UNIVERSIDAD DEL BÍO-BÍO

FACULTAD DE CIENCIAS EMPRESARIALES

DEPARTAMENTO DE INFORMÁTICA

DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE DATOS DEL BANCOESTADO CONTACTO 24 HORAS LOTA S.A. BASADO EN LA METODOLOGÍA DE TRABAJO CICLO DEMING/PDCA

PROYECTO PARA OPTAR AL TÍTULO DE INGENIERO CIVIL EN INFORMÁTICA

Fabián Salazar Galleguillos

Profesor guía: Oscar Gericke

07 de mayo de 2018

Concepción – Chile

ÍNDICE

Índice tablas

Índice figuras

1 Introducción

BancoEstado Contacto 24 horas S.A es una filial del Banco del Estado de Chile, cuya función es entregar un servicio no presencial, con cobertura nacional e internacional utilizando la vía telefónica e internet, es decir un call center o centro de contacto.

Algunos de los servicios que entrega este centro de contacto son: la captación de clientes, entrega de información de productos o servicios, aviso de vencimiento de obligaciones, telemarketing, asistencia técnica, actualización de datos, estudios de opinión y satisfacción de clientes además de tracking publicitario, la promoción de campañas, servicios de ayuda a los ejecutivos, ofrecimiento de créditos de consumo, créditos hipotecarios, seguros, tarjetas de crédito y atención de preventa y postventa a los clientes de los segmentos de Personas, Micro empresarios y Pequeños empresarios, entre otros.

En esta organización el área de datos posee una gran responsabilidad, debido a que, los datos que se manipulan, no son cualquier tipo de información, sino que, es información bancaria, que para el centro de contacto es de gran relevancia, porque contiene datos sensibles sobre los clientes del Banco del Estado de Chile, por lo tanto, es muy importante para esta empresa velar por la confidencialidad, disponibilidad e integridad de la información.

Por lo anteriormente mencionado, germinó la idea de diseñar un modelo de gestión de la seguridad de la información basada en la metodología de trabajo llamada ciclo deming/PDCA[1], y de esta manera, poder gestionar los riesgos permitiendo al equipo de seguridad de la información tener un soporte sólido para sustentar ante gerencia un plan de inversión en seguridad de la información, donde con evidencias y cálculos de los impactos que se pueden presentar ante la materialización de un incidente, es posible presentar de forma clara, las posibles soluciones para la mitigación correctiva, preventiva o detectiva de estos eventos no deseados, y de esta forma, garantizar que la inversión cubra las brechas de seguridad más importantes y otorgue una medición de la eficacia de sus controles.

A continuación se presentará de manera concisa los capítulos que componen este proyecto.

El primer capítulo es la introducción del proyecto.

El segundo capítulo es la definición de la empresa donde se diseñará el modelo de gestión de la seguridad de la información.

El tercer capítulo es la definición de este proyecto, se define a través de sus objetivos generales, objetivos específicos, y por último, la justificación del por qué implementar el proyecto en la organización.

[1] Las siglas PDCA vienen de su abreviatura en ingles Plan, Do, Check y Act. Estas siglas representan las cuatro etapas de esta metodología, en español estas etapas se llaman: Planear, Hacer, Verificar Y Actuar.

El cuarto capítulo es el marco teórico, el cual contiene la información clave para facilitar la comprensión de la metodología de trabajo utilizada llamada ciclo deming/PDCA, también de la normativa Nch-ISO27001 y el fundamento teórico del diseño del modelo de gestión seguridad de la información.

El quinto capítulo es la definición de las actividades realizadas en cada etapa de la metodología de trabajo llamada ciclo Deming/PDCA (Plan/planificar, Do/Hacer, Check/Verificar, Act/Actuar).

El sexto capítulo es donde se presenta el desarrollo del modelo de gestión de seguridad de la información propuesto en el centro de contacto.

En el séptimo capítulo se presenta un estudio de factibilidad técnica, operativa y económica de dos situaciones (caso real y caso hipotético), también una conclusión del estudio realizado.

En el octavo capítulo se encuentra la conclusión de este proyecto.

Por último, se encuentra toda la bibliografía utilizada.

Antes de continuar, es importante mencionar que por razones administrativas este proyecto no abarcará en su totalidad la normativa Nch-ISO27001, pero sí contará con las actividades más importantes para la administración del centro de contacto.

Dentro de las actividades definidas en conjunto al sub-gerente de planificación y control del centro de contacto se encuentra, la definición de alcance del modelo de gestión de seguridad de la información, el inventario de activos de información del área de datos, análisis de riesgo, tratamiento de las amenazas aplicando controles recomendados por la normativa y la definición de un indicador que nos expresara la efectividad del modelo de gestión de seguridad de la información.

2 Descripción de la empresa

2.1 Antecedentes generales de la Empresa

Nombre: BancoEstado Contacto 24horas S.A.

Dirección: Avda. El Parque 179, Región del Bío Bío, Lota.

Rubro: Instituciones Bancarias.

Principales productos y/o servicios que ofrece: Promoción de campañas, servicios de ayuda a los ejecutivos, ofrecimiento de créditos de consumo, créditos hipotecarios, seguros, tarjetas de crédito y atención de preventa y postventa a los clientes de los segmentos de Personas, Micro empresarios y Pequeños empresarios.

2.2 Descripción Contexto

A continuación se describe los principales aspectos de BancoEstado Contacto 24horas S.A (BEC24H) y del Área Problema, el recurso humano que lo compone y las funciones más relevantes.

2.2.1 Descripción Banco Estado Contacto 24 horas S.A (BEC24H)

Este capítulo es elaborado a partir de página web de la corporación BancoEstado (Corporativo.bancoestado.cl, 2017) y reuniones con el sub-gerente de planificación y control Javier Painén Painén, abril 2017.

Banco del Estado de Chile es la institución bancaria que atiende al mayor número de personas a lo largo del territorio nacional, consolidándose como la entidad bancaria con la red más extensa del país, compuesta de sucursales, cajeros automáticos, dispensadoras de saldos, buzoneras, sucursales de ServiEstado y puntos de atención Caja Vecina.

La misión del banco estado es "*Existimos para que Chile sea un país más inclusivo, equitativo y con oportunidades que lleguen a todos.*" (BancoEstado, 2017). Por lo mismo el banco ha tenido que incurrir en la participación de sociedades quienes actualmente le prestan servicios que facilitan el cumplimiento de sus metas. De esta forma, se agrega a la red BancoEstado otras filiales como son:

- BancoEstado S.A. Administradora General de Fondos.
- BancoEstado Centro de Servicios S.A.
- BancoEstado Contacto 24 horas S.A.
- BancoEstado S.A. Corredores de Bolsa.
- BancoEstado Corredores de Seguros S.A.
- BancoEstado Microempresa S.A. Asesorías Financieras.
- BancoEstado Servicio de Cobranzas S.A.
- Red Global S.A.

- Sociedad de Servicios Transaccionales Caja Vecina S.A.

La fuerte competencia que se vive en el sector bancario, impulsó la búsqueda de nuevas estrategias de competencias, que sean capaces de entregar una ventaja competitiva para las distintas instituciones bancarias. Bajo este enfoque, tomó gran importancia para el banco la idea de mejorar la calidad en el servicio a sus clientes, para ello, se pensó en poner a disposición de sus clientes un servicio de atención y ayuda a distancia que les permitiera realizar actividades referentes al banco, pero sin la necesidad de estar presentes físicamente en alguna filial o sucursal. La situación anterior determinó la creación de la sociedad BancoEstado Contacto 24 Horas S.A., cuya función es proveer al Banco del Estado de Chile un servicio no presencial, con cobertura nacional e internacional utilizando la vía telefónica e internet, es decir un centro de contacto.

La prestación de servicios incluye la captación de clientes, entrega de información de productos o servicios, aviso de vencimiento de obligaciones, telemarketing, asistencia técnica, actualización de datos, estudios de opinión y satisfacción de clientes además de tracking publicitario.

Por otro lado el Centro de contacto cumple un rol fundamental en la promoción de campañas, servicios de ayuda a los ejecutivos, ofrecimiento de créditos de consumo, créditos hipotecarios, seguros, tarjetas de crédito y atención de preventa y postventa a los clientes de los segmentos de Personas, Micro empresarios y Pequeños empresarios, entre otros. La misión del centro de contacto se puede enumerar como sigue:

1) Satisfacer las necesidades de BancoEstado, desarrollando y manteniendo, en su representación, relaciones comerciales y de servicio, en forma no presencial, con sus clientes y usuarios. Funciona como empresa filial de la Corporación BancoEstado, ofreciendo un servicio cobertura nacional e internacional de información a sus clientes vía telefónica e internet. Es una organización autónoma que funciona bajo la figura de una sociedad de apoyo al giro de esta entidad bancaria, y que está bajo la regulación de la Superintendencia de Bancos e Instituciones Financieras de Chile.

2) Apoyar a BancoEstado en su relación con sus clientes de manera no presencial, de tal forma, que estos cuenten en cualquier momento y durante las 24 horas del día, con la información que soliciten, sin necesidad de acercarse en forma presencial a una sucursal y sin importar el lugar dónde se encuentren.

3) En el año 2000 previniendo la necesidad de mantener un contacto personalizado con sus clientes, dado el alto volumen de consultas y transacciones electrónicas y en posesión de una base de clientes afín al uso del teléfono, ve la necesidad de dar acceso a los servicios BancoEstado a la mayor parte de la población y considera importante dar soporte a los otros canales de distribución.

Para lo anterior, se proyecta instalar un Centro de Contacto, lo cual se conjuga con la preocupación social del gobierno de la época producto del cierre de las minas de carbón de la octava región, lo que incentiva aún más a hacer realidad este proyecto en la comuna de Lota donde permanece ya desde hace 16 años.

De esta manera, el centro de contacto del Banco Estado se convierte en pionera de su género, constituyendo un ejemplo de descentralización de iniciativas empresariales del país.

Esta filial, integra soporte dirigido a clientes BancoEstado en el ámbito de la Plataforma Comercial y Servicio al Cliente. En el año 2001 partió con 59 trabajadores, sin embargo, hoy supera el millar de personas, posicionándose y validándose como un canal no presencial de ventas, pre-ventas y post-ventas que ha logrado adecuarse a los requerimientos de la industria y su cliente. Además la dotación de recurso humano ha permitido cumplir con su compromiso social manteniendo una constante oportunidad de trabajo para los habitantes de la zona.

La misión del centro de contacto es *"Entregar Soluciones a los Usuarios y Clientes de BancoEstado con interacciones oportunas de Excelencia y Calidad, contribuyendo al crecimiento y consolidación de éste, en el mercado Financiero Nacional."* (BancoEstado Contacto 24horas, 2017).

Hoy en día la estructura organizacional se describe en la Figura Nº1.

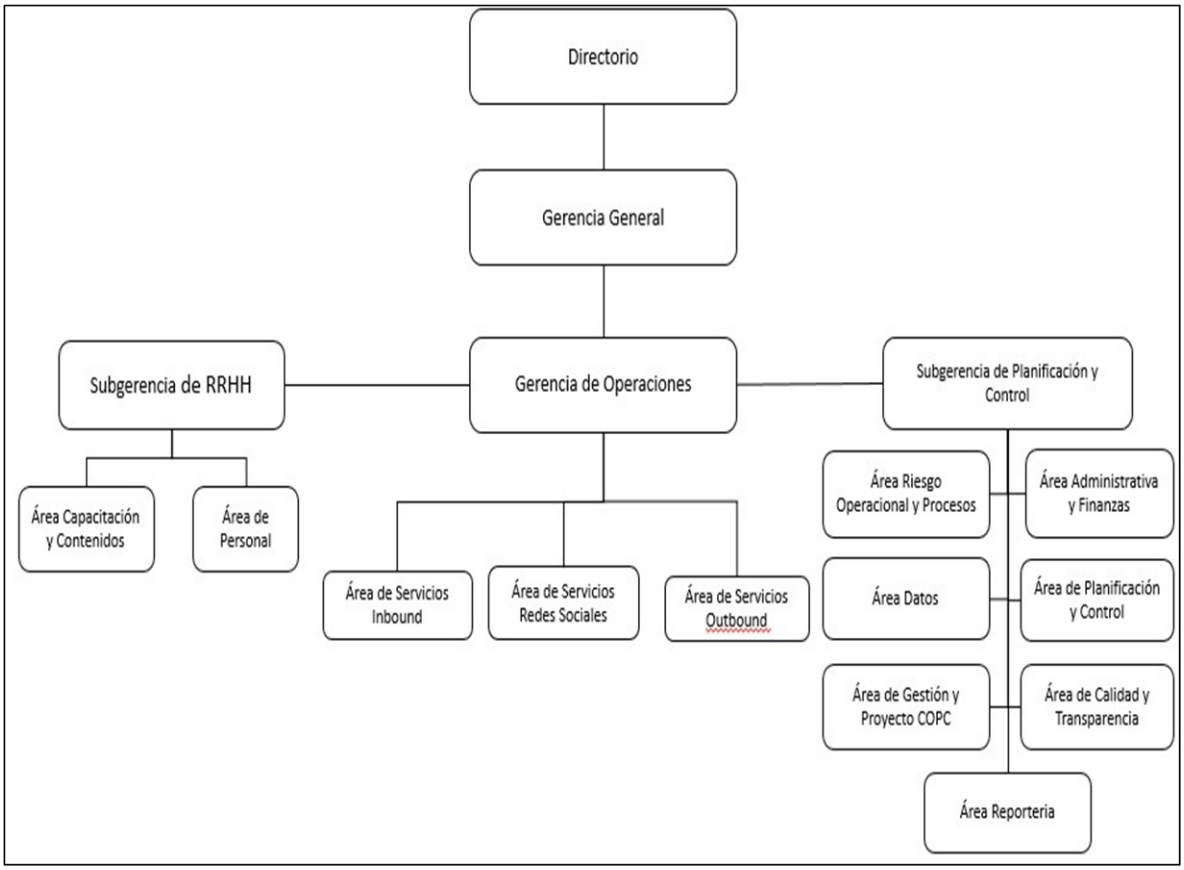


Figura 1: ***Organigrama BEC24H***

Fuente: Elaboración propia a partir de una reunión con el sub-gerente de planificación y control del centro de contacto, Abril 2017.

2.2.2 Descripción del Área Problema

El Área de Datos pertenece a la Sub-Gerencia de Planificación y Control, esta Área apunta a la centralización sistemática de datos provenientes de las distintas áreas de BancoEstado Contacto 24 Horas S.A. con el fin de poder establecer indicadores acordes a cada una de las unidades, que les permita ver la situación de sus procesos internos, administrar los recursos necesarios para prevenir y cumplir realmente con los pedidos de los clientes o determinar la existencia de desviaciones entre lo planificado y lo obtenido, con tal de optimizar los cuellos de botella que limitan la gestión.

El Área cumple con una labor fundamental dentro del Centro de Contacto, debido a que en esta Área es donde se centra gran parte de la información de la empresa, y a su vez información que representa un valor importante en los procesos claves de BancoEstado Contacto 24 Horas.

El recurso humano del área cumple un rol fundamental, este está compuesto por un equipo de seis personas.

- Cinco Analistas de Datos
- Un Coordinador

Este equipo está liderado por un coordinador el cual está encargado de planificar, organizar, dirigir y controlar las tareas de cada uno de los trabajadores que pertenecen al área de datos, además de comunicar los lineamientos estratégicos, impuestos por el mandante o por la gerencia de BancoEstado Contacto 24 Horas al equipo de trabajo, así como también definir lineamientos propios que estructurarán cómo se trabajará dentro del área. Por otra parte, el equipo de cinco analistas de datos trabaja en conjunto aplicando las mejores prácticas de la ingeniería en el diseño de bases de datos, desarrollo de componentes, administración de bases de datos, desarrollo y dirección de sistemas, todo esto con el fin de apoyar la gestión del centro de contacto; manteniendo información fidedigna, oportuna y actualizada.

2.3 Descripción de la problemática

Dada la importancia del área, descrita en el apartado anterior, y al constatar, que el centro de contacto no posee un modelo de gestión de seguridad de la información, y también, verificar empíricamente que el único recurso para verificar que realmente sus datos no pueden ser vulnerados por intrusión de agentes externos o cualquier otro tipo de amenazas, es la confianza depositada en la adquisición de servidores de Entel[2], en el que el proveedor le asegura dentro del contrato, velar por la seguridad de su información mediante certificaciones obtenidas, aplicación de firewall[3] y con la realización de copias de seguridad de sus datos cada 48 horas sin poder optar a registros históricos, donde eventualmente, pudiesen buscar versiones anteriores.

Cabe destacar que en estos servidores es donde la organización contiene el corazón de sus aplicativos que apoyan la gestión del centro de contacto, y además bases de datos importantes para el funcionamiento de los procesos del centro de contacto.

Entonces, como el lineamiento del centro de contacto es velar por la confidencialidad, integridad y disponibilidad de la información bancaria de su millar de clientes y al constatar que el área problema no posee ningún tipo plan de acción definido en caso de la materialización de una amenaza a la información, se genera la necesidad de diseñar un modelo de gestión de seguridad de la información basado en la metodología de trabajo ciclo deming o PDCA para poder gestionar de manera correcta los riesgos que hay en la materialización de una amenaza a la información bancaria de los clientes.

[2] Proveedor de los servidores del centro de contacto.

[3] "Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad"(Cisco.com, 2017)

3 Definición del Proyecto

3.1 Objetivo general

Diseñar un Modelo de Gestión de Seguridad de la Información en el Área de Datos para el Centro de Contacto Lota Banco Estado basado en la metodología de trabajo ciclo deming / PDCA (Planificar, Hacer, Verificar y Actuar).

3.2 Objetivos específicos

- Analizar la metodología de trabajo ciclo deming o PDCA.
- Analizar los procesos generales ventas del Centro de Contacto Lota Banco Estado de forma empírica y los controles del área de datos.
- Diseñar el modelo de gestión de seguridad de la información.
- Ejecutar las actividades del modelo de gestión de seguridad de la información propuesto.

Siglas

ISO: International Organization for Standardization (Organización Internacional de Normalización).

NCH: Norma Chilena.

BEC24H: BancoEstado Contacto 24 horas S.A

ANEXO A: ”El Anexo A suele ser utilizado como una referencia para la implementación de medidas de protección de la información, así como para comprobar que no se están dejando de lado medidas de seguridad necesarias que no habían sido consideradas dentro de una organización.” (Mendoza, M., 2015).

Ciclo PDCA: Es una metodología de trabajo que consta de 4 etapas: Plan (Planificar), Do (Hacer), Check (Verificar), Act (Actuar). Con el fin de crear un Plan de mejora continua.

3.3 Justificación del proyecto

Fuente: elaboración propia, abril 2017

Cuando se trata de información bancaria, podemos deducir inmediatamente que dicha información tiene una alta valoración para la organización, por ende, es sumamente relevante para la organización velar por la confidencialidad, disponibilidad e integridad de la información, de esta manera, lograr diseñar un modelo de gestión de seguridad con el cual se sabrá cómo reaccionar en caso de que se materialice una amenaza.

También se debe mencionar que la información es crucial para la toma de decisiones dentro de una organización, tener en consideración que el centro de contacto BancoEstado utiliza y posee información relevante y confidencial, por lo tanto, es necesario gestionar de manera correcta los riesgos.

Como beneficio se puede recalcar que al gestionar incidentes permite al equipo de seguridad de la información tener un soporte sólido para sustentar ante gerencia un plan de inversión en seguridad de la información, donde con evidencias y cálculos de los impactos que se pueden presentar ante la materialización de un incidente, es posible presentar de forma clara las posibles soluciones para la mitigación correctiva, preventiva o detectiva de estos eventos no deseados, y de esta forma poder garantizar que la inversión cubra las brechas de seguridad más importantes para la gerencia, y también realizar una medición de la eficacia de los controles.

Otra de las ventajas que se tiene al gestionar incidentes son las evidencias, lo cual para casos de fraudes internos o externos permite entregar al área legal una prueba válida ante un posible proceso administrativo interno o judicial, para lo cual es conveniente que esta recopilación de evidencias se realicen cumpliendo las normas legales para este procedimiento

El modelo de gestión de seguridad de la información a diseñar se puede aplicar dentro del centro de contacto BancoEstado 24 horas sin impactar a los demás sistemas que participan dentro de la organización, debido a que, este modelo de gestión de seguridad de la información es basado en la metodología de trabajo llamado ciclo deming o PDCA que es un ciclo iterativo de mejora continua, lo que significa que los sistemas que se encuentran en la organización experimentarán una mejora significativa y continua en la confidencialidad, integridad y disponibilidad de la información, por lo tanto, generará beneficios dentro de la organización en temas de la Seguridad de la Información.

4 Marco Teórico

4.1 Ciclo Deming/PDCA

4.1.1 Descripción de la metodología

A partir del foro web maestros de la calidad (maestros de la calidad, 2012).

Esta metodología se hizo conocida por el Dr. Edwards Deming ingeniero en eléctrica en la Universidad de Wyoming, en 1925 obtuvo la maestría en física y matemáticas en la Universidad de Colorado, finalmente en 1928 obtuvo el doctorado en física en la Universidad de Yale donde fue contratado como profesor.

> "*El prestigio de Deming está muy relacionado con el éxito de la industria japonesa, del cual es considerado en gran parte responsable. Con sus elocuentes conferencias en 1950 a los líderes empresariales japoneses, logró un cambio en su mentalidad administrativa y los convenció de que la calidad era un arma estratégica. Con argumentos contundentes demostraba los altos costos en que una empresa incurre cuando no tiene un proceso planeado para administrar su calidad, el desperdicio de materiales y productos rechazados, el costo de trabajar dos o más veces los productos para eliminarles defectos, o las reposiciones y compensaciones pagadas a los clientes por las fallas en los mismos*."

El ciclo Deming también llamado espiral de mejora continua o ciclo de calidad, es basado en un concepto ideado por Walter A. Shewhart[4], y se utiliza para estructurar y ejecutar planes de mejora de calidad a cualquier nivel ejecutivo u operativo.

Este ciclo consta de cuatro pasos o etapas:

- **Planificar:** Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar, también se desarrolla de manera objetiva y profunda un plan. Se auto formulan preguntas como, ¿Qué hacer?, ¿Cómo hacerlo?
- **Hacer:** Se comprueba en pequeña escala o sobre la base de ensayo como ha sido planeado hacer lo planificado, también se realizan los cambios necesarios para implantar la mejora propuesta.
- **Verificar:** se supervisa si se obtuvieron los efectos esperados y la magnitud de los mismos. De esta forma se verifican si los sucesos ocurrieron según lo planificado.
- **Actuar:** se actúa en consecuencia, ya sea generalizando el plan si dio resultados y tomando medidas preventivas para que la mejora no sea reversible, o reestructurando el plan debido a que los resultados no fueron

[4] Walter Andrew Shewhart (18 de marzo de 1891 - 11 de marzo de 1967) fue un físico, ingeniero y estadístico estadounidense, conocido como el padre del control estadístico de la calidad. (Calidad total, 2012)

satisfactorios, con lo que se vuelve a iniciar el ciclo. Se auto formulan preguntas como, ¿Cómo mejorar la próxima vez?

Esta metodología se basa en catorce principios:

1) Crear constancia en la mejora de productos y servicios, con el objetivo de ser competitivo y mantenerse en el negocio, además proporcionar puestos de trabajo.

2) Adoptar una nueva filosofía de cooperación en la cual todos se benefician, y ponerla en práctica enseñándola a los empleados, clientes y proveedores.

3) Desistir de la dependencia en la inspección en masa para lograr calidad. En lugar de esto, mejorar el proceso e incluir calidad en el producto desde el comienzo.

4) Terminar con la práctica de comprar a los más bajos precios. En lugar de esto, minimizar el costo total en el largo plazo. Buscar tener un solo proveedor para cada ítem, basándose en una relación de largo plazo de lealtad y confianza.

5) Mejorar constantemente y por siempre los sistemas de producción, servicio y planeamiento de cualquier actividad. Esto va a mejorar la calidad y la productividad, bajando los costos constantemente.

6) Establecer entrenamiento dentro del trabajo (capacitación).

7) Establecer líderes, reconociendo sus diferentes habilidades, capacidades y aspiraciones. El objetivo de la supervisión debería ayudar a la gente, máquinas y dispositivos a realizar su trabajo.

8) Eliminar el miedo y construir confianza, de esta manera todos podrán trabajar más eficientemente.

9) Borrar las barreras entre los departamentos. Abolir la competición y construir un sistema de cooperación basado en el mutuo beneficio que abarque toda la organización.

10) Eliminar eslóganes, exhortaciones y metas pidiendo cero defectos o nuevos niveles de productividad. Estas exhortaciones solo crean relaciones de rivalidad, la principal causa de la baja calidad y la baja productividad reside en el sistema y este va más allá del poder de la fuerza de trabajo.

11) Eliminar cuotas numéricas y la gestión por objetivos.

12) Remover barreras para apreciar la mano de obra y los elementos que privan a la gente de la alegría en su trabajo. Esto incluye eliminar las evaluaciones anuales o el sistema de méritos que da rangos a la gente y crean competición y conflictos.

13) Instituir un programa vigoroso de educación y auto mejora.

14) Poner a todos en la compañía a trabajar para llevar a cabo la transformación. La transformación es trabajo de todos.

El doctor Edwards Deming enfatizó que existen siete enfermedades que se contraponen a la búsqueda de la calidad, estas son:

1) Falta de constancia en los propósitos.
2) Énfasis en las ganancias a corto plazo y los dividendos inmediatos.
3) Evaluación por rendimiento, clasificación de méritos o revisión anual de resultados.
4) Movilidad de ejecutivos
5) Gerencia de la compañía basándose solamente en las cifras visibles.
6) Costos médicos excesivos.
7) Costo excesivo de garantías.

4.2 Normativa Nch- ISO 27001

4.2.1 Descripción de la normativa

El Instituto Nacional de Normalización describe lo siguiente sobre el modelo de gestión de seguridad de la información (Instituto Nacional de Normalización, 2013, p.3),

> "*La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma."*

Esto significa que se deja de operar de una manera intuitiva y se comienza a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización.

4.2.2 Anexo A

El Instituto Nacional de Normalización describe lo siguiente sobre el Anexo A de la Nch-ISO27001 (Instituto Nacional de Normalización, 2013, pp. 13-27).

Anexo A
(Normativo)
Objetivos de control de referencia y controles

A.5 Políticas de seguridad de la información		
A.5.1 Orientación de la dirección para la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	Control La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Control Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	Control Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.
A.6.1.3	Contacto con autoridades	Control Se deben mantener los contactos apropiados con las autoridades pertinentes
A.6.1.4	Contacto con grupos especiales de interés	Control Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.

A.6.1.5	Seguridad de la información en la gestión de proyecto	Control Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.
A.6.2 Dispositivos móviles y trabajo remoto		
Objetivo: Garantizar la seguridad del trabajo remoto y uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Control Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles
A.6.2.2	Trabajo remoto	Control Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.
A.7 Seguridad ligada a los recursos humanos		
A.7.1 Previo al empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados		
A.7.1.1	Selección	Control Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.
A.7.1.2	Términos y condiciones de la relación laboral	Control Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Responsabilidades de la dirección	Control La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Concientización, educación y formación	Control Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben

	en seguridad de la información	recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales pertinentes para su función laboral.
A.7.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información.
A.7.3 Desvinculación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.		
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	Control Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral.
A.8 Administración de activos		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.		
A.8.1.1	Inventario de activos	Control Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.
A.8.1.2	Propiedad de los activos	Control Los activos que se mantienen en inventario deben pertenecer a un dueño.
A.8.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.

A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.		
A.8.2.1	Clasificación de la información	Control La información debe ser clasificada en términos de requisitos legales, valor criticidad y sensibilidad para la divulgación o modificación sin autorización.
A.8.2.2	Etiquetado de la información	Control Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Control Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.8.3 Manejo de los medios		
Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.		
A.8.3.1	Gestión de los medios removibles	Control Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de los medios	Control Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.
A.8.3.3	Transferencia física de medios	Control Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.
A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basadas en los

		requisitos del negocio y de seguridad de la información.
A.9.1.2	Accesos a las redes y a los servicios de la red	Control Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.
A.9.2 Gestión de acceso del usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.		
A.9.2.1	Política de control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información.
A.9.2.2	Accesos a las redes y a los servicios de la red	Control Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.
A.9.2.3	Gestión de derechos de acceso privilegiados	Control Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Control Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuario	Control Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Control Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	Control Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.

A.9.4 Control de acceso al sistema y aplicaciones		
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	Control Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.
A.9.4.2	Procedimientos de inicio de sesión seguro	Control Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de claves	Control Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.
A.11 Seguridad física y del ambiente		
A.11.1 Áreas seguras		
Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.		
A.11.1.1	Perímetro de seguridad física	Control Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen

		ya sea información sensible o crítica y las instalaciones de procesamiento de información.
A.11.1.2	Controles de acceso físico	Control Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, salas e instalaciones	Control Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones.
A.11.1.4	Protección contra amenazas externas y del medio ambiente	Control Se debe diseñar y aplicarla protección física contra daños por desastre natural, ataque malicioso o accidentes.
A.11.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar procedimientos para trabajar en áreas seguras.
A.11.1.6	Áreas de entrega y carga	Control Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
A.11.2 Equipamiento		
Objetivo: Prevenir perdidas, daños, hurtos o el compromiso de los activos así como la interrupción de las actividades de la organización.		
A.11.2.1	Ubicación y protección del equipamiento	Control El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.
A.11.2.2	Elementos de soporte	Control Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.
A.11.2.3	Seguridad en el cableado	Control Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información contra interceptación, interferencia o daños.

A.11.2.4	Mantenimiento del equipamiento	Control El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.
A.11.2.5	Retiro de activos	Control El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización.
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	Control Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Seguridad en la reutilización o descarte de equipos	Control Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización.
A.11.2.8	Equipo de usuario desatendido	Control Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escrito y pantalla limpios	Control Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12 Seguridad de las operaciones		
A.12.1 procedimientos operacionales y responsabilidades		
Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	Control Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información

		y los sistemas que afecten la seguridad de la información.
A.12.1.3	Gestión de la capacidad	Control Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales	Control Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.
A.12.2 Protección contra código malicioso		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.		
A.12.2.1	Controles contra código malicioso	Control Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.
A.12.3 Respaldo		
Objetivo: Proteger en contra de la perdida de datos.		
A.12.3.1	Respaldo de la información	Control Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.
A.12.4 Registro y monitoreo		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de evento	Control Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registros	Control Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.
A.12.4.3	Registros del administrador y el operador	Control

		Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	Control Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia.
A.12.5 Control del software de operación		
Objetivo: Asegurar la integridad de los sistemas operacionales.		
A.12.5.1	Instalaciones del software en sistemas operacionales	Control Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	Control Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
A.12.7 Consideraciones de la auditoría de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.		
A.12.7.1	Controles de auditoria de sistemas de información	Control Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.		
A.13.1.1	Controles de red	Control

		Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.
A.13.1.3	Separación en la redes	Control Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	Control Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.
A.13.2.2	Acuerdos sobre transferencia de información	Control Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.
A.13.2.3	Mensajería electrónica	Control La información involucrada en la mensajería electrónica debe ser debidamente protegida.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Control Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdo de no divulgación que reflejan las necesidades de protección de la información de la organización.
A.14 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.		

A.14.1.1	Análisis y especificación de requisitos de seguridad de información	Control Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicación en redes	Control La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales y su divulgación y modificación no autorizada.
A.14.1.3	Protección de las transacciones de servicios de aplicación	Control La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.
A.14.2 Seguridad de procesos de desarrollo y soporte		
Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	Control Las reglas para el desarrollo de software y de sistema deben ser establecidas y aplicadas a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios del sistema	Control Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	Control Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.

A.14.2.5	Principios de ingeniería de sistema seguro	Control Se debe establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación de sistema de información.
A.14.2.6	Entorno de desarrollo seguro	Control Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.
A.14.2.7	Desarrollo tercerizado	Control La organización debe supervisar y monitorear la actividad del desarrollo de sistema tercerizado.
A.14.2.8	Prueba de seguridad del sistema	Control Durante el desarrollo se debe realizar la prueba de funciona
A.14.2.9	Prueba de aprobación del sistema	Control Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para prueba.		
A.14.3.1	Protección de datos de prueba	Control Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa.
A.15 Relaciones con el proveedor		
A.15.1 Seguridad de la información en las relaciones con el proveedor		
Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	Control Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de proveedor a los activos de la organización.
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	Control Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar almacenar, comunicar o

		proporcionar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	Control Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministro del producto.
A.15.2 Gestión de entrega del servicio del proveedor		
Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos de proveedor.		
A.15.2.1	Supervisión y revisión de los servicios de proveedor	Control Las organizaciones deben supervisar, revisar y auditar la entrega del servicio del proveedor.
A.15.2.2	Gestión de cambios a los servicios del proveedor	Control Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	Control Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.
A.16.1.2	Informe de eventos de seguridad de la información	Control Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.
A.16.1.3	Informe de las debilidades de seguridad de la información	Control Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de

		la información en los sistemas o servicios, observada o que se sospeche.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Control Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información.
A.16.1.5	Respuesta ante incidentes de seguridad de la información	Control Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control Se deben utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	Control La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
A.17.1 continuidad de la seguridad de la información		
Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	Control La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad.

A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Control Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento con los requisitos legales y contractuales		
Objetivo: Evitar incumplimiento de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Control Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	Control Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y al uso de productos de software patentados.
A.18.1.3	Protección de los registros	Control Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de la información de identificación personal	Control Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.
A.18.1.5	Regulación de los controles criptográficos	Control Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones pertinentes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.		

A.18.2.1	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.
A.18.2.3	Verificación del cumplimiento técnico	Control Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.

Tabla 1: ***Anexo A Nch-ISO27001***

4.2.3 Anexo nº4: Controles de normas específicas de seguridad para la mitigación de riesgos

A partir de un documento interno del centro de contacto. (Metodología de Gestión de Riesgo Tecnológico, 2017, pp. 49 -57).

Anexo nº4: Controles de Normas específicas de Seguridad de la información

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE01	Organización de la seguridad	1.1	Definición de roles de seguridad	Se busca que la Corporación BancoEstado tenga una definición de los roles asociados a la gestión de la seguridad precisos y actualizados.
NE01	Organización de la seguridad	1.2	Segregación de funciones	Se busca que los usuarios posean accesos segregados a sus funciones, manteniendo el principio de menor privilegio.
NE01	Organización de la seguridad	1.3	Contacto con autoridades y grupos de interés	Se busca que la Corporación BancoEstado mantenga un nivel de contacto adecuado con los organismos reguladores, fuerzas de orden y grupos de interés, de tal manera de poder actuar rápidamente ante un problema relacionado con la seguridad de la información.
NE01	Organización de la seguridad	1.4	Seguridad de la información en la administración de proyectos	Se busca que los aspectos relativos a la seguridad de la información estén presentes en cada uno de los proyectos relevantes de la Corporación BancoEstado
NE02	Seguridad de RRHH	2.1.1	Antes del Empleo - Selección	Se busca que el proceso de selección de personal considere aspectos de seguridad de la información.
NE02	Seguridad de RRHH	2.1.2	Antes del Empleo - Términos y condiciones de empleo	Se busca que los contratos del personal contengan cláusulas de seguridad de la información
NE02	Seguridad de RRHH	2.2.1	Durante el Empleo - Responsabilidades de la dirección	Se busca que la corporación vele por el cumplimiento de las políticas por parte de los usuarios
NE02	Seguridad de RRHH	2.2.2	Durante el Empleo - Concientización y capacitación sobre	Se busca que la corporación BancoEstado esté constantemente ofreciendo

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
			seguridad de la información	capacitaciones de seguridad a sus empleados
NE02	Seguridad de RRHH	2.2.3	Durante el Empleo - Proceso disciplinario	Se busca que la corporación BancoEstado genere sanciones ante incumplimientos de seguridad de la información
NE02	Seguridad de RRHH	2.3	Término de la relación contractual y cambio de empleo	Se busca que existan clausulas en el contrato que resguarden la confidencialidad de la información incluso terminando la relación con el empleador.
NE03	Clasificación y Control de Activos de Información	3.1.1	Responsabilidad sobre los activos - Inventario de activos	Se busca que exista un inventario de activos y esté actualizado
NE03	Clasificación y Control de Activos de Información	3.1.2	Responsabilidad sobre los activos - Propiedad de activos	Se busca que los activos de información tengan asignado un responsable.
NE03	Clasificación y Control de Activos de Información	3.1.3	Responsabilidad sobre los activos - Uso responsable de los activos	Se busca que los usuarios utilicen los activos de manera responsable
NE03	Clasificación y Control de Activos de Información	3.1.4	Responsabilidad sobre los activos - Devolución de activos	Se busca que los usuarios hagan devolución de los activos de información una vez terminado el empleo
NE03	Clasificación y Control de Activos de Información	3.2.1	Clasificación de la información - Niveles de clasificación de la información	Se busca que la corporación BancoEstado posea niveles de clasificación de activos en cuanto a su integridad, confidencialidad y disponibilidad
NE03	Clasificación y Control de Activos de Información	3.2.2	Clasificación de la información - Etiquetado de información	Se busca que los activos de información posean un etiquetado físico o digital según corresponda, de tal manera de advertir a los usuarios sobre las condiciones de su uso.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE03	Clasificación y Control de Activos de Información	3.2.3	Clasificación de la información - Medidas de protección sobre los activos	Se busca que la Corporación BancoEstado establezca medidas de protección sobre la información sensible
NE04	Control de Acceso	4.1.1	Requisitos para el control de acceso - Lineamientos para el control de acceso	Se busca que existan procedimientos de administración de accesos de usuarios que contengan las autorizaciones correspondientes.
NE04	Control de Acceso	4.1.2	Requisitos para el control de acceso - Control de acceso a redes y control de red	Se busca que la corporación BancoEstado cuente con controles de acceso a la red adecuados
NE04	Control de Acceso	4.2.1	Administración de acceso a los usuarios - Registro y cancelación de registro de usuarios	Se busca que la Corporación BancoEstado mantenga a todo su personal asociado a una cuenta de usuario única
NE04	Control de Acceso	4.2.2	Administración de acceso a los usuarios - Entrega de acceso a los usuarios	Se busca que la asignación de las credenciales a los usuarios esté regulado.
NE04	Control de Acceso	4.2.3	Administración de acceso a los usuarios - Administración de derechos de acceso privilegiado	Se busca que existan controles sobre el uso de las cuentas de altos privilegios
NE04	Control de Acceso	4.2.4	Administración de acceso a los usuarios - Administración de los mecanismos de autenticación de los usuarios	Se busca que los usuarios posean mecanismos de autenticación que garanticen la integridad y confidencialidad de la información.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE04	Control de Acceso	4.2.5	Administración de acceso a los usuarios - Revisión de los derechos de los accesos a usuarios	Se busca que los cambios a los derechos de acceso de los usuarios estén precedidos por un proceso de análisis de riesgo.
NE04	Control de Acceso	4.2.6	Administración de acceso a los usuarios - Eliminación o ajuste de los permisos de usuario	Se busca que exista un procedimiento que asegure la eliminación o bloqueo de usuarios una vez terminado el empleo, y el bloqueo de usuarios en caso de licencias o vacaciones.
NE04	Control de Acceso	4.3	Resguardo de información de autenticación	Se busca que los usuarios mantengan cuidado en el uso de sus claves de usuario.
NE04	Control de Acceso	4.4.1	Control de acceso a sistemas y aplicaciones - Restricción de acceso a la información	Se busca que todos los usuarios tengan un puesto de trabajo acorde a sus funciones
NE04	Control de Acceso	4.4.2	Control de acceso a sistemas y aplicaciones - Procedimientos de inicio de sesión seguro	Se busca que exista un límite de tiempo para una sesión activa.
NE04	Control de Acceso	4.4.3	Control de acceso a sistemas y aplicaciones - Sistema de administración de contraseñas	Se busca que las claves estén protegidas en cuanto a confidencialidad e integridad, además de velar porque los usuarios no compartan sus contraseñas.
NE04	Control de Acceso	4.4.4	Control de acceso a sistemas y aplicaciones - Uso de programas privilegiados	Se busca que el uso de software privilegiado esté restringido.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE04	Control de Acceso	4.4.5	Control de acceso a sistemas y aplicaciones - Control de acceso al código fuente del programa	Se busca garantizar que el acceso a código fuente de los sistemas esté restringido.
NE05	Seguridad Física y Ambiental	5.1.1	Áreas seguras - Perímetro de seguridad física	Se busca que las instalaciones de procesamiento de información confidencial posean protección contra acceso físico no deseado.
NE05	Seguridad Física y Ambiental	5.1.2	Áreas seguras - Controles de entrada física	Se busca que las instalaciones de procesamiento de información confidencial tengan control de acceso físico.
NE05	Seguridad Física y Ambiental	5.1.3	Áreas seguras - Protección de oficinas, salas e instalaciones	Se busca que las oficinas, salas y otras instalaciones menores donde se maneje información confidencial tengan medidas que controlen el acceso a las mismas.
NE05	Seguridad Física y Ambiental	5.1.4	Áreas seguras - Áreas de carga y descarga	Se busca asegurar que las áreas de carga y descarga estén debidamente aisladas y protegidas.
NE05	Seguridad Física y Ambiental	5.2.1	Equipos - Ubicación y protección de equipos	Se busca que el equipamiento esté ubicado en lugares aislados del público
NE05	Seguridad Física y Ambiental	5.2.2	Equipos - Servicios básicos de apoyo	Se busca que los servidores estén protegidos contra fallas eléctricas.
NE05	Seguridad Física y Ambiental	5.2.3	Equipos - Seguridad del cableado	Se busca que el cableado en los centros de datos estén debidamente protegidos contra intercepción
NE05	Seguridad Física y Ambiental	5.2.4	Equipos - Mantenimiento de equipos	Se busca que exista un proceso de mantenimiento regular de los equipos en las salas de servidores.
NE05	Seguridad Física y Ambiental	5.2.5	Equipos - Seguridad de los equipos y los activos fuera de las oficinas	Se busca garantizar que los equipos que salgan de las instalaciones físicas de la Corporación BancoEstado estén debidamente protegidos.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE05	Seguridad Física y Ambiental	5.2.6	Equipos - Eliminación o reutilización segura de los equipos	Se busca garantizar que los equipos que sean dados de baja posean borrado seguro de información
NE05	Seguridad Física y Ambiental	5.2.7	Equipos - Equipos no supervisados por los usuarios	Se busca garantizar que los equipos que estén desatendidos (no utilizados físicamente por usuarios) estén debidamente protegidos.
NE05	Seguridad Física y Ambiental	5.2.8	Equipos - Política de escritorios y pantalla limpios	Se busca asegurar que la información confidencial sea almacenada en un mobiliario seguro
NE06	Seguridad de Operaciones	6.1.1	Procedimientos y responsabilidades operacionales - Procedimientos operativos documentados	Se busca que estén documentados los principales procedimientos de operación (instalación y configuración inicial de servidores, almacenamiento y respaldo de información, monitoreo de sistemas y manejo de incidentes) estén debidamente documentados.
NE06	Seguridad de Operaciones	6.1.2	Procedimientos y responsabilidades operacionales - Administración de cambios	Se busca que todos los cambios relevantes hayan sido previamente autorizados por el comité de cambios.
NE06	Seguridad de Operaciones	6.1.3	Procedimientos y responsabilidades operacionales - Administración de la capacidad	Se busca que la Corporación BancoEstado mantenga un monitoreo constante de la capacidad de sus sistemas y la proyección a futuro de las mismas.
NE06	Seguridad de Operaciones	6.1.4	Procedimientos y responsabilidades operacionales - Separación de entornos de desarrollo, pruebas y operacionales	Se busca que los ambientes de producción, test y desarrollo se encuentren debidamente separados.
NE06	Seguridad de Operaciones	6.2	Protección contra malware	Se busca que la Corporación BancoEstado se encuentre debidamente protegido contra el malware

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE06	Seguridad de Operaciones	6.3	Respaldo de información	Se busca que los activos de información estén debidamente respaldados, al menos para el caso de los servidores.
NE06	Seguridad de Operaciones	6.4.1	Registro y monitoreo - Registro de eventos	Se busca que los sistemas posean log de eventos debidamente configurados.
NE06	Seguridad de Operaciones	6.4.2	Registro y monitoreo - Protección del registro de operación	Se busca que los log de eventos que están siendo registrados estén debidamente protegidos.
NE06	Seguridad de Operaciones	6.4.3	Registro y monitoreo - Registro del administrador y el operador	Se busca que en particular las actividades de cuentas de altos privilegios queden debidamente registradas.
NE06	Seguridad de Operaciones	6.4.4	Registro y monitoreo - Sincronización de relojes	Se busca que los relojes de los servidores tuviesen la misma hora, de tal manera de asegurar que los registros de eventos sean consistentes en cuanto a la hora de los mismos.
NE06	Seguridad de Operaciones	6.5	Instalación y administración de software	Se busca que la instalación de software esté controlada, tanto en la instalación de paquetes como su actualización.
NE06	Seguridad de Operaciones	6.6	Administración de vulnerabilidades	Se busca que la Corporación BancoEstado realice de forma periódica procesos técnicos de análisis de vulnerabilidades.
NE06	Seguridad de Operaciones	6.7	Consideraciones sobre la auditoría de los sistemas de información	Se busca que las labores de auditoría estén debidamente planificadas
NE07	Seguridad de las comunicaciones	7.1.1	Administración de la seguridad de redes - Controles de red	Se busca que los equipos conectados a la red estén debidamente identificados, y que la Corporación BancoEstado posea controles de disponibilidad de redes.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE07	Seguridad de las comunicaciones	7.1.2	Administración de la seguridad de redes - Seguridad de los servicios de redes	Se busca que en la implementación de nuevos servicios de red exista un análisis de seguridad previo, además se busca que las instalaciones de redes inalámbricas estén previamente autorizadas.
NE07	Seguridad de las comunicaciones	7.1.3	Administración de la seguridad de redes - Segregación en las redes	Se busca que las redes de la Corporación BancoEstado estén debidamente segregadas
NE07	Seguridad de las comunicaciones	7.2.1	Transferencia de información - Requisitos para el intercambio de información	Se busca que los acuerdos de transferencia de información entre el Banco y terceros estén debidamente documentados.
NE07	Seguridad de las comunicaciones	7.2.2	Transferencia de información - Mensajería electrónica	Se busca que el personal posea buenas prácticas para el uso de mensajería electrónica
NE07	Seguridad de las comunicaciones	7.2.3	Transferencia de información - Acuerdos de confidencialidad	Se busca que todos los contratos con terceros posean acuerdos de confidencialidad.
NE07	Seguridad de las comunicaciones	7.2.4	Transferencia de información - Dispositivos de almacenamiento masivo	Se busca que la Corporación BancoEstado tenga restringido el uso de dispositivos de almacenamiento masivo. Además se busca que existan procedimientos de baja de dichos dispositivos y buenas prácticas en su uso.
NE07	Seguridad de las comunicaciones	7.2.5	Transferencia de información - Dispositivos móviles	Se busca que la conexión de dispositivos móviles a la red del Banco esté debidamente autorizada por GTEC.
NE07	Seguridad de las comunicaciones	7.3.1	Criptografía - Uso de controles criptográficos	Se busca que la generación de nuevas llaves criptográficas para proteger información venga precedido por un análisis de riesgo
NE07	Seguridad de las comunicaciones	7.3.2	Criptografía - Administración de llaves criptográficas	Se busca que las claves criptográficas estén debidamente protegidas.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.1.1	Requisitos de seguridad de los sistemas de información - Análisis y especificación de los requisitos de seguridad de la información	Se busca que todo proyecto de desarrollo de software tenga consideraciones sobre seguridad de la información
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.1.2	Requisitos de seguridad de los sistemas de información - Protección de información en redes públicas	Se busca que las aplicaciones expuestas a la red consideren técnicas de desarrollo seguro.
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.1.3	Requisitos de seguridad de los sistemas de información - Protección de transacciones en las aplicaciones	Se busca que los sistemas transaccionales posean mecanismos que protejan la integridad y confidencialidad de los datos transferidos.
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.1	Seguridad en los procesos de desarrollo y soporte - Desarrollo seguro	Se busca que todo desarrollo posea consideraciones de desarrollo seguro.
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.2	Seguridad en los procesos de desarrollo y soporte - Control de cambios del sistema	Se busca que todo cambio en el desarrollo del sistema esté aprobado por control de cambios.
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.3	Seguridad en los procesos de desarrollo y soporte - Revisión técnica de las aplicaciones después de los cambios en la plataforma base	Se busca que los cambios relevantes en las plataformas base de la Corporación BancoEstado consideren pruebas funcionales posteriores a los mismos.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.4	Seguridad en los procesos de desarrollo y soporte - Restricciones a los cambios de paquetes de software	Se busca que el acceso a las librerías de software esté debidamente restringido
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.5	Seguridad en los procesos de desarrollo y soporte - Entorno de desarrollo seguro	Se busca que el ambiente de desarrollo esté debidamente protegido
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.6	Seguridad en los procesos de desarrollo y soporte - Desarrollo externalizado	Se busca que exista control sobre las actividades de desarrollo que hayan sido externalizadas, a fin de garantizar que existan consideraciones de seguridad en las mismas.
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.2.7	Seguridad en los procesos de desarrollo y soporte - Pruebas de aceptación y seguridad del sistema	Se busca que los pasos a producción vengan acompañados de un set de pruebas técnicas y funcionales que garanticen su correcto funcionamiento.
NE08	Adquisición, Desarrollo y Mantenimiento de sistemas	8.3	Datos de prueba	Se busca que los datos de prueba utilizados en la fase de test estén debidamente protegidos y que en caso de utilizar datos de producción exista una autorización previa.
NE09	Relación con Terceros	9.1.1	Seguridad de la información en las relaciones con los proveedores - Seguridad de la información en las relaciones con los proveedores	Se busca que en la gestión de proveedores se consideren los requisitos de seguridad de la información.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE09	Relación con Terceros	9.1.2	Seguridad de la información en las relaciones con los proveedores - Abordar la seguridad dentro de los acuerdos con los proveedores	Se busca que los contratos con proveedores posean cláusulas orientadas a garantizar la seguridad de la información.
NE09	Relación con Terceros	9.2.1	Administración de prestación de servicios de proveedores - Monitoreo y revisión de los servicios del proveedor	Se busca que la prestación de servicios por parte de terceros esté debidamente regulada, monitoreada y auditada.
NE09	Relación con Terceros	9.2.2	Administración de prestación de servicios de proveedores - Administración de cambios en los servicios del proveedor	Se busca que los cambios a los servicios consideren una evaluación de riesgos.
NE10	Gestión de Incidentes	10.1.1	Administración de incidentes y mejoras de seguridad en la información - Responsabilidades y procedimientos	Se busca que estén establecidos las responsabilidades y procedimientos de gestión de incidentes.
NE10	Gestión de Incidentes	10.1.2	Administración de incidentes y mejoras de seguridad en la información - Informe de eventos de seguridad de la información	Se busca que los usuarios reporten los incidentes asociados a la seguridad y que existan reportes de gestión asociados a los incidentes ocurridos en el período de análisis.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE10	Gestión de Incidentes	10.1.3	Administración de incidentes y mejoras de seguridad en la información - Respuesta ante incidentes de seguridad de la información	Se busca que exista una respuesta ante los incidentes reportados.
NE10	Gestión de Incidentes	10.1.4	Administración de incidentes y mejoras de seguridad en la información - Aprendizaje de los incidentes de seguridad de la información	Se busca que exista un análisis global de los incidentes ocurridos y se generen planes de mejora continua que permitan minimizar la ocurrencia de incidentes similares.
NE10	Gestión de Incidentes	10.1.5	Administración de incidentes y mejoras de seguridad en la información - Recopilación de evidencia	Se busca que todos los incidentes tengan asociada evidencia que pueda servir para su resolución.
NE11	Gestión de continuidad	11.1	Requisitos para la continuidad del negocio	Se busca que exista cumplimiento de la Política Integral de continuidad del Negocio de BancoEstado.
NE11	Gestión de continuidad	11.2	Disponibilidad de las instalaciones de procesamiento de la información	Se busca que las instalaciones de procesamiento de información posean condiciones de redundancia.
NE12	Cumplimiento Normativo	12.1.1	Cumplimiento con los requisitos legales y contractuales - Derechos de propiedad intelectual	Se busca que la Corporación BancoEstado tenga establecidos procedimientos que permitan garantizar el derecho de propiedad intelectual.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
NE12	Cumplimiento Normativo	12.1.2	Cumplimiento con los requisitos legales y contractuales - Protección de registros	Se busca que la información sobre la cual se tenga que mantener un registro histórico regulado se mantenga durante el plazo mínimo establecido.
NE12	Cumplimiento Normativo	12.1.3	Cumplimiento con los requisitos legales y contractuales - Privacidad y protección de información personal identificable	Se busca que la Corporación BancoEstado mantenga debidamente protegida la privacidad de la información personal de los clientes.
NE12	Cumplimiento Normativo	12.2.1	Revisiones de la seguridad de la información - Revisión independiente de la seguridad en la información	Se busca que las políticas y la gestión de seguridad de la información sean revisadas periódicamente.
NE12	Cumplimiento Normativo	12.2.2	Revisiones de la seguridad de la información - Revisión de cumplimiento técnico	Se busca que las principales aplicaciones tengan una revisión técnica periódica.

Tabla 2: ***Anexo nº4: Controles de Normas Específicas de Seguridad de la Información.***

4.2.4 Comparativa

Luego de realizar un cruce entre la Nch-ISO27001 y los Controles de Normas Específicas de Seguridad, se comprueba que, el anexo nº4: Controles de Normas Específicas de Seguridad de la Metodología de Gestión de Riesgos Tecnológicos del centro de contacto contiene un 90,35% de los controles propuesto por la Nch-ISO27001. Con Respecto al 9,65% restante, el jefe del área de datos del centro de contacto asume el riesgo de no abarcar en un 100% la Nch-ISO27001, debido a que, no es prioridad para la empresa conseguir la certificación inmediata de la Nch-ISO27001 en el 2017, porque los recursos están destinados a otros proyectos internos del centro de contacto BancoEstado Lota.

El cruce realizado es el siguiente:

Controles del anexo "A" de la nch27001:2013 que NO ESTÁN en el Anexo nº4: Controles de normas específicas de seguridad del centro de contacto BancoEstado.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
A.5	Política para la seguridad de la información	A.5.1.1	Políticas para la seguridad de la información	La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.
A.5	Política para la seguridad de la información	A.5.1.2	Revisión de las políticas de seguridad de la información	Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continúas.
A.6.2	Dispositivos Móviles y Trabajo remoto	A.6.2.2	Trabajo remoto	Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.
A.8.3	Manejo de los medios	A.8.3.1	Gestión de los medios removibles	Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.

Código	Norma Específica	N° Control	Nombre Control	Objetivo perseguido
A.8.3	Manejo de los medios	A.8.3.2	Eliminación de los medios	Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.
A.8.3	Manejo de los medios	A.8.3.3	Transferencia física de medios	Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.
A.11.1	Áreas seguras	A.11.1.4	Protección contra amenazas externas y del ambiente	Se debe diseñar y aplicar la seguridad física contra daños por desastres naturales, ataques maliciosos o accidentes.
A.11.1	Áreas seguras	A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.
A.11.2	Equipamiento	A.11.2.5	Retiro de Activos	El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización.
A.18.1	Cumplimiento con los requisitos legales y contractuales	A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1	Cumplimiento con los requisitos legales y contractuales	A.18.1.5	Regulación de los controles criptográficos	Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones pertinentes.

Tabla 3: ***Cruce de los controles de la Nch-ISO27001 que no están en el Anexo nº4: controles específicos de seguridad de la información del BancoEstado Contacto 24 horas Lota.***

Fuente: elaboración propia, Junio 2017.

4.3 Estado del arte

Fuente: Elaboración propia, junio 2017.

Al centrarse en la organización en la que se diseñará este modelo gestión de seguridad de información, claramente se puede identificar que pertenece al rubro de instituciones bancarias, debido a que, es una filial del BANCO DEL ESTADO DE CHILE, así mismo, se puede determinar sus competencias más significativas, que son los siguientes bancos: BANCO DE CHILE, BANCO SANTANDER-CHILE, BANCO DE CREDITO E INVERSIONES, SCOTIABANK CHILE, BANCO BILBAO VIZCAZAYA ARGENTARIA (BANCO BBVA), ITAÚ-CORPBANCA.

Luego del estudio de todas las memorias anuales del periodo 2016 de estas instituciones, se puede determinar lo siguiente:

- Banco de chile no posee certificación de la ISO 27.001. (Memoria Anual 2016, 2017).
- Banco Santander no posee certificación de la ISO 27.001. (Informe Anual 2016, 2017).
- Banco de Crédito e Inversiones no posee certificación de la ISO 27.001. (Memoria Integrada 2016,2017).
- Banco Scotiabank Chile no posee certificación de la ISO 27.001. (Gbm.scotiabank.com, 2017).
- Banco Itaú-Corpbanca no pose certificación de la ISO 27.001. (Banco.itau.cl, 2017).
- Banco Bilbao Vizcazaya Argentaria (BBVA) no posee certificación de la ISO 27.001, pero si poseen certificación en la ISO 14.001 que indica cómo establecer un sistema de gestión ambiental efectiva. (BBVA NOTICIAS, 2017).

Tras el estudio de las memorias anuales de los bancos que son competidores directos del Banco del Estado de Chile, se procedió a analizar la encuesta anual correspondiente al año 2016 de la ISO[5], en Chile sólo hay 49 empresas certificadas en la ISO 27001:2005(ISO SURVEY DATA, 2017)[6]. Dentro de las 49 organizaciones certificadas se puede destacar la presencia de la empresa Sinacofi[7], la que posee dentro de su cartera de clientes al Banco del Estado de Chile, esta organización en la memoria anual del año 2010 dice lo siguiente (Mundo Sinacofi, 2010):

[5] International Organization for Standardization.

[6] Encuesta anual realizada por la International Organization for Standardization, en español, Organización Internacional de Normalización. Estas encuestas se pueden revisar desde un repositorio online, el cual contiene todos los resultados obtenidos de las encuestas realizadas en planillas formato Excel.

[7] Sistema Nacional de Comunicaciones Financieras. "cuyo objetivo principal fue la administración, operación y desarrollo de una red electrónica, para apoyar en forma eficiente la acción comercial y operativa de las instituciones financieras de nuestro país, mediante el intercambio de información de valor." (Sinacofi.cl, 2017)

> "*SINACOFI lleva años en la senda de la mejora continua y trabajando en su sistema de gestión de seguridad de la información y de calidad, ambos auditados por la norma ISO 27001:2005 e ISO 9001:2008, respectivamente. Atributos únicos de nuestros servicios en el mercado y que garantizan a nuestros clientes que nuestra excelencia de servicio se encuentra certificada por terceros expertos en la materia, siendo hoy el único buró de crédito del país en obtener dichas certificaciones*"

Por ende, se destaca que el centro de contacto de BancoEstado se transforma en un pionero dentro de las instituciones bancarias en tomar la iniciativa de realizar un proyecto de seguridad de la información utilizando controles basados en el ANEXO A de la Nch-ISO27001. Esto producirá una gran ventaja competitiva a la organización.

4.4 Fundamento Teórico de la propuesta

4.4.1 La información

A partir de la red de expertos en la normativa Nch-ISO27001 (Iso27000.es, 2017).

> "*Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración*."

4.4.2 Seguridad

A partir de (Peso, Ramos y Peso, 2004).

Seguridad viene a ser la protección de los activos (la definición de activos está en el apartado **4.4.4 Activos de información**) frente a acciones o situaciones no deseadas, mediante la implantación de los controles, lo que suele suponer una inversión y un esfuerzo.

4.4.3 Seguridad de la Información

A partir de (Meneses Benítez, 2007).

Son todas las actividades orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento, independientemente de la forma en que ésta se presente.

En este ámbito se adoptan las siguientes definiciones:

- **Integridad.** Salvaguardar la exactitud y completitud de la información y de sus métodos de procesamiento.
- **Confidencialidad.** Asegurar que la información es accesible sólo para quienes tengan acceso autorizado.
- **Disponibilidad.** Asegurar que los usuarios autorizados tengan acceso a la información y sus activos asociados cuando lo requieran.

4.4.3.1 Importancia de la seguridad de la Información para la organización.

El manejo de la información es fundamental para cualquier empresa, con ello se puede lograr un alto nivel competitivo dentro del mercado y obtener mayores niveles de capacidad de desarrollo.

La seguridad de la información recalca su importancia como la protección de la confidencialidad, integridad y disponibilidad de los activos

de información según sea necesario para alcanzar los objetivos de funcionamiento de la organización.

4.4.3.2 Beneficios de la Seguridad de la Información

Existen numerosas e importantes razones para afrontar el desarrollo de una metodología para el diseño de un modelo de gestión de la seguridad de la información:

- **Reducción de Costos:** Al detectar los principales focos de fallos y errores, y eliminarlos o reducirlos hasta donde es posible, se evitan costosos incidentes de seguridad.
- **Optimizar los recursos y las inversiones de tecnología:** Habrá una motivación de negocio detrás de estas decisiones, por lo que la dirección podrá comprenderlas y apoyarlas de manera más consciente.
- **Protección en la Organización:** Con una metodología que garantice una adecuada estructura para un modelo de gestión de la seguridad de la información se evitan interrupciones en el flujo de procesos de la organización, debido a que, se está asegurando de una manera eficaz la protección de la misma en base a políticas adecuadas.
- **Mejora de la Competitividad:** Cualquier mejora en la gestión de la organización redunda en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza en la organización, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.
- **Cumplimiento Legal y reglamentario:** Gestionando de manera coordinada la seguridad se tendrá un marco donde incorporar los nuevos requisitos y poder demostrar los organismos correspondientes para el cumplimiento de los mismos.
- **Mantener y mejorar la imagen corporativa:** Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y servicios.

4.4.4 Activos de Información

A partir del foro de expertos en la normativa Nch-ISO27001. (Iso27000.es, 2017).

Un activo es *"En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización."* Por lo tanto, necesita ser protegida.

A partir de un documento interno del centro de contacto (Metodología de Gestión de Riesgo Tecnológico, 2017, pp.3-4), los activos se clasifican en dos tipos dentro del centro de contacto BancoEstado 24 horas:

- **Activos Principales:** Son los activos que forman parte de procesos importantes y la información en sí.
- **Activos de Soporte:** Los cuales incluyen: Hardware, Software, Redes, Personal, Sitios (infraestructura) y estructura organizativa.

4.4.5 Inventario de Activos

A partir de la red de expertos del programa de mejoramiento de la gestión y metas de eficiencia institucional sistema de seguridad de la información. (Guía Metodológica 2014, 2017).

Se denomina activo a cualquier información o elemento que otorga algún valor para la organización.

El objetivo del inventario de activos es poder tener un diagnóstico de la empresa determinando qué tan críticos son los activos que participan en los procesos claves de la organización. Según la guía metodológica 2014 para poder llevar a cabo este diagnóstico, se necesita crear una planilla Excel con tres secciones: descripción de procesos, identificación de activos, y análisis de criticidad, los que serán especificadas en los siguientes apartados:

4.4.5.1 Descripción de procesos

En esta sección de la planilla que representa el inventario de activos, se debe describir los procesos, subprocesos y etapas relevantes que tiene participación el área a inventariar. Cabe destacar que si el área no tiene participación en procesos, subprocesos o etapas relevantes dentro del funcionamiento de la empresa, estas columnas se deben dejar especificadas pero sin información en la planilla Excel.

- Procesos: Corresponde al nombre del proceso de negocio (de provisión de productos/servicios estratégicos) al cual pertenecen los activos de información a incluir en el inventario.
- Subprocesos: Son aquellos subprocesos en los que puede estar dividido el proceso transversal mencionado en la columna anterior, dependiendo de la complejidad del mismo.

- Etapas Relevantes: Detalle de las fases más importantes que se deben desarrollar en cada subproceso para dar origen a los productos.

4.4.5.2 Identificación de Activos

En esta sección del inventario de activos, se caracterizan los activos identificados de la siguiente manera:

- **Activo:** Nombre del activo de información, en este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características.
- **Identificador:** En este campo se debe incluir el código dado por la organización al activo, en caso de corresponder a un activo de información no inventariado, este campo se debe completar con un número correlativo, que permita identificar en forma única al activo.
- **Tipo:** se pueden clasificar de la siguiente manera:

  - **Persona:** Funcionario o personal a honorarios que participa en un proceso de negocio.
  - **Documento:** Corresponde a un escrito que refleja el resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.
  - **Base de Datos:** Es la información sistematizada y organizada.
  - **Formulario:** Corresponde a documentos utilizados para recoger información.
  - **Software**: Programa computacional empaquetado producido por una empresa que lo comercializa.
  - **Sistema:** Programa computacional desarrollado por la institución o por un externo a medida, cuyo objetivo es apoyar un proceso de negocio.
  - **Equipos:** Objetos o dispositivos que realizan o apoyan la realización de una función.
  - **Infraestructura:** Construcción que permite alojar algunas o todas las funcionalidades de la institución.
  - **Datos:** Se le llama a la información en formato digital que se resguarda en las bases de datos.

- **Ubicación:** Corresponde al lugar físico dónde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.

- **Responsable / dueño:** Corresponde al rol o cargo de la persona propietaria del activo.

- **Soporte:** Corresponde al medio en el cual se encuentra registrado el activo, este puede ser en papel o digital.
- **Manipulación:** Identificación de la(s) persona(s) que utiliza(n) el activo de información, ya sea modificándolo, actualizándolo, trasladándolo o limpiándolo.
- **Persona autorizada para copiar:** Corresponde al rol o cargo de la(s) persona(s) autorizada para copiar el activo (aplicable al activo de información en papel y copias en medios magnéticos).
- **Medio de almacenamiento:** Descripción de la forma de guardar el activo cuando no está en uso dentro del proceso mismo.
- **Tiempo de retención:** Corresponde al tiempo en el cual el activo de información debe ser mantenido por la Institución en el medio de almacenamiento.
- **Disposición:** Corresponde al destino que se le da al activo de información una vez transcurrido el tiempo de retención.
- **Recuperación (criterio):** Forma en la cual es posible buscar el activo de información. En lo específico, es el criterio de búsqueda o los datos con los cuales se puede localizar el activo.

4.4.5.3 Análisis de criticidad

Fuente: a partir de un documento interno del centro de contacto. (Metodología de Gestión de Riesgo Tecnológico, 2017, pp.15-19).

El análisis de criticidad se realiza para obtener un diagnóstico de la empresa en relación a la confidencialidad, integridad y disponibilidad de los activos de información identificados, con este análisis se definen los activos críticos para el funcionamiento de la organización.

Para definir los activos críticos de la empresa es necesario calcular la criticidad de los activos de información, para ello primeramente se deben definir los niveles de confidencialidad, integridad y disponibilidad, como también su medición cuantitativa.

En lo que respecta al atributo de confidencialidad se clasifica en los siguientes niveles:

- Confidencial Nivel 1: Es información que requiere el mayor nivel de restricción por cuanto su divulgación a terceros permitiría acceder directamente a información que posibilita la realización de operaciones en perjuicio del Banco o de sus clientes. Ejemplo: Claves.

- Confidencial Nivel 2: Es la información protegida por la Ley de Secreto y Reserva Bancaria, su divulgación podría tener repercusiones en la responsabilidad legal del Banco, con todos los efectos colaterales que esta situación pudiera acarrear. Ejemplo: Información de movimientos y saldos en cuentas corrientes.

- Confidencial Nivel 3: Es información protegida por Ley (diferente al Secreto y Reserva Bancaria), por cláusulas contractuales de confidencialidad o calificada como tal por el propio Banco, su divulgación puede producir efectos directos en la responsabilidad legal, reputación del Banco, en el desarrollo de las estrategias comerciales y puede otorgar ventajas indebidas a competidores del Banco o a terceros. Ejemplo: Base de datos de clientes.

- Confidencial Nivel 4: Es información referida al Banco o la Corporación que es distribuida dentro del Banco para el conocimiento de sus funcionarios sin restricciones. Ejemplo: Procedimientos internos.

- Información Pública: Es aquella de libre disposición fuera de la organización, ya sea porque así lo ha establecido la ley o así lo ha dispuesto el dueño o responsable de dicha información. Ejemplo: Balances.

Confidencialidad	
Categorias	Ponderación
Información Pública	1
Nivel 4	2
Nivel 3	3
Nivel 2	4
Nivel 1	5

Tabla 4: ***Valores Confidencialidad***

En cuanto a su atributo de integridad, todos los activos del Banco deben ser íntegros, con excepción de aquellos casos donde se acepta que la información tenga una pérdida menor de integridad, pero manteniendo una certeza estadística. Siendo así, clasificada como:

- Nivel I: Activos Íntegros.
- Nivel II: Activos Íntegros con excepciones.

Integridad	
Categorias	Ponderación
Nivel I	5
Nivel II	1

Tabla 5: ***Valores Integridad***

En cuanto a su atributo de disponibilidad, los activos se valoran en los siguientes niveles:

- Nivel I: Activos de información que son imprescindibles para la operación del Banco y para las cuales se requiere continuidad.
- Nivel II: Activos de información que son importantes para la Corporación BancoEstado, pero que pueden mantener una discontinuidad por un período limitado de tiempo.
- Nivel III: Activos de información que no son relevantes para la operación de la Corporación BancoEstado y para las cuales no se requiere continuidad.

Disponibilidad	
Categorias	Ponderación
Nivel I	5
Nivel II	3
Nivel III	1

Tabla 6: ***Valores Disponibilidad***

Luego de haber clasificado los niveles de confidencialidad, disponibilidad e integridad en la planilla del inventario de activos para obtener los activos críticos para la organización, estos se calculan de la siguiente manera, se suman mediante sus puntajes ponderados según las tablas anteriormente especificadas (tabla 2,3,4), y se determina la criticidad de acuerdo a la tabla 5, esta va dependiendo de la cantidad de variables evaluadas, puede ser la criticidad por una variable, por dos o tres variables[8]:

Criticidad 1 var		C.Criticidad 2 var		C.Criticidad 3 var	
Valor suma total	Categoría	Valor suma total	Categoría	Valor suma total	Categoría
1	Baja	1	Baja	1	Baja
2	Media Baja	2	Baja	2	Baja
3	Media	3	Media Baja	3	Baja
4	Media Alta	4	Media Baja	4	Media Baja
5	Alta	5	Media	5	Media Baja
		6	Media	6	Media Baja
		7	Media Alta	7	Media
		8	Media Alta	8	Media
		9	Alta	9	Media
		10	Alta	10	Media Alta
				11	Media Alta
				12	Media Alta
				13	Alta
				14	Alta
				15	Alta

Tabla 7: ***Nivel de criticidad según variables***

[8] Las variables pueden ser: confidencialidad, integridad o disponibilidad.

- Las categorías de la criticidad son:
    - Baja
    - Media Baja
    - Media
    - Media Alta
    - Alta

4.4.6 Amenaza

Según la red de expertos del foro web ISO27001.es, (Iso27000.es, 2017).

Una amenaza se define como *"Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o a una organización."*

En las organizaciones los activos de información están sujetos a distintas formas de amenazas. Estas podrían llegar a causar un incidente no deseado generando una posible materialización de la amenaza, lo que podría generar un daño a la organización y a sus activos.

Para el centro de contacto de BancoEstado 24 horas, las amenazas pueden ser de distintos tipos. Por Ejemplo:

- Fallos de hardware
- Fallos de software
- Acciones de personal
- Penetración por terminales
- Robos de datos, servicios, equipo.
- Incendio
- Problemas eléctricos.
- Errores de usuario.
- Cambios de programa.
- Problemas de telecomunicaciones.

Estas amenazas son las más comunes y pueden provenir de factores técnicos, organizacionales y del entorno, combinadas también con decisiones administrativas deficientes.

4.4.7 Riesgo

Fuente: a partir de un documento interno del centro de contacto. (Metodología Riesgo Operacional en Procesos, 2017).

El riesgo corresponde a la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la organización.

4.4.7.1 Tipos de riesgos

El riesgo inherente: Es el riesgo intrínseco a cualquier actividad, sólo por el hecho de existir. Para disminuirlo, una entidad necesita contar con Controles o Mitigadores, que disminuyan su probabilidad de ocurrencia y/o el impacto que puede producir.

El riesgo residual: Es el riesgo que permanece después de que se han desarrollado mecanismos de control y mitigación. Controles eficientes y robustos pueden convertir actividades con riesgos inherentes altos, en actividades con riesgos residuales pequeños.

4.4.7.2 Determinación del Riesgo

Para calcular el Riesgo Inherente y Residual, se utilizarán las siguientes fórmulas:

Riesgo Inherente	Impacto X Probabilidad
Riesgo Residual	Riesgo Inherente X (1 - (Efectividad del Control – 1) X 0,25) RI=I*P RR=RI-[(EC-1)*0,25]*RI RR=Alfa*RI donde Alfa=1-(EC-1)*0,25 RR=Alfa*I*P=I*(Alfa*P)=I*P´ donde P´=Alfa*P es una nueva probabilidad afectada por la efectividad del control. Lo anterior indica que para el cálculo del riesgo residual los controles se interpretan matemáticamente como alterando la probabilidad de ocurrencia. Por lo tanto el riesgo residual es la combinación del mismo impacto ponderado por una probabilidad 'X' posterior a la ejecución de los controles.

La Escala de Riesgo Inherente y Riesgo Residual, es la siguiente:

Riesgo Inherente	
RI = Probabilidad * Impacto	Niveles
0 < RI <= 2	No Significativo
2 < RI <= 4	Leve
4 < RI <= 8	Medio
8 < RI <= 15	Alto
15 < RI <= 25	Muy Alto

Tabla 8: ***Riesgo Inherente***

Riesgo Residual	
RR=RI-[(EC-1)*0,25]*RI	Niveles
0 < RR <= 2	No Significativo
2 < RR <= 4	Leve
4 < RR <= 8	Medio
8 < RR <= 15	Alto
15 < RR <= 25	Muy Alto

Tabla 9: ***Riesgo Residual***

4.4.8 Análisis de Riesgo

Fuente: a partir de dos documentos internos del centro de contacto. (Metodología Riesgo Operacional en Procesos, Metodología de Gestión de Riesgo Tecnológico, 2017).

Una vez realizado el inventario de activos y teniendo en claridad cuáles son los activos críticos para la empresa, se requiere analizar todas las posibles amenazas, con la finalidad de poder cuantificar el riesgo inherente o la severidad que hay en que una amenaza se materialice, de esta manera, poder mitigar controles dentro del anexo A de la ISO 27001:2013 (ISO, 2013) y poder crear tratamientos que minimicen el impacto en el negocio,

Los activos que procederán al análisis de riesgo son los que fueron calificados con criticidad media, media alta o alta en el inventario de activos. La identificación y el análisis de riesgo se realizarán identificando los siguientes factores:

- **Amenazas**: Corresponde a un incidente no deseado, que puede dar lugar a daños independiente de si se tiene registro de su materialización en el pasado. En este punto se deben identificar todas las amenazas a las que el activo puede verse sometido.

- **Registro histórico de su frecuencia**: Periodicidad con que se ha producido el evento/ incidente descrito, que se encuentre registrado. En caso de no haber registro indicar "No hay registro".

- **Descripción del Riesgo:** Descripción del riesgo que amenaza el activo de información, entendiéndose éste como las condiciones de debilidad en los activos que pueden ser afectadas por la existencia de una amenaza concreta, y las consecuencias que esto tiene.

- **Probabilidad de ocurrencia**: Posibilidad de que el riesgo se materialice, este punto debe ser consistente con el registro histórico, en caso de que haya. Los valores posibles son:

  - ❖ Muy Rara vez
  - ❖ Rara vez
  - ❖ Ocasional
  - ❖ Frecuente
  - ❖ Muy Frecuente

Probabilidad	
Categorias	Ponderación
Muy Rara Vez	1
Rara Vez	2
Ocasional	3
Frecuente	4
Muy Frecuente	5

Tabla 10: ***Probabilidad***

- **Impacto:** Es el coste para la empresa que se tiene cuando se materializa un incidente, que puede o no ser medido en términos estrictamente financieros. Por Ejemplo: pérdida de reputación, implicaciones legales, etc. El impacto se mide de la siguiente manera:

  - ❖ No Significativo
  - ❖ Leve
  - ❖ Medio
  - ❖ Alto
  - ❖ Muy Alto.

Impacto	
Categorias	Ponderación
No Significativo	1
Leve	2
Medio	3
Alto	4
Muy Alto	5

Tabla 11: ***Impacto***

- **Severidad o Riesgo Inherente:** Es el riesgo intrínseco a cualquier actividad, sólo por el hecho de existir, corresponde al nivel de gravedad del riesgo, este será calculado de acuerdo al apartado **4.4.7.2 Determinación del riesgo**[9]. Los resultados posibles son:
    - ❖ No Significativo
    - ❖ Leve
    - ❖ Medio
    - ❖ Alto
    - ❖ Muy Alto

Luego de esto es necesario definir el/los control/controles para mitigar el riesgo, estos se definen desde el anexo A que recomienda la ISO NCh- 27.001. Una vez identificados los controles, es necesario establecer si se cumple o no el control, en caso de ser positivo el cumplimento, se debe estrictamente colocar la evidencia con la cual se cumple el control y el nombre especifico del tratamiento mencionado, en caso contrario, se debe crear un plan de acción para el cumplimiento de los controles identificados.

Finalmente se debe analizar la efectividad del control que corresponde al riesgo residual del control.

[9] Léase el capitulo **4.4.7.2 Determinación del Riesgo**

4.4.9 Controles

Según la red de expertos del foro web ISO27001.es, (Iso27000.es, 2017).

"Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo."

TIPOS DE CONTROL

Se diseñan para cumplir varias funciones.

Preventivos*:* Anticipan eventos no deseados antes de que sucedan.

Detectivos: Identifican los eventos en el momento en que se presentan.

Correctivos: Aseguran que las acciones correctivas sean tomadas para revertir un evento no deseado.

Ventajas

Controles Preventivos

- Son más rentables
- Deben quedar incorporados en los sistemas
- Evitan costos de corrección o reproceso

Controles Detectivos.

- Son más costosos que los preventivos
- Miden la efectividad de los preventivos
- Algunos errores no pueden ser evitados en la etapa preventiva
- Incluyen revisiones y comparaciones (registro de desempeño)
- Conciliaciones, confirmaciones, conteos físicos de inventarios, análisis de variaciones, técnicas automatizadas, etc.

Controles Correctivos

- Reducir el impacto de una amenaza.
- Remediar los problemas descubiertos por los controles detectivos.
- Identificar la causa de un problema.
- Corregir los errores que surjan de un problema.

4.4.9.1 Efectividad de los Controles

Fuente: a partir de un documento interno del centro de contacto. (Metodología Riesgo Operacional en Procesos, 2017).

La efectividad de los controles se mide a través del riesgo residual, utilizando dos variables, la probabilidad de ocurrencia o frecuencia en la cual se ejecutan los controles y el impacto que tienen el control sobre la amenaza. Se miden de la siguiente manera:

- **Probabilidad de ocurrencia**: Frecuencia en la cual se ejecutan los controles. Los valores posibles son:
    - ❖ Muy Rara vez
    - ❖ Rara vez
    - ❖ Ocasional
    - ❖ Frecuente
    - ❖ Muy Frecuente

Probabilidad	
Categorias	Ponderación
Muy Rara Vez	1
Rara Vez	2
Ocasional	3
Frecuente	4
Muy Frecuente	5

Tabla 12: ***Probabilidad de ocurrencia en la Efectividad de los controles.***

- **Impacto:** Corresponde a los efectos que tiene el control sobre la materialización de la amenaza. Los valores posibles son:

  - ❖ No Significativo
  - ❖ Leve
  - ❖ Medio
  - ❖ Alto
  - ❖ Muy Alto.

Impacto	
Categorias	Ponderación
No Significativo	1
Leve	2
Medio	3
Alto	4
Muy Alto	5

Tabla 13: ***Impacto del control***

Riesgo Residual: Es el riesgo que permanece después de que se han desarrollado mecanismos de control y mitigación. Controles eficientes y robustos pueden convertir actividades con riesgos inherentes altos, en actividades con riesgos residuales pequeños. Este será calculado de acuerdo al apartado **4.4.7.2 Determinación del Riesgo**.

Se mide de la siguiente manera:

- ❖ No Significativo
- ❖ Leve
- ❖ Medio
- ❖ Alto
- ❖ Muy Alto

Riesgo Residual	
RR=RI-[(EC-1)*0,25]*RI	Niveles
0 < RR <= 2	No Significativo
2 < RR <= 4	Leve
4 < RR <= 8	Medio
8 < RR <= 15	Alto
15 < RR <= 25	Muy Alto

Tabla 14: ***Riesgo Residual de la Efectividad de los controles.***

5 Diseño de la propuesta de seguridad de la información basada en el ciclo deming/PDCA

Según la Instituto Nacional de Normalización (Instituto Nacional de Normalización, 2013, p. 1)

> "*Esta norma ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información."*

Entonces, se puede claramente identificar que la metodología más apta es la llamada ciclo Deming o ciclo PDCA (Plan, Do, Check, Act) que es un ciclo de mejora continua que consta de 4 etapas que son Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). Siendo esta metodología la base para la implementación del modelo de gestión de seguridad de la información en el área de datos del centro de contacto BancoEstado 24 horas. A continuación se describen las 4 etapas del ciclo PDCA.

Cabe mencionar que el modelo de gestión de seguridad de la información no abarcará completamente el ANEXO A de la ISO 27001, debido a que, la dirección del centro de contacto BancoEstado 24 horas por razones administrativas, no cuenta con presupuesto necesario para abarcar en todo ámbito lo que propone esta norma, y también, se debe tener en cuenta que el periodo que en el que se realiza un proyecto de título es demasiado acotado.

5.1 PLAN (Planificar)

Esta etapa es la inicial, es una fase de diagnóstico, en donde se analiza el área en la que se implementará el modelo de gestión de seguridad de la información. Para ello, se realizaran tres actividades claves para esta instancia.

5.1.1 Alcance del Modelo de Gestión de Seguridad de la Información (MGSI).´

La ISO27001 dice esto sobre la definición del alcance de un modelo de gestión de la seguridad de la información.

"**4 Contexto de la organización**

4.1 Comprender la organización y su contexto

La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr e(los) resultado(s) esperado(s) de su sistema de gestión de la seguridad de la información.

NOTA Determinar estos asuntos se refiere a establecer el contexto externo e interno de la organización, considerado en ISO 31000:2009, 5.3

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) Las partes interesadas que son pertinentes para el sistema de gestión de la seguridad de la información; y

b) Los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir requerimientos legales y regulatorios, así como obligaciones contractuales.

4.3 Determinar el alcance del sistema de gestión de la seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la Información para establecer su alcance.

Al determinar este alcance, la organización debe considerar:

a) los asuntos externos e internos tratados en 4.1;

b) los requerimientos tratados en 4.2; y

c) interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.

El alcance estará disponible como información documentada." (Instituto Nacional de Normalización, 2013, pp. 2-3).

5.1.2 Inventario de Activos de Información.

Esta segunda etapa se realizará en el área de datos solamente, inventariando todos sus activos de información, esto está determinado en el alcance del modelo de gestión de seguridad de la información.

El inventario de activos de información se define en el apartado **4.4.5 Inventario de Activos** del fundamento teórico.

5.1.3 Análisis de Riesgo.

El análisis de riesgo se define en el apartado **4.4.8 Análisis de Riesgo** del fundamento teórico.

Aquí se utilizan los controles propuestos por el área de riesgo tecnológico del centro de contacto BancoEstado Lota, puesto que, al ser una entidad financiera se debe regir por lo que propone la Superintendencia de Bancos e Instituciones Financieras (SBIF). Léase estos controles en el apartado **4.2.3 Anexo nº4: controles específicos de seguridad de la información para la mitigación de riesgos.**

5.2 DO (Hacer)

En esta etapa las actividades involucradas adquieren la calidad de compromisos, entonces, luego de realizar un análisis del área de datos del centro de contacto, donde se identificaron los activos críticos para el área, y también, se mitigaron los riesgos que hay cuando se materializa una amenaza, a través de los controles que propone el anexo nº4 de la Metodología de Gestión de Riesgos Tecnológicos del centro de contacto BancoEstado Lota, estos controles se encontrarán en el desarrollo de este proyecto en el apartado **6.5 Plan General de Seguridad de la Información.** Como acción siguiente, se procede a realizar las siguientes actividades, dentro de ellas está el nombramiento del encargado de seguridad, la constitución del comité de seguridad, y por último, el plan general de seguridad donde se comprometen los controles a implementar para una correcta gestión del riesgo.

5.2.1 Nombramiento del Encargado de Seguridad.

Esta decisión pasa por el Jefe de Servicio, quien nombra como asesor directo en esta materia al Encargado de Seguridad.

Las labores principales de este consisten en tener a su cargo el desarrollo de las políticas de seguridad, control y mantenimiento.

Este nombramiento del encargado de seguridad debe estar documentado.

5.2.2 Constitución del Comité de Seguridad.

Este comité está presidido por el encargado de seguridad de la información y por los encargados de las áreas mencionadas.

- Jefe Operaciones o Tecnologías de Información.
- Jefe de Recursos Humanos.
- Encargado de Calidad.
- Encargado de Riesgos.
- Asesor Jurídico (Abogado de la Institución).
- Jefes de Áreas Funcionales o encargados de procesos.

Esta constitución del comité de seguridad debe estar documentado.

5.2.3 Plan General de Seguridad de la Información.

Esta es la definición de los controles que se busca implementar en el área. Para la generación de este documento se deben considerar los resultados del análisis de criticidad y el análisis de riesgo.

Para esto se define:

- **Producto esperado:** Corresponde al control definido en la etapa anterior que se quiere implementar.
- **Responsable:** Nombre y cargo del responsable de la implementación del producto.
- **Actividades:** Secuencia de actividades que se deben realizar para la obtención del producto.
- **Fecha de Inicio:** Corresponde a la fecha de inicio de la actividad.
- **Fecha de Término:** Corresponde a la fecha de término de la actividad.

Esta Actividad debe estar documentada.

5.2.4 Definición de indicadores

Estos indicadores sirven para medir la efectividad del control a aplicar, y con esto, poder medir la efectividad del modelo de gestión de seguridad de la información, el indicador definido se encuentra en el apartado **4.4.9.1 Efectividad de los Controles** del fundamento teórico.

5.3 CHECK (verificar): Revisar el modelo de gestión de seguridad de la información (MGSI).

Una vez puesto en marcha el plan de seguridad se debe revisar periódicamente. Lo importante es ir completando las planillas de seguimientos que acompañan la ejecución de los controles implementados en la etapa anterior. En esta fase es donde se ocupan los indicadores para ver qué tan efectivos son nuestros controles en el MGSI.

5.4 ACT (Actuar): Mantener y mejorar el MGSI.

En esta etapa final es donde se analizan las observaciones escritas en las planillas de seguimiento correspondientes a cada uno de los controles implementados, se deben realizar propuestas de mejoras, con el fin de poder crear un plan de mejora para el siguiente ciclo de la metodología ocupada, porque hay que recordar que el ciclo Deming es una metodología de mejora continua.

6 Desarrollo

Dentro de la primera etapa de la metodología, las primeras actividades realizadas fueron:

6.1 Definición del Alcance del Modelo de Gestión de Seguridad de la información (MGSI).

Básicamente la Nch-ISO27001 dice que para la definición de un modelo de gestión de seguridad de la información, primero se debe conocer la organización tanto en sus asuntos internos como externos, para así con esto contribuir a una mejor comprensión de la empresa con respecto a sus necesidades y expectativas, las cuales son importantes para definir los objetivos, y además, poder sacar potencial para cumplir a cabalidad las metas propuestas (Instituto Nacional de Normalización, 2013, pp. 2-3).

A continuación se presenta la definición del alcance del modelo de gestión de seguridad de la información.

Definición del Alcance del SGSI

Objetivos

- Realizar un inventario de activos del área problema del centro de contacto.
- Realizar análisis de criticidad de los activos críticos.
- Realizar análisis de riesgo a los activos de criticidad media, alta y muy alta.
- Mitigar el riesgo inherente con controles propuesto en el anexo nº4 Controles
- Crear un plan general de seguridad de información, en el cual, se implementen controles de concientización de la seguridad de información y controles de respaldo de sus bases de datos y aplicativos del área de datos.
- Medir los controles a través del riesgo residual expuesto en la metodología de gestión de riesgo tecnológico.
- Crear planillas de seguimientos de los controles implementados, para así, poder realizar observaciones sobre la conformidad que tiene el usuario con respecto al control implementado.

Observaciones:

- Debido al tiempo que se dispone para realizar este proyecto y los pocos recursos dispuestos al estudiante para llevarlo a cabo, se consideraron estas actividades como las más claves dentro de la implementación basada en la Nch-ISO27001. A pesar de no abarcar en un 100% esta norma, para la empresa es sumamente importante este proyecto, porque se da un paso importante en la seguridad de la información, como también se adquiere experiencia en cómo trabajar la norma a través de la metodología utilizada[10], lo que en un futuro esta organización utilizará para la certificación en la ISO27001.

- Las planillas de seguimientos en un caso de tener observaciones de no conformidad, el comité de seguridad debe por obligación generar soluciones y aplicarlas en la segunda iteración de la metodología, con esto se consigue tener

[10] Ciclo PDCA o ciclo Deming

un modelo de gestión de seguridad de la información con una mejora continua en el tiempo.

6.2 Inventario de Activos de información

A continuación se presentan imágenes del inventario de activos de información implementado.

		Banco Estado Centro de Contacto 24 hrs																	
		IDENTIFICACIÓN DE ACTIVOS													ANÁLISIS DE CRITICIDAD				
	Activo	Identificador	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
	Analista de Datos	1	Persona	Área de Datos	Encargado del Área de Datos			Encargado Área Datos					Nivel I		Nivel I	Alta
	Contraseñas de Acceso	2	Datos	Área de Datos	Analista de Datos	Digital	Analista de Datos		Digital	TRIMESTRALES	Permanente		Nivel I		Nivel I	Alta
	Cubiculos de Analista de Datos	3	Infractuctura	Área de Datos	Servicio Generales		Analista de Datos, Servicio			Permanente	Permanente		Nivel 4		Nivel III	Media Baja
	Aire Acondicionado	4	Infractuctura	Área de Datos	Servicio Generales		Analista de Datos, Servicio			Permanente	Permanente		Nivel 4		Nivel III	Media Baja
	Generador Electrico	5	Infractuctura	Grupo Electrógeno	Servicio Generales		Encargado de Servicio Generales			Permanente	Permanente		Nivel 4		Nivel I	Media Alta
	Oficina de Datos	6	Infractuctura	Área de Datos	Servicio Generales		Analista de Datos, Servicio			Permanente	Permanente		Nivel 4		Nivel I	Media Alta
	Redes Computacionales	7	Equipo	Área Soporte tecnologico	Soporte Teenologico		Analista de Datos, Soporte	Encargado de Soporte tecnologico		Permanente	Permanente	Conexión LAN	Nivel I	Nivel I	Nivel I	Alta
	Servicio de Internet	8	Equipo	Área Soporte tecnologico	Soporte Teenologico		Analista de Datos, Soporte	Encargado de Soporte tecnologico		Permanente	Permanente	Conexión LAN / WIFI	Nivel I	Nivel I	Nivel I	Alta
	Linea Telefónica	9	Equipo	Área Soporte tecnologico	Soporte Teenologico		Analista de Datos, Soporte	Encargado de Soporte tecnologico		Permanente	Permanente	Telefonia IP	Nivel I	Nivel I	Nivel II	Alta

Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

LISTO

Figura 2: ***Inventario de Activos.***

		Banco Estado Centro de Contacto 24 hrs																	
		IDENTIFICACIÓN DE ACTIVOS													ANÁLISIS DE CRITICIDAD				
	Activo	Identificador	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
13	Dispositivo De Almacenami	10	Equipo	Área de Datos	Encargado del Área de Datos		Analista de Datos	Encargado Área Datos y Analistas		Permanente	Permanente	Insertando el dispositivo en algún Puerto USB	Nivel 1	Nivel I	Nivel II	Alta
14	Pc-Desarrollo	11	Equipo	Área de Datos	Soporte Tecnologico		Analista de Datos, Soporte	Encargado de Soporte tecnologico		Permanente	Permanente	Nombre de usuario y Contraseña	Nivel 1	Nivel I	Nivel I	Alta
15	PC-BIBANCO	12	Equipo	Área de Datos	Soporte Tecnologico		Analista de Datos, Soporte	Encargado de Soporte tecnologico		Permanente	Permanente	Nombre de usuario y Contraseña	Nivel 1	Nivel I	Nivel I	Alta
16	Softlandrp(\softland)[W:]	13	Equipo	Área de Datos	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital permanente	Ruta direccion servidor, con autentificacion(ID y Password)	Nivel 1	Nivel I	Nivel I	Alta
17	C$(\\186.67.80.217)(W:)/ Servidor e-	14	Equipo	SANTIAGO	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado Área Datos	Racks de almacenamiento de	Permanente	Almacenamiento Digital permanente	Ruta direccion servidor, con autentificacion(ID y Password)	Nivel 1	Nivel I	Nivel I	Alta
18	C$(\tbibanc oestado)(Z:)	15	Equipo	Área de Datos	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital permanente	Ruta direccion servidor, con autentificacion(ID y Password)	Nivel 1	Nivel I	Nivel I	Alta
19	Servidor de Desarrollo	16	Equipo	Área de Datos	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital permanente	Ruta direccion servidor, con autentificacion(ID y Password)	Nivel 1	Nivel I	Nivel I	Alta
20	Servidor de Comunicaciones(hostin	17	Equipo	Virtual	Soporte De Hosting.cl	Digital	Analista de Datos, Soporte	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital permanente	Ruta direccion servidor, con autentificacion(ID y Password)	Nivel 1	Nivel I	Nivel I	Alta
21	Outlook	18	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Almacenamiento Digital permanente	Nombre del Software	Nivel 1	Nivel I	Nivel I	Alta

... Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

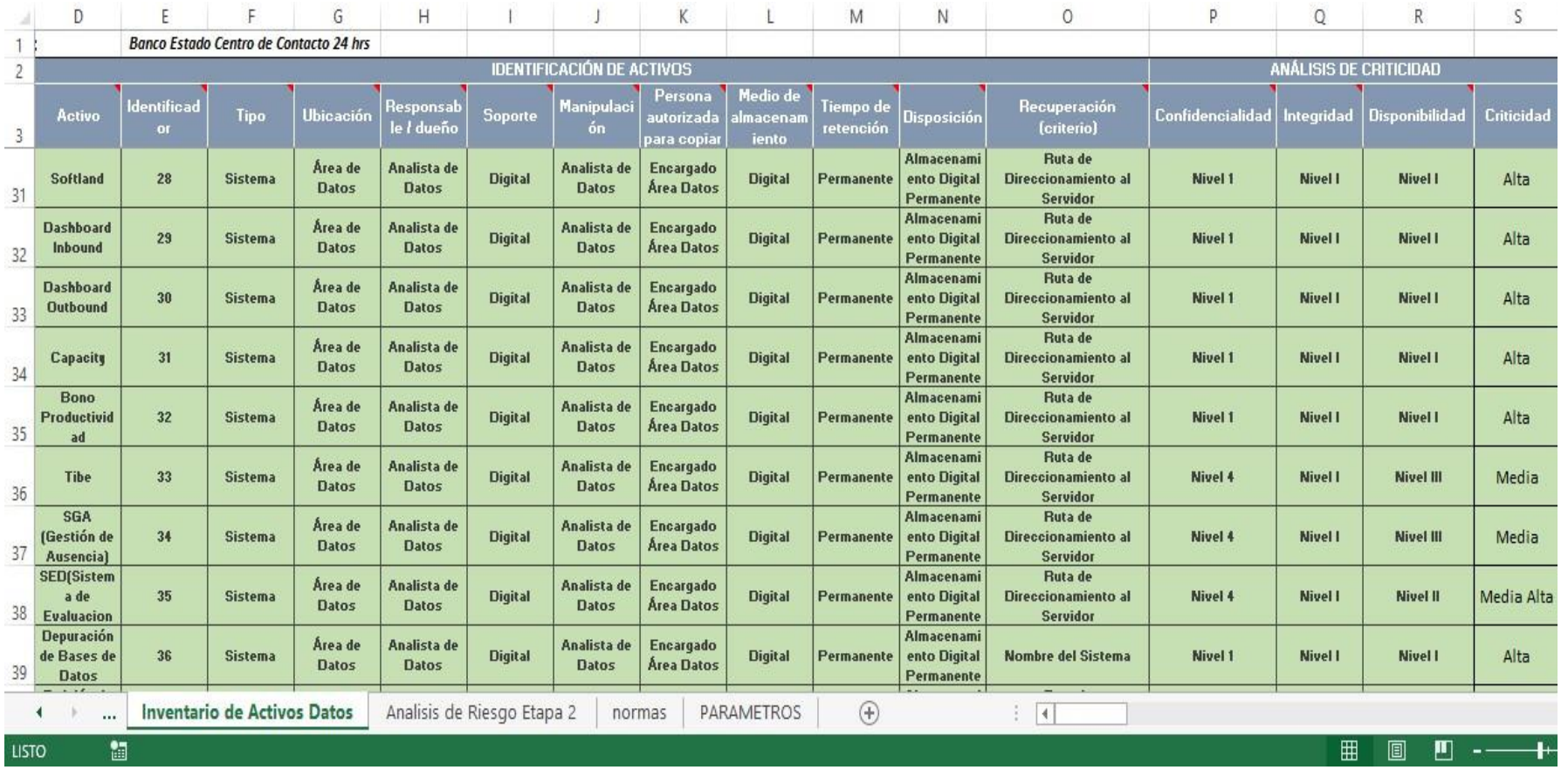
Figura 3: ***Inventario de Activos.***

	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1		*Banco Estado Centro de Contacto 24 hrs*														
2		IDENTIFICACIÓN DE ACTIVOS											ANÁLISIS DE CRITICIDAD			
3	Activo	Identificador	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
22	Sql Server Management Studio	19	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Con Licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
23	Microsoft Visual Studio	20	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Con Licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
24	Microsoft Visual Studio	21	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Con Licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
25	Microsoft Visual Studio Data	22	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Con Licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
26	Microsoft Visual Studio Team	23	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Con Licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
27	Google Chrome	24	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	Almacenamiento Digital permanente	Nombre del Software	Nivel 4	Nivel I	Nivel III	Media
28	WINDOWS 8.1 PRO	25	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	con licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
29	WINDOWS XP Pro	26	Software	Área Soporte tecnologico	Soporte Tecnologico	Digital	Analista de Datos, Soporte	Encargado de Soporte tecnologico	Digital	Permanente	con licencia	Nombre de Software	Nivel 1	Nivel I	Nivel I	Alta
30	Tracking	27	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de trackingUI, con autentificacion(ID y Password)	Nivel 1	Nivel I	Nivel I	Alta

Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

LISTO

Figura 4: ***Inventario de Activos.***



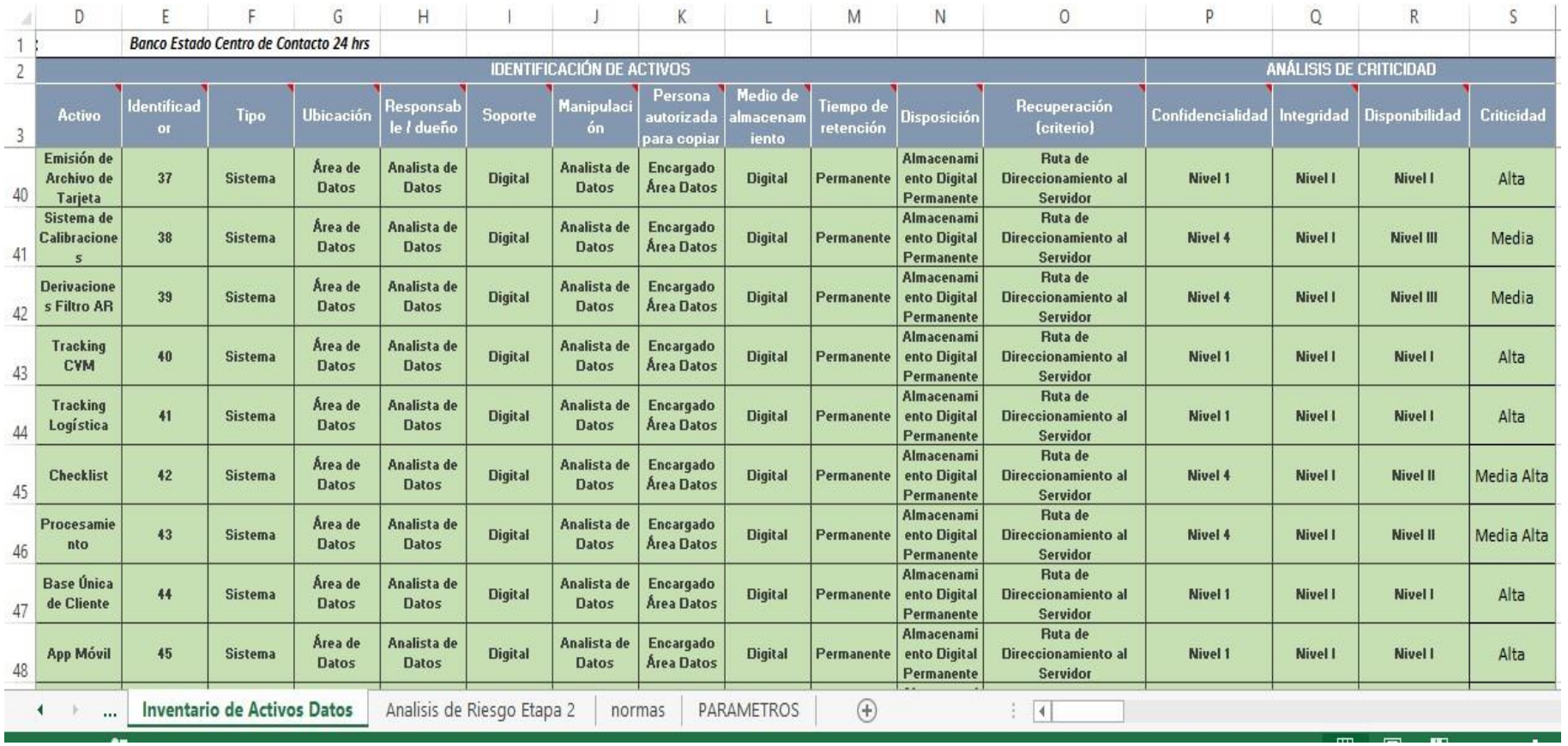
Banco Estado Centro de Contacto 24 hrs

	IDENTIFICACIÓN DE ACTIVOS												ANÁLISIS DE CRITICIDAD			
	Activo	Identificador	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
31	Softland	28	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
32	Dashboard Inbound	29	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
33	Dashboard Outbound	30	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
34	Capacity	31	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
35	Bono Productividad	32	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
36	Tibe	33	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel III	Media
37	SGA (Gestión de Ausencia)	34	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel III	Media
38	SED(Sistema de Evaluacion	35	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel II	Media Alta
39	Depuración de Bases de Datos	36	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Nombre del Sistema	Nivel 1	Nivel I	Nivel I	Alta

Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

LISTO

Figura 5: ***Inventario de Activos.***



	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1		Banco Estado Centro de Contacto 24 hrs														
2	IDENTIFICACIÓN DE ACTIVOS												ANÁLISIS DE CRITICIDAD			
3	Activo	Identificador	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
40	Emisión de Archivo de Tarjeta	37	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
41	Sistema de Calibraciones	38	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel III	Media
42	Derivaciones Filtro AR	39	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel III	Media
43	Tracking CYM	40	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
44	Tracking Logística	41	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
45	Checklist	42	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel II	Media Alta
46	Procesamiento	43	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel II	Media Alta
47	Base Única de Cliente	44	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
48	App Móvil	45	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta

... | Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

Figura 6: ***Inventario de Activos.***

	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1		Banco Estado Centro de Contacto 24 hrs														
2		IDENTIFICACIÓN DE ACTIVOS											ANÁLISIS DE CRITICIDAD			
3		Activo	Identificador	Tipo	Ubicación	Responsable / dueño	Soporte	Manipulación	Persona autorizada para copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Recuperación (criterio)	Confidencialidad	Integridad	Disponibilidad	Criticidad
43		Tracking CYM	40	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
44		Tracking Logística	41	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
45		Checklist	42	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel II	Media Alta
46		Procesamiento	43	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 4	Nivel I	Nivel II	Media Alta
47		Base Única de Cliente	44	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
48		App Móvil	45	Sistema	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento Digital Permanente	Ruta de Direccionamiento al Servidor	Nivel 1	Nivel I	Nivel I	Alta
49		Bases De Datos	46	Base de datos	Área de Datos	Analista de Datos	Digital	Analista de Datos	Encargado Área Datos	Digital	Permanente	Almacenamiento eno Digital Permanente	Nombre de la base.bak	Nivel 1	Nivel I	Nivel I	Alta
50																
51																
52																

Figura 7: ***Inventario de Activos.***

6.3 Análisis de Riesgos

Esta actividad se encuentra a continuación en las siguientes imágenes. Se destaca que solo se muestran los controles que se cumplen, debido a que, el análisis de riesgo es muy extenso para agregarlo al informe de manera completa.

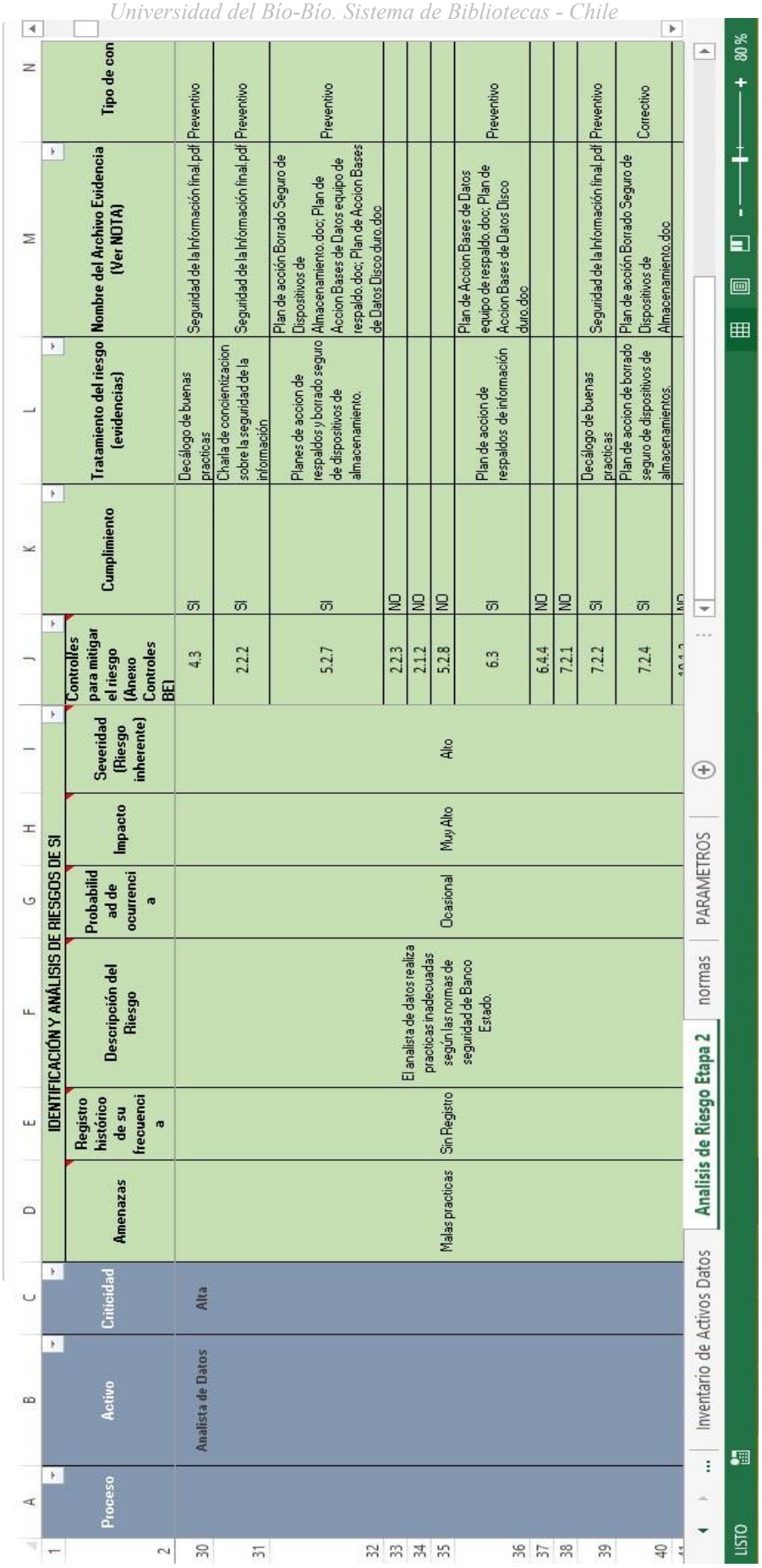
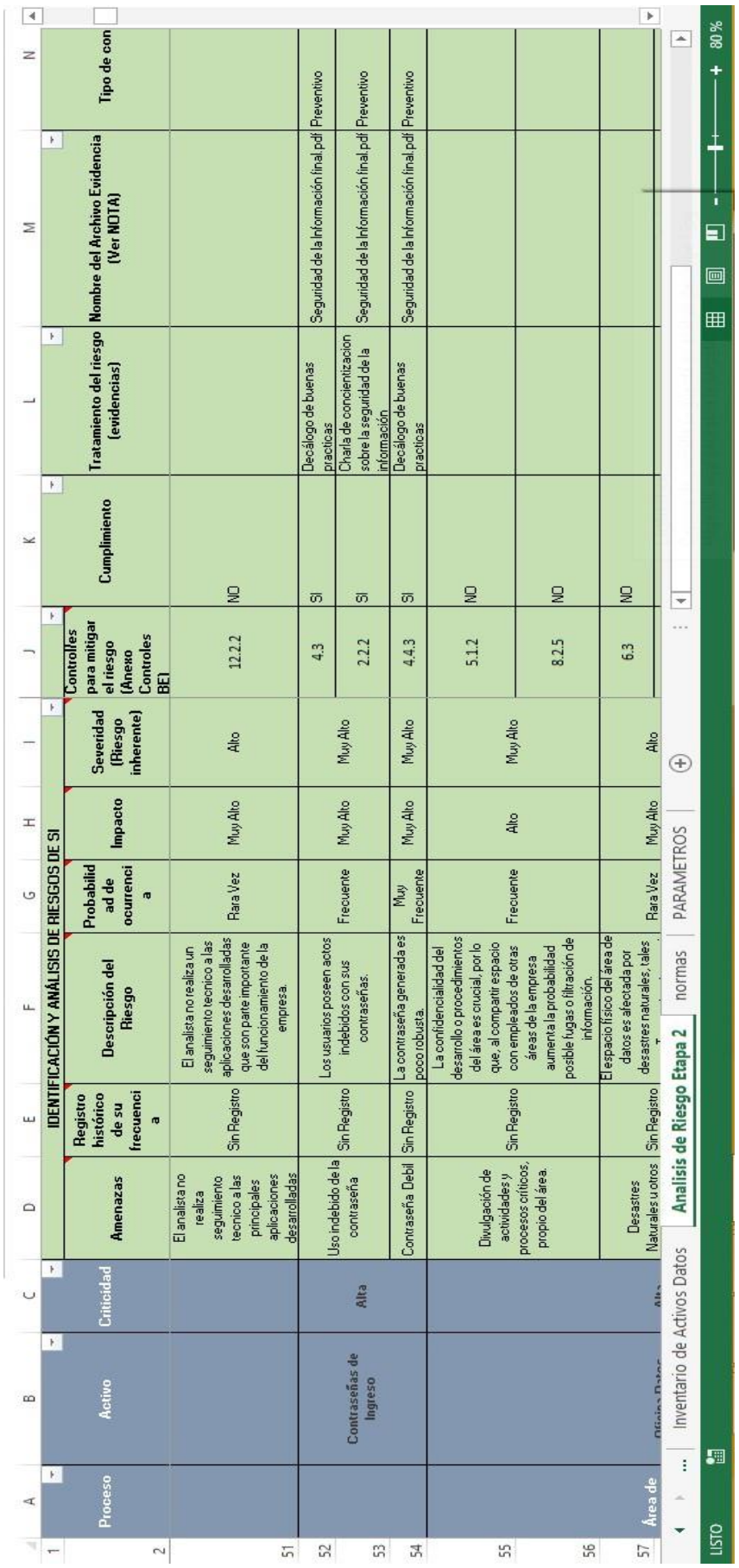


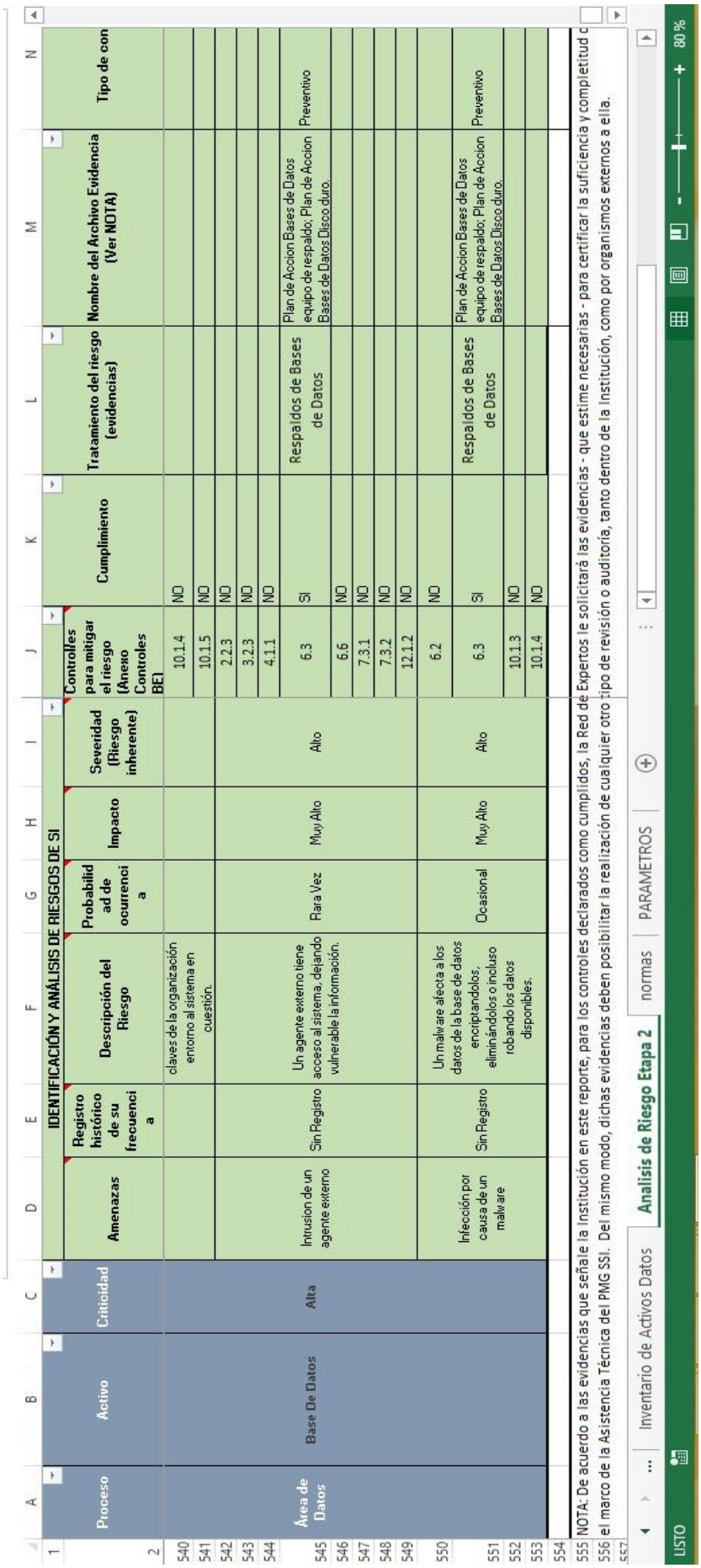
Figura 8: ***Análisis de Riesgo.***



Proceso	Activo	Criticidad	IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS DE SI						Cumplimiento	Tratamiento del riesgo (evidencias)	Nombre del Archivo Evidencia (Ver NOTA)	Tipo de con
			Amenazas	Registro histórico de su frecuencia	Descripción del Riesgo	Probabilidad de ocurrencia	Impacto	Severidad (Riesgo inherente)	Controles para mitigar el riesgo (Anexo Controles BE)			
Área de	Activos Datos	Alta	Desastres Naturales u otros	Sin Registro	El espacio físico del área de datos es afectada por desastres naturales, tales	Rara Vez	Muy Alto	Alto	6.3	NO		
	Contraseñas de Ingreso	Alta	Divulgación de actividades y procesos críticos, propio del área.	Sin Registro	La confidencialidad del desarrollo o procedimientos del área es crucial, por lo que, al compartir espacio con empleados de otras áreas de la empresa aumenta la probabilidad posible fugas o filtración de información.	Frecuente	Alto	Muy Alto	8.2.5	NO		
									5.1.2	NO		
			Contraseña Debil	Sin Registro	La contraseña generada es poco robusta.	Muy Frecuente	Muy Alto	Muy Alto	4.4.3	SI	Seguridad de la Información final.pdf	Preventivo
			Uso indebido de la contraseña	Sin Registro	Los usuarios poseen actos indebidos con sus contraseñas.	Frecuente	Muy Alto	Muy Alto	2.2.2	SI	Seguridad de la Información final.pdf	Preventivo
									4.3	SI	Seguridad de la Información final.pdf	Preventivo
			El analista no realiza seguimiento tecnico a las principales aplicaciones desarrolladas	Sin Registro	El analista no realiza un seguimiento tecnico a las aplicaciones desarrolladas que son parte importante del funcionamiento de la empresa.	Rara Vez	Muy Alto	Alto	12.2.2	NO		

Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

Figura 9: ***Análisis de Riesgo.***



Proceso	Activo	Criticidad	IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS DE SI						Cumplimiento	Tratamiento del riesgo (evidencias)	Nombre del Archivo Evidencia (Ver NOTA)	Tipo de con
			Amenazas	Registro histórico de su frecuencia	Descripción del Riesgo	Probabilidad de ocurrencia	Impacto	Severidad (Riesgo inherente)	Controles para mitigar el riesgo (Anexo Controles BE)			
Área de Datos	Base De Datos	Alta			claves de la organización entorno al sistema en cuestión.				10.1.4	NO		
									10.1.5	NO		
			Intrusion de un agente externo	Sin Registro	Un agente externo tiene acceso al sistema, dejando vulnerable la información.	Rara Vez	Muy Alto	Alto	2.2.3	NO		
									3.2.3	NO		
									4.1.1	NO		
									6.3	SI	Respaldos de Bases de Datos	Plan de Accion Bases de Datos equipo de respaldo; Plan de Accion Bases de Datos Disco duro.	Preventivo
									6.6	NO		
									7.3.1	NO		
									7.3.2	NO		
									12.1.2	NO		
			Infección por causa de un malware	Sin Registro	Un malware afecta a los datos de la base de datos encriptandolos, eliminándolos o incluso robando los datos disponibles.	Ocasional	Muy Alto	Alto	6.2	NO		
									6.3	SI	Respaldos de Bases de Datos	Plan de Accion Bases de Datos equipo de respaldo; Plan de Accion Bases de Datos Disco duro.	Preventivo
									10.1.3	NO		
									10.1.4	NO		

NOTA: De acuerdo a las evidencias que señale la Institución en este reporte, para los controles declarados como cumplidos, la Red de Expertos le solicitará las evidencias - que estime necesarias - para certificar la suficiencia y completitud d
el marco de la Asistencia Técnica del PMG SSI. Del mismo modo, dichas evidencias deben posibilitar la realización de cualquier otro tipo de revisión o auditoría, tanto dentro de la Institución, como por organismos externos a ella.

Inventario de Activos Datos | Analisis de Riesgo Etapa 2 | normas | PARAMETROS

LISTO

80 %

Figura 10: ***Análisis de Riesgo.***

En la segunda etapa de la metodología, las actividades realizadas fueron las siguientes:

6.4 Definición del Comité y Encargado de seguridad

Los Documentos que se generaron fueron, la definición del comité y encargado de seguridad y una planilla de registros, esta última permite validar el compromiso de las personas asignadas, también poder tener un documento oficial con respecto a este punto.

Observación: Por decisiones del directorio de la empresa, no se pudo asignar personas a los puestos que se requieren.

6.5 Plan General de Seguridad de la Información

Se ejecutan los controles comprometidos en el plan general de seguridad de información. Esta actividad se encuentra a continuación**.**

Plan General de Seguridad de la Información

PRODUCTO ESPERADO	RESPONSABLE	ACTIVIDADES	FECHA DE INICIO	FECHA DE TERMINO	RESPONSABLE DE LA ACTIVIDAD	DIFUSIÓN/SENSIBILIZACIÓN	CAPACITACIÓN
Respaldo de las bases de datos en un disco duro.	Fabian Salazar	Plan de Acción Bases de Datos Disco duro	12/09/2017	Sin fecha de termino	Carlos Leiva Beneventi	difusión en la charla de concientización de SGSI	Cuando se apruebe la cotización de los requerimientos para la ejecución de este plan de acción
Respaldo de las bases de datos en un equipo de respaldo.	Fabian Salazar	Plan de Acción Bases de Datos equipo de respaldo	por definir	por definir	Carlos Leiva Beneventi	difusión en la charla de concientización de SGSI	Cuando se apruebe la cotización de los requerimientos para la ejecución de este plan de acción
Manual de Borrado seguro de dispositivos de almacenamiento	Fabian Salazar	Plan de acción Borrado Seguro de Dispositivos de Almacenamiento	12/09/2017	Sin fecha de termino	Carlos Leiva Beneventi	difusión en la charla de concientización de SGSI	Cuando se apruebe la cotización de los requerimientos para la ejecución de este plan de acción
Charla sobre el sistema de gestión de seguridad de la información	Fabian Salazar	Plan de acción Concientización del Sistema de Gestión de Seguridad de la información	22/09/2017	22/09/2017	Fabian Salazar Galleguillos		no posee capacitación
Decálogo de Buenas Practicas	Fabian Salazar	Plan de Acción Decálogo de Buenas Practicas	22/09/2017	22/09/2017	Fabian Salazar Galleguillos		no posee capacitación

Observación 1: En las celdas donde aparece " por definir", se debe a que por decisiones de directorio el centro de contacto no cuenta con presupuesto para comenzar a implementar el plan de acción.

Observación 2: Todos los planes de acción están documentados para que la empresa los aplique cuando sea necesario.

Estos controles son orientados por el BancoEstado contacto 24 horas Lota, en el documento llamado Anexo nº4: Controles específicos de seguridad de la información, se especifica en el apartado **4.2.3 Anexo nº4: controles específicos de seguridad de la información para la mitigación de riesgos.**

6.6 Definición de Indicadores.

El indicador utilizado es el riesgo residual, éste se encuentra definido en el apartado **4.4.9.1 Efectividad de los Controles** del fundamento teórico.

En la tercera etapa se le realizó un seguimiento a los controles implementados y se calculó la efectividad de estos mismos.

Y las actividades realizadas son:

6.7 Concientización de un Sistema de gestión de seguridad de la información.

En seguida se muestran los temas tratados en la charla de Concientización de un modelo de gestión de seguridad de la información (MGSI):

- ¿En qué consiste la seguridad de la información?
  - Triada CIA (Confidencialidad, Integridad y Disponibilidad)
- Activos de Información
  - ¿Qué son los activos de información?
  - Clasificación de activos de información
  - Inventario de activos de información
- Análisis de Riesgo
  - ¿Qué importancia tiene el análisis de riesgo?
  - Tipos de amenazas
  - Evaluación de riesgos
- Controles
  - ¿Qué son los controles?
    - ¿Cuál es su objetivo?
    - Tipos de Controles
  - Planes de acción (difusión)
  - Indicadores

Esta charla se realizó al equipo de trabajo del área de datos, con el fin de darles a conocer los conceptos básicos dentro de un MGSI y para evitar que el analista de datos tenga malas prácticas dentro de la seguridad de la información.

A continuación se muestran los resultados del impacto que tuvo el control en el área.

INTEGRANTES DEL ÁREA DE DATOS	CALIFICACIONES ANTES DE LA CHARLA	CALIFICACIONES DESPUES DE LA CHARLA	Porcentaje de Mejora
Mariana Valderrama Rivera	6,1	7	14,8%
Jorge Escobar Avello	2,8	7	150,0%
Gonzalo Olivares Lopez	3,4	7	105,9%
Nestor Ortega Parra	4,3	5,8	34,9%
Nestor Oñate Lagos	3,4	6,7	97,1%
Francisico Campos Salgado	3,4	5,2	52,9%
Carlos Leiva Beneventi	5,2	6,7	28,8%

Tabla 15: ***Resultados de la Prueba de diagnóstico antes y después de la charla.***

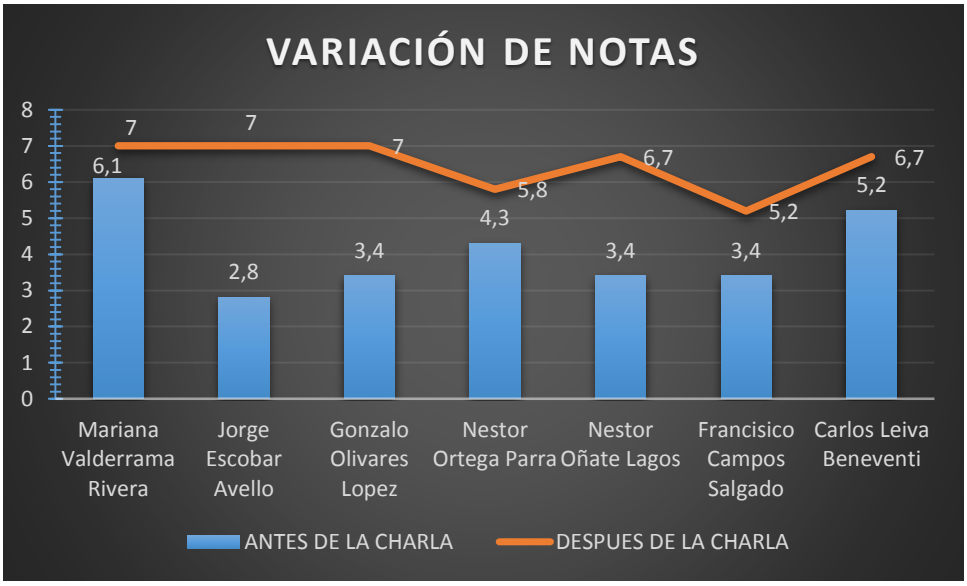


Grafico 1: Variación de los resultados de la prueba diagnostico antes y después de la charla

La charla obtuvo excelentes resultados, esto se determinó a través de una prueba de diagnóstico aplicada antes y después de la charla, al evaluar la efectividad del control basado en el impacto que tiene el control sobre la materialización de una amenaza y la probabilidad en la que se ejecuta este control, el resultado de nuestro indicador resulto ser medio, esto quiere decir que el plan de acción aplicado fue exitoso, debido a que, el riesgo antes de aplicar el control tenía un nivel alto y luego de aplicar el control el riesgo que hay en que se materialice una amenaza es medio, podemos reafirmar que el control aplicado es efectivo, puesto que, reduce el impacto que hay en la materialización de la amenaza.

Este plan de acción mitiga el riesgo de que el analista de datos realice malas prácticas con respecto a la seguridad de la información.

La pauta de la prueba realizada es la siguiente:

Prueba de Diagnóstico de Seguridad de la Información

Nombre:…….
Fecha: _ _ /_ _ /_ _ _ _

I. Encierre en un círculo la respuesta correcta.

1. ¿En qué consiste la Seguridad de la Información según la ISO27001?

a. Consiste en preservar la confidencialidad, integridad y disponibilidad de la información.

b. Consiste en resguardar la información ante ataques informáticos.

c. Consiste en establecer y mantener los programas, controles y políticas de seguridad dentro de la organización.

d. Consiste en establecer políticas de seguridad y planes de acción ante posibles amenazas a la información.

2. ¿Qué es la información?

a. Es todo el conjunto de datos que se encuentra en formato digital en la organización.

b. Es todo el conjunto de datos que se encuentra almacenado en la Base de Datos en la organización.

c. Es todo el conjunto de datos que otorga un valor adicional a la organización.

d. Es todo el conjunto de datos que se encuentra en cualquier tipo de formato en la organización.

3. En el Contexto de la Seguridad de la Información ¿Qué es un Activo?

a. Un Activo es todo lo que otorga valor a la organización.

b. Un Activo es cualquier tipo de información que posee la organización.

c. Un Activo es cualquier tipo de información que es parte de la operación de la organización.

d. Un Activo es el valor total de los elementos que tiene la organización

4. Cual/es de las afirmaciones son correctas con respecto a la Clasificación de Activos:

I. Un Activo se clasifica en: Activo fijo y Activo Pasivo.

II. Un Activo se clasifica en: Activo de Soporte, Activo Principales y Activos Intangibles.

III. Un Activo se clasifica en: Activo de información, Activo fijo y Personas.

IV. Un Activo no se clasifica, debido a que, todo en la organización es un Activo.

a. Solo I b. Solo II c. Solo III d. Todas Son Correctas

5. Un MGSI….

I. Conoce, Gestiona y minimiza los riesgos informáticos.

II. Almacena, Controla y maneja los riesgos informáticos.

III. Garantiza la seguridad de la información

IV. Garantiza la información de la seguridad.

a. Solo I b. solo I y III c. I, II y III d. Ninguna es Correcta

6. ¿Qué son los Controles en un MGSI?

a. Es el conjunto de medidas reactivas de la organización.

b. Es el conjunto de medidas preventivas y reactivas de la organización.

c. Es una planilla en la cual se realiza el control del personal.

d. Anticipan eventos no deseados antes de que sucedan.

7. ¿Qué Significa las siglas MGSI?

- **a. Modelo General de Seguridad de la Informática.**
- **b. Modelo de Gestión de Seguridad de la Informática.**
- **c. Modelo General de Seguridad de la Información.**
- **d. Modelo de Gestión de Seguridad de la Información.**

8. ¿Cómo se Clasifican la Criticidad de los Activos de Información?

- **a. Baja, Media, Alta.**
- **b. Baja, Media baja, Media, Media Alta, Alta.**
- **c. No Significativo, Menor, Leve, Catastrófico.**
- **d. Menor, Leve, Catastrófico.**

9. Los principios de la Seguridad de la Información son:

- **I. Confidencialidad**
- **II. Integridad**
- **III. Autenticación**
- **IV. Privacidad**
- **V. Disponibilidad**

a. I y II Son Correctas **b. I, II y V** **c. I, II, III y V** **d. Todas**

10. ¿Qué es La Triada CIA?

- **a. Es la Confidencialidad, Integridad y Autenticidad de la Información.**
- **b. Es la Confidencialidad, Integridad y Disponibilidad de la Información.**
- **c. Es la Creación e innovación de nuevas normas de Seguridad.**
- **d. Es la Creación, innovación y autenticidad de la Información.**

11. Según la Corporación BancoEstado ¿Cómo se Clasifica la Probabilidad en el Análisis de Riesgo?

a. **Baja, Media baja, Media, Media Alta, Alta.**
b. **Baja, Media, Alta**
c. **Rara vez, Poco Probable, Probable, Casi siempre, Frecuentemente.**
d. **Muy Rara Vez, Rara Vez, Ocasional, Frecuente, Muy Frecuente.**

12. Según la Corporación BancoEstado ¿Cómo se Clasifica el Impacto en el Análisis de Riesgo?

a. **Baja, Media baja, Media, Media Alta, Alta.**
b. **No Significativo, Leve, Medio, Alto, Muy Alto**
c. **Baja, Media, Alta**
d. **Insignificante, Menor, Moderado, Mayor, Catastrófico.**

13. Según Corporación BancoEstado ¿Cómo se Clasifica La Confidencialidad?

a. **Baja, Media baja, Media, Media Alta, Alta.**
b. **Nivel 1, Nivel 2, Nivel 3, Nivel 4 y Nivel 5.**
c. **Nivel 1, Nivel 2, Nivel 3, Nivel 4 e Información Pública.**
d. **Baja, Media, Alta**

14. Según la Corporación BancoEstado ¿Cómo se Clasifica La Disponibilidad?

a. **Baja, Media, Alta**
b. **Nivel 1, Nivel 2 y Nivel 3.**
c. **Baja, Media baja, Media, Media Alta, Alta.**
d. **Disponible y No disponible**

15. Según la Corporación BancoEstado ¿Cómo se Clasifica La Integridad?

a. **Baja, Media baja, Media, Media Alta, Alta.**
b. **Nivel 1, Nivel 2 y Nivel 3.**
c. **Baja, Media, Alta**
d. **Nivel 1 y Nivel 2**

16. ¿Qué es el Riesgo Inherente?

a. **Es el riesgo intrínseco de cada actividad.**
b. **Es el riesgo que subsiste, después de haber implementado controles.**
c. **El riesgo inherente es la probabilidad que un peligro se presente en una actividad de la organización.**
d. **Es el riesgo que tiene la organización.**

17. La usurpación de identidad se considera …

a. **Un Ataque**
b. **Un Riesgo**
c. **Una Amenaza**
d. **Una Vulnerabilidad**

18. ¿Cuál es el objetivo de realizar el Análisis de Riesgo?

a. **Identificar los Riesgos asociados al negocio.**
b. **Identificar las Amenazas asociadas al negocio.**
c. **Identificar las Amenazas de los Activos críticos.**
d. **Identificar y Clasificar las amenazas de los Activos Críticos.**

19. ¿Qué principio de la Seguridad de la informática viola el hecho de modificar la información que se trasmite a través de la red?

a. La Confidencialidad

b. La Integridad

c. La Autenticación

d. La Disponibilidad

20. ¿Qué principio de la Seguridad de la informática se incumple si tiene lugar un robo a través de la red del número de tarjeta de crédito?

a. La Confidencialidad

b. La Integridad

c. La Autenticación

d. La Disponibilidad

6.8 Decálogo de Buenas prácticas de seguridad de la información.

Dentro de la charla de concientización de un MGSI, se realizó otro plan de acción que corresponde a la creación de un decálogo de buenas prácticas. Lo cual obtuvo un resultado realmente bueno, debido a que, se logró que el equipo de trabajo tomara conciencia con respecto a los consejos dados sobre la seguridad de la información.

A continuación se muestran el decálogo de buenas prácticas expuesto a los analistas de datos:

Decálogo de Buenas Prácticas

- Utilice contraseñas seguras.
- Renueve sus contraseñas periódicamente.
- Cuidado con la información que expone en sus redes sociales.
- Mantenga su escritorio limpio.
- Mantenga las licencias de software al día.
- Use dispositivos de almacenamiento cifrados si la información es sensible.
- Bloquee sus equipos cada vez que abandona sus escritorios.
- Descargue y utilice software de fuentes confiables.
- Utilice solamente el correo institucional.
- No crea todo lo que lea en su correo electrónico.

6.9 Respaldos de Bases de Datos

Se realizó un seguimiento al plan de acción de respaldos de bases de datos.

A continuación se muestra el seguimiento que tuvo el control dentro del área de datos:

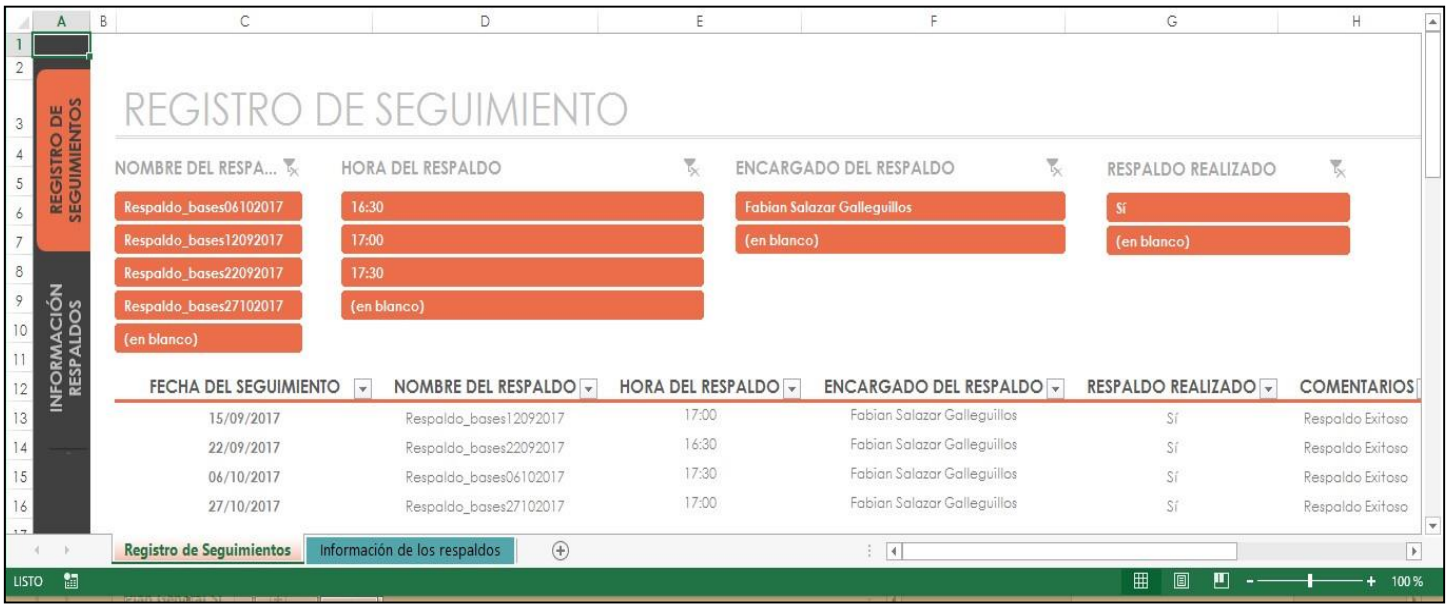


Figura 11: ***Seguimiento al plan de acción de respaldo de bases de datos.***

Figura 12: ***Seguimiento al plan de acción de respaldo de bases de datos.***

El impacto que tiene este control en el área es realmente increíble, puesto que, al realizar constantemente copias de seguridad de las bases de datos el riesgo de la pérdida total de la información por la materialización de alguna amenaza se reduce de gran manera, antes de comenzar los respaldos poseía el nivel del riesgo inherente es Alto, luego de aplicar este control el riesgo residual el nivel que hay en que se materialice dichas amenazas es No significativo, esto es simplemente porque siempre podremos recuperar los datos más recientes desde los respaldos hechos por este control.

6.10 Borrado seguro de dispositivos de almacenamiento

Cabe destacar que en este plan de acción lamentablemente no se pudo realizar sus seguimientos por falta de tiempo y apoyo de la dirección.

Este plan de acción es de borrado seguro de dispositivos de almacenamiento, el cual se deja especificado de la siguiente manera:

Procedimiento

- Para comenzar ejecutar el borrado seguro, los analistas deben analizar previamente la información del dispositivo de almacenamiento que se busca liberar su espacio, para luego, proceder a guardar en una carpeta llamada "Respaldo para Borrado Seguro Área de Datos" toda la información que los analistas no desean borrar.

- Luego el responsable de los respaldos procede a utilizar un disco duro, el cual será utilizado especialmente para respaldar la información seleccionada por los analistas en la carpeta "Respaldo para Borrado Seguro Área de Datos".

Supuesto 1: Este disco guardará solo una copia de seguridad, los respaldos que se vayan realizando a futuro se sobrescribirán.

Supuesto 2: El disco duro será formateado finalizando el año laboral que corresponde al último día hábil del año.

Supuesto 3: En el caso que el responsable de los respaldos desee seguir resguardando la información, deberá tener una autorización por correo asumiendo los riesgos. Esta autorización debe ser dada por el coordinador del área de datos, el jefe de Administración y finanzas (jefe directo del área de datos) y un analista de riesgo tecnológico y operacional, para así, el responsable de datos poder buscar su propio lugar de almacenamiento de la información.

Supuesto 4: El dispositivo de almacenamiento para borrado seguro será resguardado por el coordinador del área en un mobiliario seguro del área de datos.

- Una vez respaldada la información, El responsable de los respaldos procede a formatear de la siguiente manera el dispositivo de almacenamiento.

Paso 1: Conectar el dispositivo de almacenamiento al equipo.

Paso 2: ingresar a "este equipo" si es Windows 7, 8,10, en caso de ser en Windows xp, ingresar a "Mi pc".

Paso 3: hacer clic derecho sobre la unidad del dispositivo de almacenamiento y dar clic izquierdo en "formatear…".

Paso 4: al abrir las opciones de formateo, seleccionamos el checkbox de formateo rápido, y a continuación, iniciar.

Paso 5: desconecta el dispositivo de almacenamiento y se completa la planilla de seguimiento de borrado seguro de dispositivos de almacenamiento.

Supuesto 5: Si desea formatear su equipo de trabajo y/o respaldo, debe estrictamente comunicar y levantar la solicitud al área de soporte tecnológico.

En la cuarta etapa el análisis determinado fue el siguiente, en el centro de contacto específicamente en el área de datos se necesita realizar una inversión en seguridad de la información, porque esta área antes de comenzar este modelo de gestión de seguridad de la información se encontraba sin ningún tipo de medidas que velara por la confidencialidad, integridad y disponibilidad de la información, solamente confiaban en los contratos con los proveedores de los servidores que dispone el centro de contacto, por consiguiente, se propuso que para el siguiente ciclo de esta metodología se definiera un comité de seguridad que abarcara las tareas pendientes, tales como: Política de seguridad, Cumplimiento total de los controles que exige la normativa y actualizar todas las otras actividades ya realizadas.

7 Factibilidad

7.1 Alternativa A

Se realiza un estudio de factibilidad técnica, operativa y económica de la situación real del área de datos del BancoEstado Contacto 24 horas Lota.

7.1.1 Factibilidad Técnica

- Hardware

Gear SLIM-65a AMD Athlon 5150 es un computador de escritorio el cual cumple con los requisitos necesarios para realizar todas las actividades relacionadas a la implementación del proyecto.

Características

- Modelo: SLIM-65ª
- Sistema Operativo: Free DOS (Sin Sistema Operativo). Equipo Compatible con Windows 7, 8, 8.1 y 10.
- Procesador: AMD Athlon5150 1.6GHz (2M Caché)
- Número de núcleos: Quad Core
- Tarjeta de video: Graficas Radeon^{tm} R3 - Integrada
- Almacenamiento: 1TB,SATA III, 7.200 rpm
- Memoria RAM: 4GB DDR3L 1600MHZ – PC3 10600(1X4 GB), 2 Slot, Soporte máx. 16 GB
- Placa Madre: ASUS AMD AM1M-A
- Unidad Óptica: DVD-RW SATA 24X
- Teclado: Incluye Teclado Multimedia KSK-117K USB NEGRO
- Mouse: Incluye Mouse MS-117C Óptico USB Negro
- Parlantes: No incluye
- Audio: Realtek® ALC887-VD 8-Channel High Definition Audio
- LAN: Realtek® 8111GR, 1 x Gigabit LAN
- Puertos de acceso(frontal); 2 x entrada USB ; 1 x Audio, Micrófono
- Puertos de acceso(Posterior); 1 x PS/2 Teclado/Mouse; 1 x DVI-D; 1 x D-SUB(VGA); 1 x HDMI; 1 x LAN(RJ45); 2 X USB 3.0 ; 2 X USB 2.0; 3 X Audio Jack(s)

- Software

Estos son los componentes necesarios para la implementación de este modelo propuesto:

- Sistema Operativo
  - Windows 10 Pro
- Procesador de Texto
  - Microsoft Office Profesional 2016
- Navegador Web
  - Mozilla Firefox
  - Google Chrome

7.1.2 Factibilidad Operativa

BancoEstado Contacto 24 horas Lota es una filial de la institución bancaria Banco del Estado de Chile, cuando se trata de información bancaria ésta tiene una alta valoración para la organización, para ello, es muy relevante velar por su seguridad.

Tras reuniones con el directorio de la organización, germinó la idea de implementar un modelo de gestión de riesgos basado en la Nch-ISO 27.001, cuyo objetivo es gestionar los riesgos correctamente, con el fin de minimizar los costos que hay en la materialización de las amenazas a la información.

Como beneficio se puede recalcar que al gestionar incidentes permite al equipo de seguridad de la información tener un soporte sólido para sustentar ante gerencia un plan de inversión en seguridad de la información, donde con evidencias y con cálculos de los impactos que se pueden presentar ante la materialización de un incidente, es posible presentar de forma clara las posibles soluciones para la mitigación del riesgo de la materialización de eventos no deseados, y de esta forma poder garantizar que la inversión cubra las brechas de seguridad más importantes, y también, una medición de la eficacia de sus controles.

Otra de las ventajas que se tiene al gestionar incidentes son las evidencias, lo cual para casos de fraudes internos o externos nos permite entregar al área legal una prueba válida ante un posible proceso administrativo interno o judicial, para lo cual es conveniente que esta recopilación de evidencias se realicen cumpliendo las normas legales para este procedimiento.

La empresa teniendo en cuenta los impactos positivos que tiene la implementación de este modelo, está de acuerdo con la ejecución del proyecto propuesto.

7.1.3 Factibilidad Económica

7.1.3.1 Presupuesto del Proyecto

- Costo de Personal

La propuesta no estima que se deba realizar un gasto adicional en costos de personal, debido a que, el banco cuenta con el recurso humano adecuado para el desarrollo de este proyecto. El único costo de personal es el siguiente:

Presupuesto			
Recurso Humano	Sueldo Bruto	Descuentos legales	Sueldo liquido
Alumno Tesista	$ 333.333	$ 33.333	$ 300.000
Total Costo de Personal Mensual		$	300.000

Tabla 16: ***Presupuesto Costo de Personal***

- Costo de Capacitación al Personal

Se asume que la capacitación del diseño de este modelo está a cargo de un Alumno de la Universidad del Bío Bío en proceso de titulación, con el objetivo de obtener el título profesional de Ingeniería Civil en Informática.

- Costo de ISO 27001

Por decisión de la empresa no se debe realizar este gasto adicional, puesto que, el verdadero interés de la organización está en el modelo de gestión de riesgos, y no, en la certificación de la ISO 27001.

- Costo Hardware

La propuesta no estima que se deba realizar un gasto adicional en hardware.

El banco posee el hardware adecuado para la ejecución de este proyecto.

- Costo Software

La propuesta no estima que se deba realizar un gasto adicional en software.

El banco posee el Software adecuado para la ejecución de este proyecto.

- Costo de Implementación del Proyecto

Presupuesto			
Detalle	Valor en Pesos Chilenos (CLP)		Duración
Costo de Capacitación	$ -		6 meses
Costo de Personal Anual	$ 1.800.000		6 meses
Costo ISO 27001	$ -		-
Costo Hardware Anual	$ -		Sin estimar
Costo Software Anual	$ -		Sin estimar
Costo total Proyecto	$ 1.800.000	Duración Total del Proyecto	6 meses

Tabla 17: ***Presupuesto Implementación del Proyecto***

7.2 Alternativa B

Se realiza un estudio de factibilidad técnica, operativa y económica de una situación hipotética, en la que, una organización no cuenta con los recurso necesarios para la ejecución del diseño propuesto.

7.2.1 Factibilidad Técnica

Es idéntica a la factibilidad técnica de la alternativa A.

7.2.2 Factibilidad Operativa

Es idéntica a la factibilidad Operativa de la alternativa A.

7.2.3 Factibilidad Económica

7.2.3.1 Presupuesto del Proyecto

- Costo de Personal

La propuesta estima la necesidad de contar con un equipo de trabajo multidisciplinario, el cual está formado por 3 ingenieros civiles en informática y 2 ingenieros civil en industrial.

Estos trabajaran 9 horas diarias con derecho a 1 hora de colación al día, el horario corresponde de lunes a jueves de 09.00 am hasta 18.00 pm y viernes de 09.00 am hasta 15.00 pm.

Presupuesto				
Recurso Humano	Sueldo Bruto	Descuentos legales	Viáticos	Sueldo liquido
Ingeniero civil en Informática	$ 1.100.000	$ 209.000	$ 80.000	$ 971.000
Ingeniero civil en Informática	$ 1.100.000	$ 209.000	$ 80.000	$ 971.000
Ingeniero civil en Informática	$ 1.100.000	$ 209.000	$ 80.000	$ 971.000
Ingeniero Civil en Industrial	$ 1.100.000	$ 209.000	$ 80.000	$ 971.000
Ingeniero Civil en Industrial	$ 1.100.000	$ 209.000	$ 80.000	$ 971.000
Total Costo de Personal Mensual		$		4.855.000

Tabla 18: ***Presupuesto Costo de Personal***

*Descuentos Legales equivalen al 10% AFP, 7% Salud, 2% Comisiones de la AFP (puede variar)

- Costo de Capacitación al Personal

Presupuesto	
Nombre del curso	Sistema de Seguridad de la Información
Institución	RedCapacitacion Chile
Sitio web	http://www.redcapacitacion.cl/curso/sistemas-de-seguridad-de-la-informacion-iso-27001/1323
Valor por Persona	$ 315.000

Tabla 19: ***Presupuesto Costo de Capacitación al Personal***

- Costo de ISO 27001

Presupuesto		
Producto	Francos suizos (CHF)	Pesos chilenos(CLP)
full pack ISO 27001	118 fr.	$ 73.792

Tabla 20: ***Presupuesto Costo de la ISO 27001***

* Full pack ISO 27001 cuenta con PDF en color más una publicación online dada por la International Organization for Standardization (ISO), en español, Organización internacional de normalización.

**Es necesario comprar la ISO 27001 para poder en un futuro optar a la certificación.

*** Un franco suizo equivale aproximadamente 625,35 Pesos Chilenos.

- Costo Hardware

Presupuesto		
Producto	Cantidad	Valor Unitario
Gear SLIM-65a AMD Athlon 5150	5	$ 178.990
Total en Pesos Chilenos(CLP)	$	894.950

Tabla 21: ***Presupuesto Costo Hardware***

* Gear Slim-65a AMD Athlon 5150, es un computador de escritorio, el cual cumple con los requisitos necesarios para realizar las actividades del proyecto propuesto.

- Costo Software

Presupuesto		
Producto	Cantidad	Valor Unitario
Microsoft Office Profesional 2016	5	$ 349.990
Windows 10 Pro	5	$ 179.990
Total en Pesos Chilenos(CLP)	$	2.649.900

*Tabla 22****: Presupuesto Costo Software***

* Software necesario para realizar las actividades del proyecto propuesto.

- Costo de Implementación del Proyecto

Presupuesto				
Detalle	Valor en Pesos Chilenos (CLP)			Duración
Costo de Capacitación	$	315.000		3 semanas
Costo de Personal anual	$	66.000.000		12 meses
Costo ISO 27001	$	73.792		-
Costo Hardware Anual	$	894.950		12 meses
Costo Software Anual	$	2.649.900		12 meses
Costo total Proyecto	$	69.933.642	Duración Total del Proyecto	12 meses

Tabla 23: ***Presupuesto de Implementación del Proyecto***

7.3 Conclusión de la Factibilidad

Para determinar la viabilidad del proyecto se realizó el estudio de tres ítems cruciales, los cuales son, factibilidad técnica, operativa y económica.

Este estudio se realizó en dos casos diferentes, el primero de ellos (Supuesto A) es el caso real del diseño del modelo de gestión de seguridad de la información (MGSI) en el BancoEstado Contacto 24 horas Lota, y por último, está el segundo caso (Supuesto B) en el que se formula un caso hipotético donde la empresa no cuenta con ningún recurso requerido. Los valores utilizados son basados en las remuneraciones de la empresa y cotizaciones en el mercado en la actualidad.

Se concluye lo siguiente:

En primer lugar se analizó la factibilidad técnica en la que se describe los requerimientos de hardware y software necesarios para la correcta ejecución de proyecto, los resultados son buenos, puesto que, la empresa cuenta con el hardware y software adecuados.

En segundo lugar se analizó la factibilidad operativa en la que en los dos casos el resultado fue el mismo, la empresa es consciente de los beneficios que entrega el modelo, por lo tanto, está de acuerdo con la ejecución de este proyecto.

En tercer y último lugar se analizó la factibilidad económica, los resultados son sorprendentes, en el caso real la empresa solo necesita $1.800.000, este presupuesto se debe a la remuneración del alumno tesista a cargo de la ejecución del proyecto y la capacitación del equipo de trabajo en seguridad de la información, en el caso hipotético el presupuesto es de $69.933.642, la diferencia de los costos se debió a que la empresa cuenta con los recursos necesarios.

Finalmente el estudio realizado obtuvo resultados positivos en todos los ítems analizados, entonces, se concluye que el proyecto es factible para su ejecución en el BancoEstado Contacto 24 horas Lota.

8 Conclusión

Si bien la seguridad de información es un tema mundialmente reconocido, en la realidad universitaria no es un tema que se abarque con profundidad en una malla de pregrado, por esto, al comienzo de este proyecto todo era nuevo, al ser tema interesante de estudio fue un gran desafío, incentivándome a estudiar una normativa tan exigente, la cual nos entrega todos los requerimientos claves para desarrollar y mantener un modelo de gestión de la seguridad de la información que vela por la confidencialidad, disponibilidad e integridad de la información.

Durante el desarrollo extenso de este proyecto, pude adquirir habilidades blandas necesarias para desarrollarme dentro del mundo laboral, entendiendo que éstas son absolutamente necesarias para coordinar y gestionar un proyecto de este tipo.

Finalmente puedo concluir que un modelo de gestión de seguridad de la información, también abreviado MGSI, es un proyecto que necesariamente se debe aplicar en cualquier organización que depende de los datos obtenidos por y para los procesos que mantienen el funcionamiento de una empresa, debido a que, con un MGSI nos permite gestionar los riesgos, de tal manera, poder crear planes de acciones para mitigar la materialización de las amenazas que está expuesta la información, y así, reducir todo tipos de gastos extras que implica solucionar un problema ocasionado por estas mismas, además de esto, nos sirve para realizar un análisis de todos los procesos y poder determinar los activos que son críticos dentro de la organización.

A pesar que no se abarco completamente la normativa por falta de apoyo de la organización, por lo extenso que es aplicar todos los requerimientos de la Nch-ISO27001 y por falta de recurso humano, los resultados obtenidos por este MGSI fue realmente excelente, debido a que, se cumplieron en un 100% los objetivos propuestos, se logró reducir el impacto que tiene la materialización de una amenaza en particular, y lo más importante, es que el directorio del BancoEstado Contacto 24 horas lota al ver que realmente los resultados obtenidos le otorgan un valor agregado a la organización y ayudan a mantener la confidencialidad, integridad y disponibilidad de la información bancaria.

Por último, se consiguió plantar una semilla la cual en el año 2018 tomará fuerzas y comenzará a crecer, puesto que, la empresa invertirá los recursos necesarios para conseguir la certificación por esta norma tan prestigiosa.

9 Bibliografía

- BANCO.ITAU.CL. (2017). *ORGANIZACIÓN*, DE BANCO ITAU, SITIO WEB: HTTPS://BANCO.ITAU.CL/WPS/PORTAL/BICPUBLICO/SERVICIOALCLIENTE/INSTITUCIONAL/SOBREITAU/CB/01_ORGANIZACION/, FECHA DE CONSULTA: JULIO 20, 2017.
- BANCOESTADO (2017). *MISIÓN, VISIÓN Y VALORES CORPORATIVOS*. DE BANCO DEL ESTADO DE CHILE SITIO WEB: HTTP://WWW.CORPORATIVO.BANCOESTADO.CL/ACERCA-DEL-BANCOESTADO/PLAN-ESTRAT%C3%A9GICO/MISI%C3%B3N-VISI%C3%B3N-Y-VALORES-CORPORATIVOS, FECHA DE CONSULTA: ABRIL 10 ,2017.
- BANCOESTADO CONTACTO 24 HORAS (2017). CALENDARIO OFICIAL DE BANCOESTADO CONTACTO 24 HORAS S. A, FECHA DE CONSULTA: ABRIL 10, 2017.
- BBVA NOTICIAS. (2017). *ACERCA DEL GRUPO - BBVA NOTICIAS*, DE BANCO BBVA, SITIO WEB: HTTPS://WWW.BBVA.COM/ES/INFORMACION-CORPORATIVA/ACERCA-DEL-GRUPO/, FECHA DE CONSULTA: JULIO 20, 2017.
- CALIDAD TOTAL. (JULIO 8, 2012). WALTER SHEWHART, DE CALIDAD TOTAL: HTTP://CALIDAD.OVERBLOG.COM/WALTER-SHEWHART, FECHA DE CONSULTA: ABRIL 04, 2018.
- CISCO.COM (2017). ¿QUÉ ES UN FIREWALL? DE CISCO.COM. SITIO WEB: HTTPS://WWW.CISCO.COM/C/ES_MX/PRODUCTS/SECURITY/FIREWALLS/WHAT-IS-A-FIREWALL.HTML, FECHA DE CONSULTA: ABRIL 10, 2017.
- CORPORATIVO.BANCOESTADO.CL. (2017). *ACERCA DE BANCOESTADO*. DE BANCO DEL ESTADO DE CHILE SITIO WEB: HTTP://WWW.CORPORATIVO.BANCOESTADO.CL, FECHA DE CONSULTA: ABRIL 10 ,2017.
- GBM.SCOTIABANK.COM. (2017). *PREMIOS Y CLASIFICACIONES | GLOBAL BANKING AND MARKETS*. DE BANCO SCOTIABANK, SITIO WEB: HTTP://WWW.GBM.SCOTIABANK.COM/SPANISH/ABOUTUS/SAB_AWARDS_RANKINGS.HTM, FECHA DE CONSULTA: JULIO 20, 2017.
- GUÍA METODOLÓGICA 2014 (2014). GUÍA METODOLÓGICA 2014 PROGRAMA DE MEJORAMIENTO DE LA GESTIÓN Y METAS DE EFICIENCIA INSTITUCIONAL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN, DE GOBIERNO DE CHILE, SITIO WEB: HTTP://WWW.DIPRES.GOB.CL/594/ARTICLES-51683_INTRO_GUIA_METODOLOGICA05_2014.PDF, FECHA DE CONSULTA: JULIO 20, 2017.
- INFORME ANUAL 2016. (2017). RECONOCIMIENTOS. INFORME ANUAL 2016. PP. 6-7, DE BANCO SANTANDER CHILE, SITIO WEB: HTTPS://WWW.SANTANDER.CL/NUESTRO_BANCO/INFORMACION-

CORPORATIVA-MEMORIAS-FINANCIERAS.ASP, FECHA DE CONSULTA: JULIO 20, 2017.

- INSTITUTO NACIONAL DE NORMALIZACIÓN. (2013). EN NCH-ISO 27001-TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, DE INSTITUTO NACIONAL DE NORMALIZACIÓN, P. 3, FECHA DE CONSULTA: JULIO 20, 2017.
- INSTITUTO NACIONAL DE NORMALIZACIÓN. (2013). EN NCH-ISO 27001-TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, DE INSTITUTO NACIONAL DE NORMALIZACIÓN, PP. 13-27, FECHA DE CONSULTA: JULIO 20, 2017.
- INSTITUTO NACIONAL DE NORMALIZACIÓN. (2013). EN NCH-ISO 27001-TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, DE INSTITUTO NACIONAL DE NORMALIZACIÓN, P. 1, FECHA DE CONSULTA: JULIO 20, 2017.
- INSTITUTO NACIONAL DE NORMALIZACIÓN. (2013). EN NCH-ISO 27001-TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, DE INSTITUTO NACIONAL DE NORMALIZACIÓN, PP. 2-3, FECHA DE CONSULTA: JULIO 20, 2017.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (MARZO 13, 2017). ISO/IEC 27001- DATA PER COUNTRY AND SECTOR 2006 TO 2016, DE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION SITIO WEB: HTTP://ISOTC.ISO.ORG/LIVELINK/LIVELINK?FUNC=LL&OBJID=18808772 &OBJACTION=BROWSE&VIEWTYPE=1, FECHA DE CONSULTA: JULIO 20, 2017.
- ISO27000.ES (2017). ISO27000.ES -EL PORTAL DE ISO 27001 EN ESPAÑOL. GLORSARIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. DE ISO27000.ES, SITIO WEB: HTTP://WWW.ISO27000.ES/GLOSARIO.HTML, FECHA DE CONSULTA: JULIO 20, 2017.
- MAESTROS DE LA CALIDAD. (SEPTIEMBRE 23, 2012). WILLIAM EDWARDS DEMING MAESTROS DE LA CALIDAD, DE MAESTROS DE LA CALIDAD CONOCER LA VIDA Y FILOSOFÍA DE LOS DIFERENTES MAESTROS DE LA CALIDAD: HTTP://MAESTROSDELACALIDADAC103611.BLOGSPOT.CL/P/WILLIAM-EDWARD-DEMING_23.HTML, FECHA DE CONSULTA: ABRIL 04, 2018.
- MEMORIA ANUAL 2016. (2017, MARZO 01). HITOS 2016, RECONOCIMIENTOS 2016, FACTORES DE RIESGOS. MEMORIA ANUAL 2016, DE BANCO DE CHILE, PP. 10-11 Y PP. 86-89 SITIO WEB: HTTP://WW3.BANCOCHILE.CL/WPS/WCM/CONNECT/INVERSIONISTAS/P

ORTAL/MEMORIA-ANUAL-Y-REPORTE-20F/MEMORIA-ANUAL, FECHA DE CONSULTA: JULIO 20, 2017.

- MEMORIA INTEGRADA 2016. (2017, MARZO 28). PREMIOS Y RECONOCIMIENTOS. MEMORIA INTEGRADA 2016. PP. 25-28, DE BANCO DE CRÉDITOS E INVERSIONES, SITIO WEB: HTTPS://WWW.BCI.CL/INVESTOR-RELATIONS/MEMORIA-ANUAL/FILES/MEMORIA-ANUAL-2016, FECHA DE CONSULTA: JULIO 20, 2017.
- MENDOZA, M. (ABRIL 5, 2015). ¿QUÉ ES UNA DECLARACIÓN DE APLICABILIDAD? WELIVESECURITY. SITIO WEB: HTTPS://WWW.WELIVESECURITY.COM/LA-ES/2015/04/01/QUE-ES-DECLARACION-DE-APLICABILIDAD-SOA/, FECHA DE CONSULTA: ABRIL 12, 2017.
- MENESES BENÍTEZ, G. (2007). CURSO DE SISTEMAS DE GESTIÓN DE LA INFORMACIÓN SEGÚN LA NORMA UNE-ISO/IEC 27000, PP.11–15, FECHA DE CONSULTA: JULIO 20, 2017.
- METODOLOGÍA DE GESTIÓN DE RIESGO TECNOLÓGICO. (2017). DOCUMENTO INTERNO DEL BANCOESTADO CONTACTO 24 HORAS S.A, PP. 49-57, FECHA DE CONSULTA: JULIO 20, 2017.
- METODOLOGÍA DE GESTIÓN DE RIESGO TECNOLÓGICO. (2017). DOCUMENTO INTERNO DEL BANCOESTADO CONTACTO 24 HORAS S.A, PP. 3-4, FECHA DE CONSULTA: JULIO 20, 2017.
- METODOLOGÍA DE GESTIÓN DE RIESGO TECNOLÓGICO. (2017). DOCUMENTO INTERNO DEL BANCOESTADO CONTACTO 24 HORAS S.A, PP. 15-19, FECHA DE CONSULTA: JULIO 20, 2017.
- METODOLOGÍA RIESGO OPERACIONAL EN PROCESOS. (2017). DOCUMENTO INTERNO DEL BANCOESTADO CONTACTO 24 HORAS S.A, FECHA DE CONSULTA: JULIO 20, 2017.
- MUNDO SINACOFI (2010). SINACOFI: SISTEMA NACIONAL DE COMUNICACIONES FINANCIERAS. (2011). AVANZANDO A PASOS AGIGANTADOS EN SEGURIDAD, CALIDAD Y CONTINUIDAD DEL NEGOCIO. DE SINACOFI. P. 30, SITIO WEB: HTTPS://WWW.SINACOFI.CL/DOCUMENTOS/BOLETINES/2010_EDICION_ANUAL_OK.PDF, FECHA DE CONSULTA: JULIO 20, 2017.
- PESO, RAMOS Y PESO (2014). LA SEGURIDAD: PIEZA FUNDAMENTAL DE LA NUEVA SOCIEDAD, DE EL DOCUMENTO DE SEGURIDAD (ANÁLISIS TÉCNICO Y JURÍDICO. MODELO), P. 13, FECHA DE CONSULTA: JULIO 20, 2017.