad para los procesos de detección y respuesta de eventos de ciberseguridad.
- Determinar los controles clave que permitirán superar las brechas encontradas en el diagnóstico de capacidad ejecutado a los procesos materia de la presente investigación. Asimismo, se propuso el plan de implementación para los controles identificados.
- Elaborar la hoja de ruta para la implementación de los controles propuestos, considerando, en primer lugar de prioridad, aquellos controles que fortalecerán el proceso de detección y, posteriormente, los de respuesta.

Bibliografía

Alvarado, Daisy y Zumba, Laura. (2015). "Elaborar un Plan de Gestión de Riesgos de las Tecnologías de la Información y Comunicación basada en el Marco COBIT5 para Riesgos aplicado a la Universidad de Cuenca". 2015. Recuperado de http://dspace.ucuenca.edu.ec/bitstream/123456789/22342/1/TESIS.pdf. [Consulta: 26 de agosto de 2017]

Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology. (2016). "Analysis of cibersecurity Framework RFI Responses". En *nist.gob*. 24 de marzo 2016. Recuperado de https://www.nist.gov/sites/default/files/documents/cyberframework/RFI3_Response_Analysis_final.pdf>. [Consulta: 26 de agosto de 2017]

Armin Sarabi, Parinaz Naghizadeh, Yang Liu, Mingyan Liu (2016). "Risky business: Fine-grained data breach prediction using business profiles", *Journal of Cybersecurity*, vol. 2 (1), p. 15–28.

Banco Interamericano de Desarrollo (2016). "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?". En *BID*. Marzo 2016. Recuperado http://publications.iadb.org/ [Consulta: 29 de junio de 2017]

Center for Internet Security (2018). *CIS Controls*. [PDF]. CIS. Recuperado de https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/ [Consulta: 21 de julio de 2017]

Dedeke, A. (2017). "Cybersecurity framework adoption: Using capability levels for implementation tiers and profiles". *IEEE Security & Privacy*, vol. 15(5), p. 47-54. doi:10.1109/MSP.2017.3681063.

Deloitte (2016). "La Evolución de la Gestión de Ciber Riesgos y Seguridad de la Información. Encuesta 2016 sobre Tendencias de Ciber Riesgos y Seguridad de la Información en Latinoamérica". En *Deloitte*. Julio 2016. Recuperado de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/ [Consulta: 26 de agosto de 2017]

Deloitte (2016). “Beneath the surface of a cyberattack”. *En Deloitte*. 2016. Recuperado de https://www2.deloitte.com/us/beneath-the-surface-of-a-cyberattack [Consulta: 9 de junio de 2018].

EY (2017). “El camino hacia la resilencia cibernética”. En *EY*. Marzo 2017. Recuperado de https://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resiliencia-cibernetica/ $FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf [Consulta: 12 de septiembre de 2018].

Ernst and Young (2017). “Encuesta Global de Seguridad de la Información 2016 – 2017”. Recuperado de https://www.ey.com/Publication/vwLUAssets/EY-el-camino-hacia-resiliencia-cibernetica/$FILE/EY-el-camino-hacia-resiliencia-cibernetica.pdf [Consulta: 12 de septiembre de 2018].

Hernández, J., Gallarzo, M., Espinoza, J. (2011). “Desarrollo Organizacional”. Recuperado de http://www.ebooks7-24.com/?il=4330 [Consulta: 6 de septiembre de 2018].

International Standard Organization (2014). “NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos”. Segunda edición 2014.

International Standard Organization (2015). “ISO/IEC 33020:2015 Information Technology - Process Assessment – Process measurement framework for assessment of process capability”. Versión 2015. Recuperado de https://www.iso.org/standard/54195.html [Consulta: 1 de agosto de 2017].

ISACA (2012). *COBIT 5 Procesos Catalizadores.* Versión 1.0. Illinois.

ISACA (2013). *COBIT 5 for Risk.* Versión 1.0. Illinois.

ISACA (2014). *Implementing the NIST Cybersecurity Framework.* [PDF]. ISACA. Primera edición. Fecha de consulta: 01/08/2017, <www.isaca.org/>.

ISACA (2016). *IS Audit/Assurance Program Cybersecurity: Based on the NIST Cybersecurity Framework.* [PDF]. ISACA. Primera edición. Recuperado de www.isaca.org/Knowledge-

Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx [Consulta: 1 de agosto de 2017].

ISACA (2017). *Cybersecurity Fundamentals Study Guide.* [PDF]. ISACA. Segunda Edición. Recuperado de www.isaca.org/myisaca/Pages/MyDownloads.aspx [Consulta: 1 de junio de 2017].

Lazzati, S. (2016). "El Gerente: Estrategia y Líder del Cambio". Enero 2016. Recuperado de https://ebookcentral-proquest-com.ezproxy.ulima.edu.pe/lib/bibudlimasp/ detail.action?docID=4 824310 [Consulta: 6 de septiembre de 2018].

Mccollum (2016). "Cibernéticamente expuesto". Agosto 2016. *Internal Auditor,* volumen (LXXIII: IV). 11-13.

Manos, P. (2017). *Top cyber security issues for 2017 from leidos outlook & trends. Transmission & Distribution World,* Recuperado de https://search-proquest-com.up.idm.oclc.org/docview/1876880155?accountid=41232 [Consulta: 12 de septiembre de 2018].

Mulligan, D. K., & Schneider, F. B. (2011). "Doctrine for cybersecurity". *Daedalus*, vol. 140(4), p. 70-92. Recuperado de https://search.proquest.com/docview/903303254?accountid=41232 [Consulta: 12 de septiembre de 2018].

Newsfile corp. (2017). *SEC chairman clayton issues statement on cybersecurity*. Chatham: Newstex. Recuperado de https://search-proquest-com.up.idm.oclc.org/docview/1940633479?accountid=41232 [Consulta: 6 de septiembre de 2018].

NIST (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* [PDF]. NIST. Versión 1.0. Recuperado de www.nist.gov/cyberframework [Consulta: 29 de junio de 2017].

NIST (2017). *Cybersecurity Framework Workshop 2017 Summary.* [PDF]. NIST. Recuperado de www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf [Consulta: 2 de agosto de 2017].

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. [PDF]. NIST. Versión 1.1. Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Consulta: 12 de junio de 2018].

Piper, Arthur (2016). "Resistencia cibernética". Agosto 2016. *Internal Auditor*, volumen (LXXIII: IV). 35-41.

Price Waterhouse Coopers (PWC México) (2016). *Encuesta sobre delitos económicos 2016*. Recuperado de https://www.pwc.de/de/internationale-maerkte/2017-07-04-encuesta-sobre-delitos-economicos-2016.pdf. [Consulta: 15 de junio de 2018].

Rojas Andia, Karen. "WannaCry: El botón que se pulso en Perú y el nuevo capítulo que se estrena en cibercrimen". *Gestión.pe*. Recuperado de http://gestion.pe/tendencias/wannacry-boton-que-se-pulso-peru-y-nuevo-capitulo-que-se-estrena-cibercrimen-2190526 [Consulta: 30 de junio de 2017].

RSA (2015). "Índice de Pobreza en Ciberseguridad". En *EMC*. Abril 2015. Recuperado de https://mexico.emc.com/about/news/press/2016/20160614-01.htm [Consulta: 25 de agosto de 2017].

Sasha Romanosky (2016). "Examining the costs and causes of cyber incidents". *Journal of Cybersecurity*, vol. 2 (2), p. 121–135. Recuperado de https://doi.org/10.1093/cybsec/tyw001 [Consulta: 25 de junio de 2018].

Scofield, M. (2016). "Benefiting from the NIST cybersecurity framework. Information Management". *Information Management*, vol. 50(2), p. 25-28. Recuperado de https://search.proquest.com/docview/1779940925?accountid=41232 [Consulta: 12 de septiembre de 2017].

Shackelford, Scott J, J.D., P.H.D., Proia, A. A., J.D., Martell, B., J.D., & Craig, Amanda N, M.S.C., J.D. (2015). "Toward a global cybersecurity standard of care? Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices". *Texas International Law Journal*, vol. 50(2), p. 305-355.

Recuperado de https://search.proquest.com/docview/1704865080?accountid=41232 [Consulta: 12 de septiembre de 2017].
Shen, L. (2014). "The NIST Cybersecurity Framework: Overview and Potential Impacts". *Journal of Internet Law*, vol. 18(6), p. 3-6. Recuperado de https://search.proquest.com/docview/1639830271?accountid=41232 [Consulta: 25 de agosto de 2018].

Sobowale, J. (2017). "Managing Cyber Risk". *ABA Journal*, vol. 103, p. 34-43. Recuperado de https://search-proquest-com.up.idm.oclc.org/docview/1876462152?accountid=41232 [Consulta: 25 de septiembre de 2017].

Tenable network security, inc (2016).; "Tenable network security automates and simplifies NIST cybersecurity framework adoption for commercial and government organizations". *Journal of Engineering.* Recuperado de https://search.proquest.com/docview/1772324706?accountid= 41232 [Consulta: 12 de septiembre de 2018].

Uudhila, Jambeko M. (2016). "Cyber Security Risk Management and Threat Control Model; A study carried out to enhance the protection of information in the Namibian Public Service of Information in the Namibian Public Service". Marzo 2016. Recuperado de http://repository.unam.edu.na/handle/11070/1688 [Consulta: 16 de agosto de 2017].

Yin, R. (1994). *Case study research: Design and methods.* Segunda edición. Beverly Hills, CA: Sage Publishing.

World Economic Forum. (2017). *The Global Risks Report 2017 12th Edition*. [PDF].

Anexos

Anexo 1. Marco de referencia para la mejora de la ciberseguridad del NIST

El resumen adjunto se ha extraído del documento, versión 1.1 del Framework for Improving Critical Infraestructure Cybersecurity del National Institute of Standards and Technology (NIST 2018).

El marco es un enfoque basado en gestionar los riesgos de ciberseguridad, y se compone de tres partes: el núcleo, los niveles de implementación y los perfiles del marco de referencia. El núcleo provee un conjunto de actividades para alcanzar los resultados específicos en ciberseguridad y ejemplos de referencia como guía para lograr estos resultados. Asimismo, el núcleo comprende cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

Los elementos del marco de referencia trabajan juntos, como se indica a continuación:

- Las funciones organizan las actividades de ciberseguridad en su más alto nivel. Estas funciones son identificar, proteger, detectar, responder y recuperar.
- Las categorías son las subdivisiones de una función en grupos de resultados de ciberseguridad estrechamente relacionada a necesidades y actividades particulares.
- Las subcategorías adicionalmente dividen a una categoría en resultados específicos de actividades de gestión y/o técnicas.
- Las referencias informativas, son secciones específicas de estándares, lineamientos y prácticas comunes que ilustran un método para lograr los resultados de cada subcategoría.

Las cinco funciones del núcleo y las categorías se muestran en la tabla 26.

Tabla 26. Funciones y categorías, marco NIST

Función	Categoría
Identificar: desarrolla el entendimiento organizacional para gestionar los riesgos de ciberseguridad a los sistemas, activos, datos y capacidades.	Gestión de activos
	Entorno del negocio
	Gobierno
	Evaluación de riesgos
	Estrategia de gestión de riesgos
Proteger: desarrolla e implementa las salvaguardas apropiadas para asegurar la entrega de servicios críticos de infraestructura.	Control de accesos
	Entrenamiento y concientización
	Seguridad de datos
	Procesos y procedimientos para la protección de la información
	Mantenimiento
	Tecnología protectora
Detectar: desarrolla e implementa las actividades apropiadas para identificar la ocurrencia de eventos de ciberseguridad.	Anomalía y eventos
	Monitoreo continuo de la seguridad
	Procesos de detección
Responder: desarrolla e implementa las actividades apropiadas para tomar acción con relación a incidentes de ciberseguridad detectados.	Planear la respuesta
	Comunicaciones
	Análisis
	Mitigación
	Mejorar
Recuperar: desarrolla e implementa las actividades apropiadas para mantener planes de resiliencia y para restaurar cualquier capacidad de servicio que estuviera incapacitado debido a un evento de ciberseguridad	Planeamiento de la recuperación
	Mejoras
	Comunicación

Elaboración: NIST, 2018

Con relación a las funciones de detectar y responder, que son el alcance de la presente investigación, la descripción de las categorías y de las subcategorías que las componen se muestran a continuación en las tablas 27 y 28.

Tabla 27. Categorías y subcategorías de la función de detectar

Categoría	Subcategoría
Anomalías y eventos	Una línea base de operaciones de red y flujo de datos esperado para usuarios y sistemas se ha establecido y gestionado.
	Los eventos detectados son analizados para entender los objetivos del ataque y métodos.
	Los eventos de datos son coleccionados y correlacionados desde fuentes y sensores múltiples.
	El impacto de los eventos es determinado
	Se ha establecido umbrales de alerta de los incidentes
Monitoreo continuo de seguridad	La red es monitoreada para detectar potenciales eventos de ciberseguridad.
	Se monitorea el entorno físico para detectar potenciales eventos de ciberseguridad.
	El código malicioso es detectado.
	El código móvil no autorizado es detectado.
	La actividad del proveedor de servicio externo es monitoreada para detectar eventos de ciberseguridad potenciales.
	Se monitorea al personal, conexiones, dispositivos y software no autorizado.
	Se ejecuta el escaneo de vulnerabilidades.
Procesos de detección	Los roles y responsabilidades para la detección están bien definidas para asegurar la rendición de cuentas.
	Las actividades de detección cumplen con todos los requerimientos aplicables.
	Los procesos de detección son probados.
	La información de detección de eventos es comunicada.
	Los procesos de detección con mejorados continuamente.

Elaboración: NIST, 2018

Tabla 28. Categorías y subcategorías de la función de responder

Categoría	Subcategoría
Plan de respuesta	El plan de respuesta es ejecutado durante o después de un incidente.
Comunicación	El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
	Los incidentes se reportan consistentemente con criterios establecidos.
	La información se comparte consistentemente con planes de respuesta.
	Las coordinaciones con los interesados ocurren consistentemente con planes de respuesta.
	Se comparte la información con los interesados externos para lograr una mayor conciencia de la situación en ciberseguridad.
Análisis	Las notificaciones de los sistemas de detección son investigadas.
	El impacto de los incidentes es entendido.
	Un análisis forense es ejecutado.
	Los incidentes se categorizan según los planes de respuesta.
	Los procesos son establecidos para recibir, analizar y responder a las vulnerabilidades encontradas a la organización desde fuentes internas y externas (pruebas internas, boletines o investigadores de seguridad).

Categoría	Subcategoría
Mitigación	Los incidentes son contenidos.
	Los incidentes son mitigados.
	Las recientes vulnerabilidades identificadas son mitigadas o documentadas como riesgos aceptados.
Mejora	Planes de respuesta incorporan las lecciones aprendidas.
	Las estrategias de respuesta son actualizadas

Elaboración: NIST, 2018.

Anexo 2. Implementación y programa de auditoría/aseguramiento del marco de ciberseguridad del NIST

El resumen adjunto se ha extraído de los documentos, Implementando el marco de ciberseguridad del NIST (ISACA 2014) y del Programa de auditoría/aseguramiento del marco de ciberseguridad (ISACA 2016).

Debido al incremento del volumen y sofisticación de los ciberataques, la Information Systems Audit and Control Association (ISACA) ha desarrollado un programa de aseguramiento y auditoría basado en el marco de referencia de ciberseguridad del NIST para proveer a las organizaciones con una formal y repetible manera para evaluar los controles de ciberseguridad.

El objetivo de una auditoría de ciberseguridad es proveer una evaluación de la efectividad de los procesos, políticas, procedimientos, gobierno y otros controles de ciberseguridad. La revisión se enfoca en los estándares, lineamientos y procedimientos de ciberseguridad como también en la implementación de estos controles. Además, la revisión de auditoría se basa en la auditoría operacional de los procesos de gestión de incidentes; gestión de la configuración y la seguridad de las redes y servidores; la gestión de la seguridad y concientización; gestión de la continuidad del negocio; gestión de la seguridad de la información; gobierno y prácticas de gestión de las unidades de negocio, de las tecnologías de la información y las relaciones con los proveedores.

Los pasos de auditoría han sido desarrollados para cada subcategoría del marco de referencia de ciberseguridad del NIST para evaluar la efectividad de los controles en la organización. El documento contiene una hoja de cálculo en Excel para un completo programa de auditoría/aseguramiento.

Anexo 3. ISO/IEC 33020:2015 Tecnología de la información- evaluación de procesos– marco de medición de procesos para evaluar la capacidad de los procesos

La norma define las bases para la evaluación de capacidad de los procesos e identifica el marco de medición para la capacidad de procesos y los requerimientos para cumplir con lo siguiente:

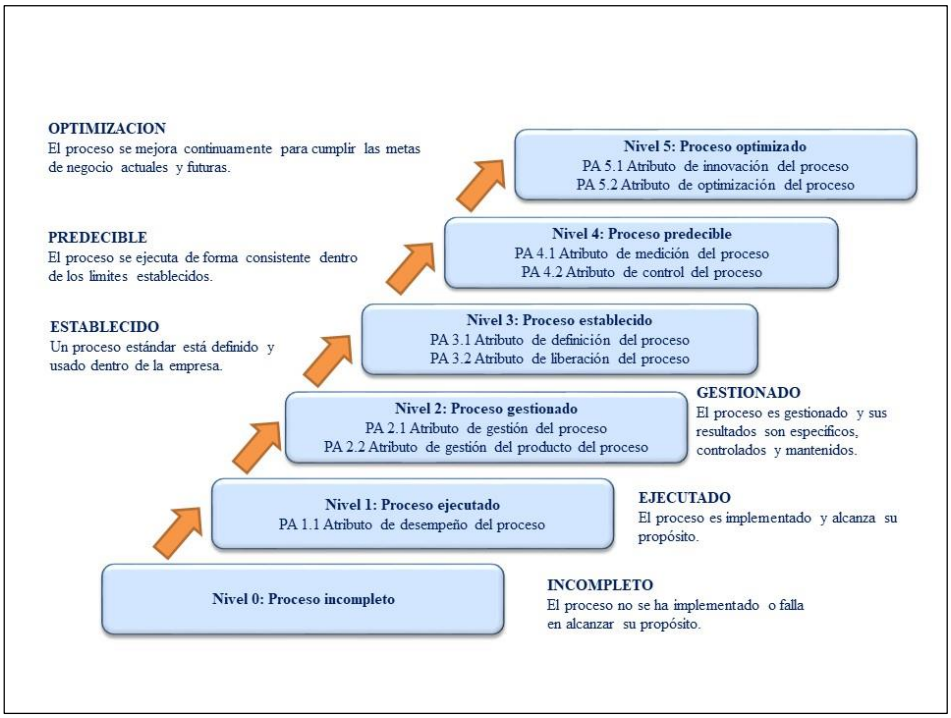
- Ejecutar una medición.
- Los modelos de referencia de los procesos.
- Los modelos de evaluación de procesos.
- Verificar la conformidad de la evaluación de procesos.

La evaluación de procesos se define como un modelo de dos dimensiones, una dimensión de proceso y una dimensión de capacidad. La dimensión de proceso es provista por un modelo de referencia de procesos externo, que define un conjunto de procesos caracterizados por enunciados de propósitos y resultados del proceso. Para el presente estudio, se definen los procesos en el marco de referencia para la mejora de la ciberseguridad del NIST. La dimensión de capacidad consiste en un marco de dimensión que comprende 6 niveles de capacidad de proceso y sus atributos de proceso asociados.

El marco de medición para la capacidad del proceso

La capacidad de los procesos es definida en una escala de seis puntos ordinales que permiten a la capacidad ser evaluada desde la escala incompleto, hasta la escala optimizado. En el gráfico 9, se muestra la escala de medición.

Gráfico 9. Escala de medición del ISO/IEC 33020



Elaboración: International Standard Organization, 2015.

La escala representa el incremento de capacidad de los procesos implementados, desde no lograr el propósito del proceso hasta cumplir las metas actuales y proyectadas de la empresa.

El marco entrega un esquema para ser usado en la medición de la capacidad de un proceso implementado con respecto a un modelo de evaluación de procesos. Dentro del marco, la medida de la capacidad está basada en un conjunto de atributos de proceso. Cada atributo define un particular aspecto de la capacidad del proceso. La extensión del logro de un atributo del proceso es caracterizada sobre una escala de medición definida. La combinación del logro de atributos del proceso y un agrupamiento de atributos de proceso juntos determina el nivel de capacidad del proceso.

Medición de los atributos del proceso

a. Escala de medición de los atributos del proceso

La extensión del logro de los atributos del proceso es medida usando una escala ordinal de medición como se define en la tabla 29.

b. Valores de medición de los atributos del proceso

La escala de medición ordinal definida será usada para expresar los niveles de cumplimiento de los atributos del proceso.

Tabla 29. Escala de medición para calificar atributos del proceso

Sigla	Escala de clasificación	Definición	Valores
N	No alcanzado	Hay poca o ninguna evidencia del logro del atributo definido en el proceso evaluado	0 a 15% de consecución
P	Parcialmente alcanzado	Existe alguna evidencia de un enfoque, y de algún logro, del atributo definido en el proceso evaluado.	>15% hasta 50% de consecución
L	Largamente alcanzado	Hay evidencia de un enfoque sistemático, y de un logro significativo, del atributo definido en el proceso evaluado. Algunas debilidades del atributo pueden existir en el proceso evaluado.	<50% hasta 85% de consecución
F	Completamente alcanzado	Hay evidencia de un enfoque completo y sistemático, y de la plena consecución, del atributo definido en el proceso evaluado. No existen debilidades importantes en el atributo.	>85% hasta 100% de consecución

Elaboración: International Standard Organization, 2015.

c. Proceso de medición de los atributos

Cada atributo del proceso deberá ser medido usando la escala ordinal definida en la tabla 29. Un proceso deberá ser evaluado para incluir el más alto nivel de capacidad definido en el alcance de la evaluación.

d. Logro de los niveles de capacidad de procesos

El nivel de capacidad alcanzado por un proceso será derivado de la valuación de los atributos del proceso.

Anexo 4. COBIT 5 para riesgos

El resumen adjunto se ha extraído del documento, COBIT 5 for Risk, versión 1.0 (ISACA 2013). Este documento está construido sobre el marco de referencia de COBIT 5 (ISACA 2012) y se enfoca en los riesgos y provee más detalle y una guía práctica para los profesionales del riesgo y otros interesados en todos los niveles de la empresa. COBIT 5 para riesgos discute los riesgos relacionados a la tecnología de la información.

COBIT 5 para riesgos presenta dos perspectivas sobre cómo usar COBIT 5 en un contexto de riesgos: la función de riesgos y la gestión de riesgos.

- La perspectiva de función de riesgos se enfoca en lo que se necesita para construir y sostener la función de riesgos dentro de la empresa.
- La perspectiva de gestión de riesgos se enfoca en los procesos de gobierno y gestión de riesgos, de cómo optimizar los riesgos y como, identificar, analizar, responder y reportar los riesgos

A continuación, se describirá la perspectiva de la gestión de riesgos

Los escenarios de riesgo

Un escenario de riesgo es una descripción de un posible evento que, cuando ocurre, tendrá un impacto incierto en el cumplimiento de los objetivos de la empresa. El impacto puede ser negativo o positivo. El proceso principal en la gestión de riesgos requiere las necesidades de los riesgos, para ser identificados, analizados y tomar decisiones sobre ellos. Un buen desarrollo de los escenarios de riesgos soporta estas actividades y los hace más realistas y relevantes a la empresa.

Los factores de riesgo

Los factores de riesgo son aquellas condiciones que influencian en la frecuencia y/o impacto al negocio de los escenarios de riesgo. Pueden ser de diferente naturaleza y pueden ser categorizados en dos categorías mayores:

- Factores contextuales. Que pueden ser divididos en factores internos y externos, siendo la diferencia el grado de control que la empresa tiene sobre ellos:
  - Factores contextuales internos. En una gran extensión bajo el control de la empresa, aunque pueden no siempre ser fácil de cambiar.
  - Factores contextuales externos. En una gran extensión, están fuera de control de la empresa.
- Capacidades. Cuán efectiva y eficiente es la empresa en un número de actividades relacionadas a las tecnologías de la información, pueden ser distinguidas del siguiente modo:
  - Capacidades de gestión de riesgos de tecnologías de la información. Indica cuán bien la empresa está ejecutando el proceso de gestión de riesgos. Este factor está correlacionado con la capacidad de la empresa para reconocer y detectar riesgos y eventos adversos.
  - Capacidades relacionadas a tecnologías de la información. Indica la capacidad de los habilitadores de COBIT 5 relacionados a la tecnología de la información. Una alta madurez con relación a los diferentes habilitadores es equivalente a altas capacidades relacionadas a TI, los cuales pueden tener un impacto positivo en reducir la tasa de frecuencia de los eventos o en reducir el impacto al negocio cuando los eventos ocurren.

La importancia de los factores de riesgos radica en la influencia que tienen sobre los riesgos. Tienen mucha influencia en la frecuencia e impacto de los escenarios de TI y deberían ser tomados en cuenta durante el análisis de todo riesgo.

La estructura del escenario de riesgos de TI

Los escenarios de riesgo contienen los siguientes componentes:

- Actor. Quien genera la amenaza que explota una vulnerabilidad. Los actores pueden ser internos o externos y pueden ser o no humanos.
- Tipo de amenaza. La naturaleza del evento es maliciosa, es accidental, es una falla de un proceso definido o es un evento natural.
- Evento. Es la divulgación de información confidencial, es la interrupción de un sistema, robo o destrucción. La acción puede incluir inefectivo diseño de sistemas o procesos, un inapropiado uso o una inefectiva ejecución de los procesos.
- Activo/recurso. Sobre qué escenario actúa. Un activo es un ítem de valor para la empresa que puede ser afectado por el evento y llegar a impactar al negocio. Un recurso es todo lo que ayuda a cumplir las metas de TI. Los activos y recursos pueden ser idénticos.
- El tiempo. La dimensión donde lo siguiente puede ser descrito, si es relevante para el escenario.

    - La duración del evento.
    - El registro del tiempo en el cual ocurre (sucede en un momento crítico).
    - La detección (es inmediata o no).
    - Desfase entre el evento y sus consecuencias (hay una inmediata consecuencia)

Los escenarios de riesgos genéricos

Los escenarios de riesgo genéricos sirven, después de su adaptación, como entrada a las actividades de análisis de riesgos, donde el resultado final de impacto al negocio (entre otros) necesita ser establecido.

Los escenarios de riesgo genéricos incluyen la siguiente información:

- Categoría de escenario de riesgos. Descripción de alto nivel de la categoría del escenario. Hay 20 categorías
- Componentes del escenario de riesgo. Da detalles acerca del tipo de amenaza, el actor, evento, activo/recurso y tiempo de cada categoría de escenario.
- Tipo de riesgo. El tipo para el cual los escenarios derivados del escenario genérico encajaran.

Anexo 5. Detalle de la evaluación de capacidad de los procesos de detectar y responder

1 Proceso: detectar

1.1 Subproceso: anomalías y eventos

1.1.1 Objetivo de control: la actividad anómala se detecta y se entiende el potencial impacto de los eventos.

Tabla 30. Subproceso anomalía y eventos

Control	Paso de prueba	Nivel de capacidad
Una línea base de las operaciones de red y de los flujos de datos esperados por los usuarios, se ha establecido y se gestiona.	1. Obtener una copia del diagrama lógico de red de la organización, los diagramas de flujo de datos y otros diagramas de redes y comunicaciones, revisar los diagramas por lo siguiente: a. Frecuencia de actualización de los diagramas. b. Exactitud y completitud de los diagramas. c. El alcance de los diagramas es adecuado para identificar ambos dominios de diferente riesgo y niveles de control.	L: Se cuenta con un diagrama completo de la red, pero está desactualizado.
	2. Determinar si se usan herramientas (esto es, sistemas de gestión de la información y eventos de seguridad (SIEM) para establecer el tráfico típico (línea base), tal que se pueda detectar el tráfico anormal.	C: Si se usan herramientas. SISC ha integrado sus herramientas de seguridad al correlacionador de eventos (SIEM) de un cliente, por estar en su red.
Los eventos detectados son analizados para entender los objetivos y métodos de ataque.	1. Obtener una copia de las políticas y procedimientos con relación al monitoreo de la red y los sistemas. a. Determinar si las políticas y los procedimientos requieren el monitoreo por actividades anómalas en puntos de control identificados.	N: No existen documentos relacionados al monitoreo de eventos anómalos de ciberseguridad.
	2. Obtener una copia de los eventos detectados (por ejemplo, alertas del IPS) y la respuesta de la organización a ellos. Revisar los eventos y respuestas para asegurar que se haya ejecutado un completo análisis de los eventos detectados.	N: No todos los eventos generados se analizan, se observó que los eventos que genera el IPS no se analizan.
Los datos de los eventos son colectados y correlacionados desde múltiples fuentes y sensores.	1. Obtener un listado de los eventos de los sistemas de monitoreo y agregación en uso en la organización, por ejemplo, SIEM, sistemas de correlación de log de eventos. 2. Obtener una lista de las fuentes que proveen datos para cada sistema de monitoreo y agregación de eventos. 3. Comparar las fuentes para identificar los puntos de control entre los dominios de diferentes niveles de control y riesgos y determine si ellos proveen adecuado monitoreo que cubra el entorno de la organización.	L: Los puntos de control proveen un buen nivel de monitoreo, pero falta agregar algunas fuentes relevantes.

Control	Paso de prueba	Nivel de capacidad
Los impactos de los eventos son determinados.	1. Obtener una copia de los eventos detectados y las respuestas de la organización a ellos. 2. Revisar los eventos, tickets y respuestas a fin de asegurar que la organización está documentando el impacto de las actividades anómala usando métricas que son aplicables a la organización.	N: No se encontró evidencia
Los umbrales de alerta a los incidentes están establecidos.	1. Obtener una copia de los mensajes de alerta, minutas de reunión, reportes y otra documentación donde los eventos detectados fueron escalados. 2. Revisar la documentación y determinar lo siguiente: a. Los eventos detectados son reportados oportunamente a alguien con el conocimiento y experiencia para resolver y escalar el evento. b. Los eventos escalados son reportados a individuos o grupos con la apropiada autoridad para tomar decisiones acerca de la respuesta en la organización. c. Se han definido umbrales tal que un evento active la apropiada respuesta.	P: Existe un procedimiento informal para escalar los eventos. No existen umbrales definidos de manera formal.

Fuente: Elaboración propia, 2018.

1.2 Subproceso: monitoreo continuo de la seguridad

1.2.1 Objetivo de control: los sistemas de información y los activos se monitorean para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.

Tabla 31. Subproceso monitoreo continuo de la seguridad

Control	Paso de prueba	Nivel de capacidad
La red es monitoreada para detectar potenciales eventos de ciberseguridad.	1.Obtener una lista del control de monitoreo implementado por la organización en los siguientes niveles: a. Redes (por ejemplo, *firewall, router, switch*). b. Sistemas operativos. c. Aplicaciones.	P: Se ha implementado monitoreo en un solo nivel. Se ha implementado el monitoreo al nivel de redes a través del uso de Firewall e IPS.
	2. Determinar si el monitoreo en cada nivel incluye la detección de eventos de ciberseguridad, accesos a cuentas no autorizadas, accesos a archivos/sistemas no autorizados, ataques de escalación de privilegios, ataques de inyección de SQL.	P: Se incluye detección de eventos de ciberseguridad en un nivel. Solo se detectan eventos a nivel de red (denegación de servicios).
El entorno físico es monitoreado para detectar potenciales eventos de ciberseguridad.	1. Obtener un inventario de las instalaciones críticas. 2. Determinar si los controles de monitoreo de la seguridad física están implementados y son apropiados para detectar potenciales eventos de ciberseguridad.	P: Solo en algunas instalaciones se han implementado controles de monitoreo a la seguridad física.

Control	Paso de prueba	Nivel de capacidad
La actividad personal es monitoreada para detectar potenciales eventos de ciberseguridad.	1. Obtener una lista de los controles de monitoreo implementados por la organización en el nivel de cuenta de usuario / aplicación. 2. Determinar si el monitoreo incluye la detección y alerta de eventos de ciberseguridad.	P: El monitoreo solo es a nivel de cuentas de usuario.
El código malicioso es detectado.	1. Obtener una copia de los procesos y procedimientos usados para detectar código malicioso en la red y servidores/puestos de trabajo. 2. Determinar si los controles de código malicioso están: a. Instalados en todos los puntos de control de red y de sistemas que apliquen. b. Actualizados regularmente. c. Configurados para ejecutar escaneo en tiempo real o escaneo periódico a intervalos regulares.	L: Existen dos atributos del control.
	3. Efectuar un chequeo muestral en los puestos de trabajo y otros dispositivos finales de usuario para verificar lo siguiente: a. Controles de código malicioso están instalados. b. Controles de código malicioso están actualizados. c. Controles de código malicioso están en capacidad de detectar código de prueba.	L: Existen dos atributos del control.
El código móvil no autorizado es detectado.	1. Obtener los procesos y procedimientos documentados usados para detectar el código móvil no autorizado que este corriendo sobre los servidores de la organización, puestos de trabajo y dispositivos. 2. Determinar si los controles de detección de código móvil bloquean el código móvil no autorizado cuando es detectado.	C: Existen controles de detección de código móvil
Se monitorea la actividad de los proveedores de servicios externos, para detectar potenciales eventos de ciberseguridad.	1. Obtener y revisar los contratos ejecutados con los proveedores de servicio externo. 2. Determinar si los contratos requieren al proveedor para: a. Notificar a la organización tan pronto como sea posible de cualquier evento de ciberseguridad sospechoso o conocido. b. Notificar a la organización tan pronto como sea posible, la terminación de cualquier empleado con credenciales de acceso a los sistemas o instalaciones de la organización. c. Implementar los controles de seguridad equivalentes a o que excedan el nivel de seguridad requerido de la organización.	P: Los contratos solo especifican uno de los controles

Control	Paso de prueba	Nivel de capacidad
Se monitorea la actividad de los proveedores de servicios externos, para detectar potenciales eventos de ciberseguridad.	3. Obtener una copia del diagrama de red lógico de la organización para determinar cómo las redes de los proveedores de servicio externo se conectan a la red de la empresa, para determinar si los controles de monitoreo están implementados en estos puntos de conexión.	C: Están implementados los controles de monitoreo
	4. Obtener y analizar una copia de las configuraciones de los sistemas por los controles de monitoreo usados, para detectar eventos de ciberseguridad originados en redes de proveedores de servicios externos.	N: Los controles de monitoreo implementados no se analizan para detectar oportunamente eventos. Es reactivo.
El monitoreo del personal, conexiones, dispositivos y software no autorizado es ejecutado.	1. Confirme la existencia de procesos y procedimientos diseñados para detectar accesos no autorizados a las instalaciones y sistemas de la organización.	L: Solo existen procedimientos para detectar accesos no autorizados a instalaciones y a la red.
	2. Efectuar un chequeo rápido de los controles de acceso no autorizado mediante el acceso a instalaciones y sistemas con permiso para probar, pero sin autorización estándar.	L: Solo se generan alertas a nivel de acceso a las instalaciones o a la red
El escaneo de vulnerabilidades es ejecutado.	1. Obtener una copia del cronograma para ejecutar el escaneo de vulnerabilidades internas y externas y los resultados de los más recientes escaneos de vulnerabilidad internos y externos. 2. Revisar el cronograma y los resultados por: a. Frecuencia. b. Termino exitoso. c. Resolución documentada o mitigación de vulnerabilidades identificadas. d. Si el alcance de las pruebas incluye todos los sistemas críticos.	P: Se ejecuta el escaneo de una manera ocasional, y se mitiga parcialmente las vulnerabilidades encontradas.

Fuente: Elaboración propia, 2018.

1.3 Subproceso: procesos de detección

1.3.1 Objetivo de control: los procesos y procedimientos de detección se mantienen y prueban para asegurar la concientización en los eventos anómalos.

Tabla 32. Subproceso procesos de detección

Control	Paso de prueba	Nivel de capacidad
Los roles y responsabilidades para la detección están bien definidos para asegurar la rendición de cuentas.	1. Obtener una copia de los procesos y procedimientos para el monitoreo de eventos anómalos electrónicos y físicos. 2. Determinar si los procesos y procedimientos asignan responsabilidades claves a individuos o posiciones específicas.	P: Las responsabilidades claves o posiciones específicas se han definido informalmente y ocasionalmente se cumplen

Control	Paso de prueba	Nivel de capacidad
La detección de actividades cumple con todos los requerimientos aplicables.	1. Obtener una copia de las leyes y regulaciones, estándares de la industria, requerimientos de seguridad internos y apetitos de riesgo aplicables a la empresa. 2. Determinar si la organización está ejecutando auditorias/pruebas para asegurar que sus actividades de detección cumplen con estos requerimientos.	N: No se ejecutan auditorías o pruebas
Los procesos de detección son probados.	1. Obtener una copia del cronograma de las pruebas de respuesta a los incidentes, los resultados de las recientes pruebas de respuesta a incidentes, y procesos y procedimientos documentados que requieren pruebas de controles de actividad anómala. 2. Revisar la documentación por: a. Completitud en las pruebas de los controles de detección de actividad anómala. b. Frecuencia de las pruebas. c. Resolución documentada o mitigación de resultados de pruebas negativas.	N: El proceso de detección no se prueba
La información de la detección de eventos es comunicada a las partes apropiadas.	1. Obtener una copia de las minutas de reunión donde la actividad anómala electrónica y física es reportada. 2. Obtener una copia de las respuestas documentadas a incidentes de actividad anómala electrónica y física reciente. 3. Comparar las minutas de reunión con los incidentes documentados y determinar si los eventos detectados son consistentemente reportados y manejados apropiadamente.	P: Los eventos detectados se reportan ocasionalmente
Los procesos de detección son mejorados continuamente.	1. Obtener una copia de las respuestas documentadas a los incidentes de actividad anómala electrónica y física reciente. Determine si las respuestas incluyen: a. Lecciones aprendidas y análisis de controles faltantes o fallidos. b. Detalle de acciones para detectar/prevenir incidentes similares en el futuro.	P: Existe evidencia ocasional de lecciones aprendidas y acciones para prevenir incidentes

Fuente: Elaboración propia, 2018.

2 Proceso: responder

2.1 Subproceso: planear la respuesta

2.1.1 Objetivo de control: los procesos y procedimientos de respuesta son ejecutados y mantenidos para asegurar la respuesta a los incidentes de ciberseguridad detectados.

Tabla 33. Subproceso planear la respuesta

Control	Pasos de prueba	Nivel de capacidad
El plan de respuesta es ejecutado durante o después de un incidente.	1. Determinar si la organización ha aprobado los planes de continuidad del negocio y de respuesta a los incidentes.	L: Solo se aprobó uno de los planes. Documento de Protocolo de Seguridad aprobado por Roger Bernedo, Director de Sistemas el 13/12/2016
	2. Obtener copias de los reportes de recientes incidentes para validar que los planes están ejecutados.	P: Los planes se ejecutaron ocasionalmente

Fuente: Elaboración propia, 2018.

2.2 Subproceso: comunicaciones

2.2.1 Objetivo de control: las actividades de respuesta son coordinadas con los interesados internos y externos

Tabla 34. Subproceso comunicaciones

Controles	Pasos de prueba	Nivel de capacidad
El personal conoce sus roles y orden de operaciones cuando una respuesta es necesaria.	1. Revisar el plan de respuesta a los incidentes para determinar si los roles y responsabilidades están definidos para los empleados.	P: Algunos roles o responsabilidades están definidos. Al reportarse una vulnerabilidad, se delega la tarea al equipo especialista quien reporta la acción correctiva tomada, luego de lo cual se cierra el reporte.
	2. Entrevistar a los empleados para determinar si conocen sus roles y responsabilidades como se definió en el plan.	P: Algunos empleados conocen su rol y responsabilidades.
	3. Revisar algunas pruebas de respuesta a los incidentes o entrenamiento entregado a los empleados para determinar si soportan la educación de los empleados en sus roles y responsabilidades.	P: Soportan parcialmente la educación de los empleados en sus roles y responsabilidades. La comunicación fluye desde el equipo que reporta la vulnerabilidad, se delega la tarea al equipo especialista quien reporta la acción correctiva tomada, luego de lo cual se cierra el reporte.
Los incidentes son reportados consistentemente con criterios establecidos.	1. Revisar el plan de respuesta a los incidentes para determinar si la estructura del reporte y los canales de comunicación están claramente definidos.	P: Los reportes y canales de comunicación están vagamente definidos. Reportado un incidente se comunica el mismo a los responsables de mitigarlo. Asimismo, según el nivel de impacto se informa a la Gerencia. Hay que formalizar estos canales.

Controles	Pasos de prueba	Nivel de capacidad
Los incidentes son reportados consistentemente con criterios establecidos.	2. Determinar si los empleados están entrenados para reportar sospechosos incidentes de seguridad.	P: Los empleados están parcialmente entrenados para reportar sospechosos incidentes de seguridad.
	3. Obtener copias de los reportes de recientes incidentes para validar la consistencia del reporte y que se sigue el plan.	P: Los reportes de incidentes son parcialmente consistentes
La información es consistentemente compartida con los planes de respuesta.	1. Revisar el plan de respuesta a los incidentes para determinar si el intercambio de información está claramente definido y como se relaciona a lo siguiente: a. Clientes b. Cumplimiento legal c. Entidades reguladoras d. Medios usados e. Organizaciones que comparten información	N: El intercambio de información no está definido.
	2. Obtener copias de los reportes de recientes incidentes para validar que la compartición es consistente y se sigue el plan.	N: No hay evidencia de que se comparte información.
La coordinación con los interesados ocurre consistentemente con planes de respuesta.	1. Revisar el plan de respuesta a incidentes para determinar si existe un procedimiento para la comunicación con los interesados internos y externos durante y a continuación de un incidente.	P: Aunque no existe un procedimiento escrito, se estableció un canal de comunicación a los interesados internos, ocurrido un incidente.
	2. Obtener copias de los reportes de recientes incidentes para validar su consistencia del y se sigue el plan.	P: Mas del 15% de reportes revisados siguen el plan de respuesta.
Intercambio voluntario de información ocurre con los interesados externos para una conciencia situacional en ciberseguridad.	1. Revisar el plan de respuesta a los incidentes para determinar si existe un procedimiento para la comunicación con los interesados externos (por ejemplo, los usuarios, proveedores, clientes) que siga a un incidente.	N: No existe un procedimiento para la comunicación con los interesados externos ocurrido un incidente.

Fuente: Elaboración propia, 2018.

2.3 Subproceso: análisis

2.3.1 Objetivo de control: el análisis es realizado para asegurar efectiva respuesta y soporte a las actividades de recuperación.

Tabla 35. Subproceso análisis

Controles	Pasos de prueba	Nivel de capacidad
Las notificaciones de los sistemas de detección son investigadas.	1.Determinar quien recibe las alertas o reportes desde la detección de los sistemas y que acciones son tomadas una vez que los reportes son recibidos.	P: Solo unas pocas alertas y reportes cuentan con evidencia de acciones tomadas.
	2. Revisar el plan de respuesta a los incidentes para determinar si las acciones tomadas siguieron el plan.	P: Solo unas pocas acciones tomadas siguieron el plan.
El impacto de los incidentes es entendido.	1. Revisar el plan de respuesta a los incidentes para determinar si hay un proceso formal para analizar y clasificar los incidentes basado en su potencial impacto.	P: Existe un proceso informal por el cual se analiza los incidentes.
	2. Revisar el currículo y la educación de los miembros del equipo de respuesta a incidentes responsables de determinar el impacto a los incidentes, para determinar si tienen el conocimiento y experiencia para entender el potencial impacto.	L: Mas de la mitad de los miembros del equipo de respuesta cuentan con el conocimiento y experiencia
Análisis forense son ejecutados.	a. Hay un proceso para asegurar que el análisis forense será ejecutado cuando se necesite.	N: No existe un proceso
	b. Determinar si las investigaciones de seguridad y análisis forense son ejecutadas por personal calificado o terceras partes.	N: No se ejecuta investigación de seguridad y análisis forense
	c. Revisar los procedimientos forenses para asegurar que incluyen controles, tales como cadena de custodia, para soportar potenciales acciones legales.	N: No se incluyen controles
Los incidentes son categorizados consistentemente con los planes de respuesta.	1. Revisar el plan de respuesta a incidentes para determinar si está diseñado para priorizar los incidentes, posibilitando una rápida respuesta para incidentes o vulnerabilidades significativas.	P: El diseño si bien no prioriza los incidentes, ocasionalmente califica el impacto de estos.
	2. Obtener copias de los reportes de recientes incidentes para validar si el reporte es consistente y sigue los planes.	P: Los reportes ocasionalmente son consistentes y sigue los planes.
Los procesos son establecidos para recibir, analizar y responder a las vulnerabilidades divulgadas en fuentes internas y externas.	1.Revisar el procedimiento de gestión de incidentes y confirmar si describe, la recepción, análisis y respuesta a las vulnerabilidades divulgadas por fuentes internas o externas.	N: No existe el procedimiento

Fuente: Elaboración propia, 2018.

2.4 Subproceso: mitigación

2.4.1 Objetivo de control: se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y resolver el incidente.

Tabla 36. Subproceso mitigación

Controles	Pasos de prueba	Nivel de capacidad
Los incidentes son mitigados.	1. Revisar el plan de respuesta a incidentes para determinar si pasos apropiados se han contemplado para mitigar el impacto de un incidente. Considere lo siguiente: a. Pasos para mitigar el incidente para prevenir daños posteriores b. Procedimientos para notificar a terceras partes potencialmente impactadas. c. Estrategias para mitigar diferentes tipos de incidentes (ej. denegación de servicio distribuido (DDoS), malware, etc.)	P: Solo se ha contemplado uno de los pasos, siendo los pasos para mitigar el incidente producido.
	2. Revisar cualquier incidente documentado para determinar si los esfuerzos de mitigación fueron implementados y efectivos.	L: Los incidentes se mitigan mayormente y casi siempre es efectiva la mitigación.
Las vulnerabilidades identificadas recientemente son mitigadas o documentadas como riesgos aceptados.	1. Determinar si los programas de monitoreo continuo de la empresa facilitan una continua concientización en amenazas, vulnerabilidades y seguridad de la información para soportar las decisiones de gestión de riesgo organizacional. Considerar lo siguiente:	L: Frecuentemente se revisan las vulnerabilidades identificadas. Las vulnerabilidades reportadas se revisan por el especialista para identificar en primer nivel si podemos ser afectados, si fuera así se trabaja la mitigación del riesgo.
	b. Los resultados generan apropiadas respuestas al riesgo basada en el apetito de riesgo de la organización.	L: Frecuentemente se generan apropiadas respuestas al riesgo. Normalmente se mitigan los riesgos, siempre que no haya gastos en que se deba incurrir para mitigarlos.

Fuente: Elaboración propia, 2018.

2.5 Subproceso: mejoras

2.5.1 Objetivo de control: las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta

Tabla 37. Subproceso mejoras

Controles	Pasos de prueba	Nivel de capacidad
Los planes de respuesta incorporan lecciones aprendidas.	1. Revisar los reportes de incidentes manejados en la organización y la documentación de prueba de los incidentes por elementos de acción y lecciones aprendidas.	P: Los reportes de incidentes revelan ocasionalmente cursos posteriores de acción y/o lecciones aprendidas
	2. Evaluar el plan de respuesta a los incidentes para determinar si los resultados de los incidentes reales y las pruebas de incidentes han sido usados para actualizar los procedimientos de respuesta, entrenamiento y pruebas.	P: Se usaron ocasionalmente para actualizar los procedimientos de respuesta
Las estrategias de respuesta son actualizadas.	1. Hay un mecanismo establecido para regularmente revisar, mejorar, aprobar y comunicar los planes.	N: No hay un mecanismo establecido
	2. La capacidad de respuesta de la organización es informada mediante las amenazas corrientes, pruebas e incidentes actuales	N: La capacidad de respuesta de la organización no es informada

Fuente: Elaboración propia, 2018.

3 Resultados de capacidad de los procesos evaluados

3.1 Proceso de detección

En las tablas 38 y 39 se muestran los resultados obtenidos de la evaluación de capacidad de los procesos de detección y respuesta.

Los valores logrados fueron los siguientes:

- Promedio del proceso detectar: 0,47 (parcialmente alcanzado).
- Promedio del proceso responder: 0,45 (parcialmente alcanzado).

Tabla 38. Resultados proceso detectar

Subproceso	Objetivos de control	Controles	Prom. control	Prom. subproceso
Anomalías y eventos	La actividad anómala se detecta y se entiende el potencial impacto de los eventos.	Una línea base de las operaciones de red y de los flujos de datos esperados por los usuarios, se ha establecido y se gestiona.	0,93	0,46
		Los eventos detectados son analizados para entender los objetivos y métodos de ataque.	0,00	
		Los datos de los eventos son colectados y correlacionados desde múltiples fuentes y sensores.	0,85	
		Los impactos de los eventos son determinados.	0,00	
		Los umbrales de alerta a los incidentes están establecidos.	0,50	

Subproceso	Objetivos de control	Controles	Prom. control	Prom. subproceso
Monitoreo continuo de la Seguridad	Los sistemas de información y los activos se monitorean para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	La red es monitoreada para detectar potenciales eventos de ciberseguridad.	0,50	0,65
		El entorno físico es monitoreado para detectar potenciales eventos de ciberseguridad.	0,50	
		La actividad personal es monitoreada para detectar potenciales eventos de ciberseguridad.	0,50	
		El código malicioso es detectado.	0,85	
		El código móvil no autorizado es detectado.	1,00	
		Se monitorea la actividad de los proveedores de servicios externos, para detectar potenciales eventos de ciberseguridad.	0,50	
		El monitoreo del personal, conexiones, dispositivos y software no autorizado es ejecutado.	0,85	
		El escaneo de vulnerabilidades es ejecutado.	0,50	
Procesos de detección	Los procesos y procedimientos de detección se mantienen y prueban para asegurar la concientización en los eventos anómalos.	Los roles y responsabilidades para la detección están bien definidos para asegurar la rendición de cuentas.	0,50	0,30
		La detección de actividades cumple con todos los requerimientos aplicables.	0,00	
		Los procesos de detección son probados.	0,00	
		La información de la detección de eventos es comunicada a las partes apropiadas.	0,50	
		Los procesos de detección son mejorados continuamente.	0,50	

Fuente: Elaboración propia, 2018.

Tabla 39. Resultados proceso responder

Subproceso	Objetivo de control	Controles	Prom. control	Prom. Subproceso
Planear la respuesta	Los procesos y procedimientos de respuesta se ejecutan y mantienen, para asegurar la respuesta.	El plan de respuesta es ejecutado durante o después de un incidente.	0,68	0,68
Comunicación	Las actividades de respuesta son coordinadas con los interesados internos y externos.	El personal conoce sus roles y orden de operaciones cuando una respuesta es necesaria.	0,50	0,30
		Los incidentes son reportados consistentemente con criterios establecidos.	0,50	
		La información es consistentemente compartida con los planes de respuesta.	0,00	

Subproceso	Objetivo de control	Controles	Prom. control	Prom. Subproceso
Comunicación	Las actividades de respuesta son coordinadas con los interesados internos y externos.	La coordinación con los interesados ocurre con planes de respuestas consistentes.	0,50	
		Intercambio voluntario de información ocurre con los interesados externos para alcanzar una más amplia conciencia en ciberseguridad.	0,00	
Análisis	El análisis es realizado para asegurar efectiva respuesta y soporte a las actividades de recuperación.	Las notificaciones de los sistemas de detección se investigan.	0,50	0,34
		El impacto de los incidentes es entendido.	0,68	
		Análisis forense son ejecutados.	0,00	
		Los incidentes son categorizados consistentemente con los planes de respuesta.	0,50	
		Los procesos son establecidos para recibir, analizar y responder a las vulnerabilidades divulgadas desde fuentes internas y externas.	0,00	
Mitigación	Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y resolver el incidente.	Los incidentes son contenidos	0,50	0,68
		Los incidentes son mitigados.	0,68	
		Las vulnerabilidades identificadas se mitigan o documentan como riesgos aceptados.	0,85	
Mejoras	Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta.	Los planes de respuesta incorporan lecciones aprendidas	0,50	0,25
		Las estrategias de respuesta son actualizadas.	0,00	

Fuente: Elaboración propia, 2018.

Nota biográfica

Luis Fernando Mendoza Silva

Nació en Lina el 14 de febrero de 1962. Titulado en Ingeniería Mecánica por la Universidad Nacional de Ingeniería. Está certificado como auditor líder en la norma ISO 20000; asimismo, cuenta con la acreditación CISA (Certified Information Systems Auditor) de ISACA y es asesor certificado de COBIT 5. De otro lado, cuenta con más de diez años de experiencia en auditoría de procesos gestión en tecnologías de la información. Actualmente, desempeña el cargo de Subgerente en la empresa Gestión de Servicios Compartidos S.A.C.

Giancarlo Roberto Vega Gallegos

Nació en Lima el 2 de febrero de 1982. Contador público colegiado de la Universidad de Lima. Asimismo, cuenta con un posgrado en Administración y Dirección Estratégica de la Universidad Peruana de Ciencias Aplicadas (UPC). De otro lado, cuenta con más de 12 años de experiencia profesional; se ha especializado en auditoría externa e interna, procesos, gestión de riesgos, control interno y buen gobierno corporativo. En los últimos 5 años, ha liderado la división de auditoría interna de importantes empresas del sector pesca y agroindustrial.