ESCUELA DE NEGOCIOS
DEPARTAMENTO DE INGENIERÍA COMERCIAL
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

UNIVERSIDAD TÉCNICA FEDERIO SANTA MARÍA

Escuela de Negocios Departamento de Ingeniería Comercial

MBA, Magíster en Gestión Empresarial

PROPUESTA DE UN MODELO ESTRATÉGICO DE SEGURIDAD DIGITAL PARA EMPRESAS EN EL MUNDO DIGITAL

Tesina de Grado presentada por

Jorge Antonio Baeza Guerra

Como requisito para optar al grado de

MBA, Magister en Gestión Empresarial

Guía de Tesina Dr. Lionel Valenzuela O.

Noviembre de 2018

TITULO DE TESINA: **“PROPUESTA DE UN MODELO ESTRATÉGICO DE SEGURIDAD DIGITAL PARA EMPRESAS EN EL MUNDO DIGITAL”**

AUTOR: **Jorge Antonio Baeza Guerra**

TRABAJO DE TESINA, presentando en cumplimiento parcial de los requisitos para el Grado de MBA Magíster en Gestión Empresarial de la Universidad Técnica Federico Santa María.

Observaciones

_____

COMISION TESINA: Lionel Valenzuela O.

Pablo Isla M.

José Miguel Gonzalez M.

Santiago, Noviembre 2018.

Todo el contenido, análisis, conclusiones y opiniones vertidas en este estudio son de mi exclusiva responsabilidad.

Nombre: JORGE A BAEZA GUERRA

Fecha: 8 Noviembre 2018

Agradezco a mi amada esposa Claudia y mi amado hijo Darek, por haberme apoyado y entendido en este proyecto de MBA, por cada fin de semana y cada día que no estuve con ellos.

CONTENIDO

Índice de Tablas

Índice de Figuras

Resumen

La cuarta revolución industrial, la economía digital, las empresas digitales, el ciberespacio, el mundo digital llegó para quedarse, las compañías mediante la digitalización están cambiando la forma tradicional en como ofrecen sus servicios y productos, es un cambio radical para las empresas que llevan tiempo en el mercado de manera tradicional, algunas empresas se han visto en dificultades dentro de este mundo digital, donde también los consumidores cambiaron, cambio la forma en como los consumidores hacen sus requerimientos al mercado, es decir la digitalización está cambiando el juego y los jugadores, mediante una larga lista de tecnologías emergentes, que pasan a conformar un espacio diferente donde se transan productos y servicios, el mercado digital, el mundo digital.

En la actualidad es impensable no acceder a productos y servicios mediante un Smartphone, la movilidad al alcance de todos, diferentes empresas han tenido que entender este cambio y han tenido que hacer modificaciones en la forma de ofrecer sus productos, algunas empresas incluso han tenido que cambiar su estrategia, otras por el contrario han ido sucumbiendo a este proceso, empresas que fueron exitosas han ido desapareciendo y muchas lo seguirán haciendo, las empresas que no se adapten al mundo digital, las empresas que no puedan llevar un proceso exitoso de transformación digital, serán menos competitivas en este mercado y su existencia estará en juego.

Pero que hace que las empresas se vean enfrentadas a problemas en este mercado digital, existen diferentes aristas que analizar y considerar para ser exitoso en la economía digital, una importante arista es la Seguridad Digital, la seguridad de los datos en el ciberespacio, la seguridad de las transacciones en el mercado digital, la seguridad de la información en el mundo digital, esta variable es una de las que puede llevar a una empresa a verse involucrada en graves problemas , incluso a raíz de un problema de seguridad digital puede poner en juego su futuro como compañía, existe un amplio historial de empresas en el mundo que se han visto envueltas en problemas de seguridad digital, problemas que pueden afectar a la imagen de la empresa, a la operación e incluso a las finanzas de las compañías y Chile no es la excepción.

En el último tiempo Chile se ha visto enfrentado a una avalancha de cambios a raíz de graves incidentes de seguridad digital que el país se ha visto enfrentado, incidentes que afectan la economía digital del país, el tema de la seguridad digital en estos tiempos tiene prioridad nacional, economistas estiman que un país con problemas en su seguridad digital, no es un país atractivo para inversionistas, por lo tanto, es necesario tomar acciones al respecto.

Este trabajo aporta justamente en eso, en proponer una estrategia de Seguridad Digital, entregar herramientas a las empresas que están en proceso de transformación digital, empresas que ya están en el mundo digital y aquellas que van hacia este proceso, este trabajo propone un modelo estratégico de cómo

abordar esta problemática, un modelo aplicable a cualquier tipo de empresa, independiente de la industria, este modelo entrega todas las herramientas necesarias para poder evitar, prevenir de manera proactiva incidentes de Seguridad Digital, estableciendo un modelo empresarial para controlar los riesgos en el ciberespacio.

Extracto

El presente trabajo tiene como objetivo desarrollar una propuesta de un Modelo de Seguridad Digital para la empresa, modelo que permita desarrollar una adecuada estrategia para enfrentar el proceso de Transformación Digital del punto de vista de la Seguridad Digital.

Se realizará una investigación de los principales desafíos de la Seguridad Digital, a nivel estratégico y también del punto de vista tecnológico, estratégico porque existen una serie de decisiones que tomar cuando se define una estrategia de Seguridad Digital, representa un cambio no menor en las organizaciones, algo que las empresas no quisieran es que su estrategia de Transformación Digital se vea truncada por un problema de seguridad.

También se investigará cómo se está enfrentando esta problemática en Chile, qué decisiones se están tomando al respecto, qué estrategias existen, cuáles son las brechas si se compara con modelos internacionales o con países desarrollados, para posterior analizar modelos que sean aplicables a la Seguridad Digital para finalmente realizar una propuesta de un modelo que sea aplicable a Chile y que permita desarrollar una adecuada estrategia de Seguridad Digital, con el objeto de que el proceso de Transformación Digital, ni la empresa en general se vea afectada por un problema de Seguridad Digital.

1. Introducción

La Transformación Digital es la revolución industrial del siglo XXI. La Innovación y los avances tecnológicos están cambiando la vida en general y también los modelos económicos.

Abordar una transformación digital se supone un cambio cultural no menor. Significa establecer nuevos valores, manejar otros modelos de relación y adquirir nuevas capacidades y herramientas, nuevas formas de hacer negocios para las empresas, un mundo global conectado, una serie de oportunidades para la innovación digital. Pero también se tiene que entender que hay nuevos retos. Es el momento de asumir una nueva cultura de riesgo, los beneficios de un proceso de Transformación Digital se pueden ver truncados sin una adecuada estrategia de Seguridad Digital.

Los beneficios de la transformación digital son evidentes, se pueden simplificar las operaciones y los procesos ahorrando tiempo y dinero, facilita la apertura a nuevos mercados o nuevos modelos de negocio diferentes a los tradicionales, con un foco especial en la experiencia del cliente. Por otra parte los clientes o consumidores tienen un apetito por toda las innovaciones digitales, facilitan la vida y entregan un acceso al producto o servicio con un par de toques en un Smartphone, es la época de los Smart, Smartphone , teléfonos inteligentes con capacidades para conectar con el mundo y obtener diferentes tipos de productos y servicios, los televisores se convierten en Smart TV, un televisor ya no sólo tiene la función de ver televisión abierta, es posible realizar compras y acceder a variados servicios, los relojes dan paso a los Smartwatches, relojes inteligentes donde también es posible realizar transacciones, esto significa que las empresas tienen nuevos modelos de negocios a definir, se deben transformar digitalmente si quieren seguir siendo competitivas.

La Transformación Digital ha de verse como una estrategia. Cada empresa, cada unidad de negocio debe conocer y valorar las herramientas tecnológicas facilitadoras que puede aplicar a sus procesos en cada eslabón de la cadena de valor, por lo tanto la Seguridad Digital también debe transformarse en una estrategia, la cual camina de la mano con la estrategia de Transformación Digital.

2. Origen y propósito del estudio

El origen de este estudio nace como una forma de generar valor en un proceso actual que se está viviendo, en esta transición, en esta llamada “Cuarta Revolución Industrial”, la Transformación Digital tiene que ir de la mano con una estrategia de Seguridad Digital, en la actualidad no se está ajeno a incidentes de Seguridad que puedan generar más de algún problema a las empresas digitalizadas o en proceso, truncando de esta manera sus objetivos, sus proyectos, poniendo en riesgo sus productos y servicios, comprometiendo muchas veces a sus clientes.

Por eso la idea es realizar una propuesta de un modelo aplicable a la realidad Chilena, que pueda ser replicado, que permita enfrentar la problemática de la Seguridad Digital, que permita desarrollar una estrategia de Seguridad Digital, que trabaje en conjunto con la estrategia de Transformación Digital y a la vez con la estrategia corporativa.

Para ello será necesario analizar la situación actual en el mundo y en Chile, determinar las brechas existentes, analizar modelos internacionales de seguridad digital y proponer una medida de mejora a estas brechas, para establecer de esta manera una estrategia de Seguridad Digital mediante un modelo estratégico, que permita tomar decisiones a la alta gerencia de cuáles son los riesgos que se podrían ver enfrentados frente a un una determinada estrategia de Transformación Digital, poder establecer remediaciones de manera proactiva y no reactiva o cambiar la estrategia si el riesgo es mayor que la decisión misma de seguir adelante con una decisión de negocio.

3. Justificación

¿Qué es la Transformación Digital?, citando algunos estudios, la empresa de tecnología (SAP, 2017) dice que el proceso de transformación digital es un “Cambio en el funcionamiento de los negocios”, (IDG, 2018) comenta que la transformación digital permite a las empresas “Reducción de Costes”, (Fundación Telefonica, 2015) dice que nos enfrentamos a un “Cambio de realidad, vivimos en un mundo conectado”.

Sin embargo, la problemática es cuál estrategia se define, para evitar que el proceso de transformación digital fracase por un problema de seguridad digital. Recientemente la red social Facebook por un mal uso de la información, se vio

enfrentada a diversos problemas que incluso llevaron a su CEO a dar explicaciones al Congreso de EEUU (CNN Español, 2018), esto también significó pérdidas en su valor bursátil como compañía (de USD190 bajó a USD150 por acción) (Yahoo Finance, 2018).

Por lo tanto, un problema de seguridad digital puede llevar a problemas operacionales, problemas de imagen corporativa, pérdidas financieras, problemas legales, e incluso, dependiendo del tipo de empresa puede llevar a su inviabilidad en el tiempo.

Por este motivo, proponer una estrategia de innovación de seguridad digital, aportará a evitar que la estrategia de Transformación Digital fracase y a las empresas ya digitalizadas les permitirá que la empresa siga siendo competitiva y viable en el tiempo

4. Objetivos

4.1 Objetivo Principal

Proponer un modelo de Innovación de Seguridad Digital, acotado, práctico y efectivo, agregando valor de modo que permita a la empresa afrontar adecuadamente los desafíos de la Transformación Digital, desafíos que van desde evitar problemas operacionales, problemas de imagen corporativa, pérdidas financieras, problemas legales, hasta evitar la inviabilidad en el tiempo de la empresa, demostrando que la seguridad digital es un proceso estratégico que va de la mano con la estrategia corporativa de las empresas.

4.2 Objetivos Específicos

- ✓ Identificar los principales desafíos de la transformación digital del punto de vista estratégico y de seguridad digital, cuál es la situación actual general a nivel mundial.
- ✓ Identificar la situación actual en Chile en seguridad digital.
- ✓ Analizar modelos aplicables a seguridad digital utilizados a nivel mundial.

- ✓ Proponer un modelo de Seguridad Digital, que permita enfrentar los desafíos de la Transformación Digital.

5. Alcance del Estudio

El estudio se centrará principalmente en el proceso de Transformación Digital que enfrentan las empresas, visto desde la perspectiva de la Seguridad Digital, con un alcance exploratorio y descriptivo, en lo que respecta a analizar los principales desafíos estratégicos y tecnológicos que deben abordar las empresas en camino a la digitalización, como también el análisis de modelos internacionales de Seguridad Digital. El estudio también considera a las empresas que ya están en el mundo digital, el modelo podrá ser aplicado en ambas empresas las que están definiendo su estrategia y las que ya están en el mundo digital.

6. Metodología de trabajo

Para llevar a cabo este estudio, la metodología a utilizar constará de varias etapas. La primera consistente en la recopilación de información necesaria para sentar las bases del análisis, información de estudios realizados por diferentes empresas del sector internacional para el caso de determinar los desafíos de la Transformación y Seguridad Digital. Para el caso de conocer la realidad actual en Chile será necesario tomar contacto con centros de estudios nacionales e internacionales donde obtener información de estudios relacionados y poder ir estableciendo una medición del nivel nacional.

Para el análisis de modelos será necesario investigar en empresas normativas británicas y americanas principalmente, para realizar la propuesta, de acuerdo a los análisis y estudios realizados, ocupando la experiencia laboral y los conocimientos adquiridos en el tema se realizará una propuesta que posicione a las empresas a un nivel internacional y a la vez puedan tener bajo control los riesgos de seguridad digital en un proceso de transformación, desarrollo y administración de Transformación Digital.

6.1 Metodología para Obtención de Información

A continuación de describe la metodología utilizada para la obtención y análisis de la información.

6.1.1 Recopilación de la Información

La información será obtenida de la siguiente manera:

- ✓ Investigación de estudios realizados por empresas del rubro digital, proveedores de servicios principalmente y centros de estudios internacionales.

- ✓ Investigación de noticias y acontecimientos relacionados que hayan ocurrido en el campo de la Seguridad Digital.

- ✓ Investigación de estudios realizados por centros de estudios y organizaciones nacionales (Chile) para poder determinar la realidad del país.

- ✓ Investigación en empresas normativas americanas y británicas para analizar modelos de seguridad digital.

6.1.2 Análisis de la Información

En una primera fase, se clasificará la información recopilada con el fin de valorizar su aporte al resultado final del estudio.

Posteriormente, se analizará la información recopilada y obtenida de diferentes fuentes, lo primero es poder detectar los desafíos de la Transformación Digital dando una mirada del punto de vista estratégico y de la Seguridad Digital.

Se analizará la información para obtener un estándar en lo que respecta a los desafíos, si bien el tema es amplio la idea es poder establecer desafíos que son comunes a cualquier tipo de empresa, independiente de la estrategia de Transformación Digital, la idea es poder determinar desafíos de Seguridad Digital que sean comunes de acuerdo a estrategias estándares de Transformación

Digital, donde se realizará también un análisis de los desafíos tecnológicos, pudiendo de esta manera construir una estrategia estándar de Seguridad Digital, identificando los desafíos que serán comunes para las empresas.

En el análisis interno en Chile la idea es poder analizar la información recopilada y poder determinar la realidad del país, que están haciendo las empresas en términos de transformación digital y cuál es su estrategia de Seguridad Digital asociada, cual es el nivel de madurez de Chile en Seguridad Digital. Estas estrategias serán comparadas con los análisis de los modelos internacionales donde se podrá determinar las brechas más relevantes para poder abordarlos en la propuesta del modelo final.

Respecto a los modelos internacionales, la idea es sacar lo mejor de cada modelo y crear un único modelo con las mejores prácticas a nivel mundial, que permitan adoptar una estrategia que sea transversal a la mayor parte de las empresas, estrategia y modelo que será la propuesta final de este estudio, que aporte valor evitando que las empresas vean truncadas sus estrategia de Transformación Digital o su desarrollo de esta por problemas de Seguridad Digital.

Finalmente se realizará una propuesta de modelo a aplicar, tomando en consideración el análisis de los modelos mayormente utilizados a nivel mundial, como también las consideraciones de acuerdo a las brechas que sean detectadas, para en un futuro validar el modelo en una empresa chilena.

7. Estado del Arte y Marco Teórico

7.1 Antecedentes

7.1.1 Transformación Digital

No han pasado muchos años y, sin embargo, cuesta recordar el tiempo en que la tecnología móvil era un lujo reservado para unos pocos. Parece que siempre hubiera existido, es parte de la cotidianidad e instrumento fundamental para la vida en sociedad. El teléfono móvil es una clase de súper-extensión del cuerpo, un cerebro con la capacidad de conectar con el entorno.
Actualmente, en algunos lugares del mundo, es más fácil tener un teléfono inteligente que un baño o agua potable. Según estimaciones de la Organización de Naciones Unidas (ONU), en el mundo hay más personas con acceso a teléfonos móviles que a baños limpios. (Fundación Telefonica, 2015)

De la época anterior, cuando los móviles tenían un alto precio y eran aparatos enormes, a la actual, no ha pasado mucho en comparación con el tiempo que han

necesitado otros grandes cambios en la vida social; sin embargo, los avances tecnológicos en dispositivos inalámbricos que permiten estar comunicados parecen no detenerse y continúan sorprendiendo a diario. De ser equipos que necesitaban una funda y protectores de pantalla, y mantenerlos lejos del agua y el polvo, ahora los móviles son dispositivos mucho más resistentes. Y la razón es sencilla: se vive en todo tipo de ambientes y el móvil vive con las personas.

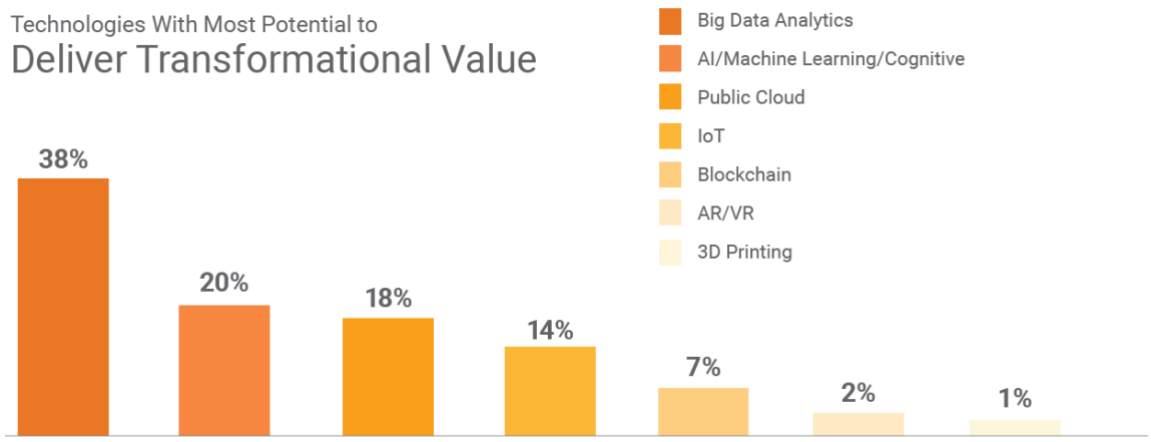
La vida está pasando a ser completamente móvil. No sólo se habla, también se come, se camina y se duerme con teléfonos. Es difícil pensar en una herramienta con la que se haya logrado tan estrecha relación como con los dispositivos móviles, y en tan poco tiempo. El teléfono móvil se ha convertido en una extensión, reducida en tamaño pero infinita en información, datos y funciones a los que se puede acceder (la banca, la identidad, productos y servicios)

La movilidad y funcionalidades que tienen estos dispositivos no sólo permiten que se pueda tomar fotografías en cualquier momento, también llevan a lugares lejanos que pueden ser de interés de las personas.

En todos los rincones del mundo y dentro de cada industria, las organizaciones están modernizando las formas en que interactúan con sus empleados, socios y clientes. La transformación digital promete cambiar drásticamente la forma en que las empresas se adaptan a nuevos mercados y presiones competitivas. También los hará mucho más receptivos y ágiles. Pero para lograr esta transformación digital, las organizaciones tienen que salir de su zona de confort para evaluar y adoptar una o más tecnologías emergentes disruptivas. (ISACA, 2017)

Las tecnologías que mayor valor aportan a la transformación digital son las siguientes:

Figura N° 1: Tecnologías con mayor potencial para entregar valor transformacional



Fuente: (ISACA, 2017)

Las cinco primeras son:

Big Data / Analytics: Conjuntos de datos que permiten a las organizaciones analizar, buscar, compartir y visualizar imágenes masivas de volúmenes de datos en áreas tan variadas como procesar información médica para comprender comportamiento del consumidor. (ISACA, 2017)

Inteligencia Artificial / Machine Learning / Tecnologías Cognitivas: Programas que realizan tareas mucho más rápido que las personas, en áreas como la medicina, comercio electrónico, robótica, detección remota y tecnologías de protección digital. (ISACA, 2017)

Cloud Público: Es un estilo de computación donde las capacidades escalables y elásticas habilitadas por TI se brindan como un servicio a clientes externos que utilizan tecnologías de internet, es decir puede admitir clientes que son externos a la organización del proveedor, generando economías de escala y uso compartido de recursos que permiten reducir costos en incrementar las opciones tecnológicas. (ISACA, 2017)

Internet de las cosas: Permite a una organización usar dispositivos “inteligentes” que pueden recopilar y transmitir datos en energía, vigilancia, transporte, monitoreo ambiental y otras industrias. (ISACA, 2017)

Blockchain: Tecnología que permite automatizar el libro mayor de una organización para facilitar las transacciones en línea, con la característica que no existen intermediaros en las transacciones, descentralizando toda la gestión, el control del proceso es de los usuarios, no de la entidad financiera. (ISACA, 2017)

Alfabetización digital, riesgo y transformación Digital

Las tecnologías emergentes que se consideran las más transformacionales también plantean los desafíos más organizacionales en términos de riesgo percibido y resistencia general al cambio.
El Ceo de ISACA Matt Loeb (ISACA, 2017) dijo que los líderes alfabetizados digitalmente son más propensos a emplear la debida diligencia para evaluar holísticamente el valor del negocio contra las tolerancias de riesgo de la organización: "Las organizaciones con liderazgo digitalmente alfabetizado están más abiertas a tomar riesgos, ver más claramente los beneficios de las tecnologías emergentes, y son más propensos a iniciar pilotos para examinar minuciosamente estas tecnologías”.

De hecho, la transformación digital debería verse como una estrategia global para la empresa, y sus beneficios deberían ser destacados, con el fin de convencer a todas las partes interesadas de su valor para la organización. Sin embargo, un digital bien formado debe saber que la transformación que se basa en tecnologías emergentes donde también debe incluir un análisis de la gestión de riesgos o amenazas, evaluando para proteger a la empresa de posibles contratiempos.

Características imprescindibles de la tecnología emergente

No es secreto que no todos los intentos de transformar un negocio tienen éxito. Si una organización tiene menos propensión para probar nuevas tecnologías emergentes, ¿es más probable que no complete su transformación digital? ¿Intentan las tecnologías emergentes ayudar a una organización en su camino hacia la transformación digital?
Las respuestas a estas preguntas se pueden encontrar en el proceso por el cual las empresas evalúan las tecnologías emergentes.
Las organizaciones que incluyen más voces y partes interesadas en el proceso parecen tener más éxito. En casi un 10 por ciento de margen, las empresas administradas por líderes alfabetizados digitalmente dependen menos del grupo de TI que actúa por sí solo para hacer evaluaciones de tecnología (37 por ciento a 46 por ciento). Y, por casi el mismo margen, están las organizaciones que confían más en equipos interdisciplinarios para examinar y probar tecnologías (34 por ciento a 26 por ciento) (Figura N° 2). (ISACA, 2017)

Figura N° 2: Factores que deben tener las tecnologías emergentes

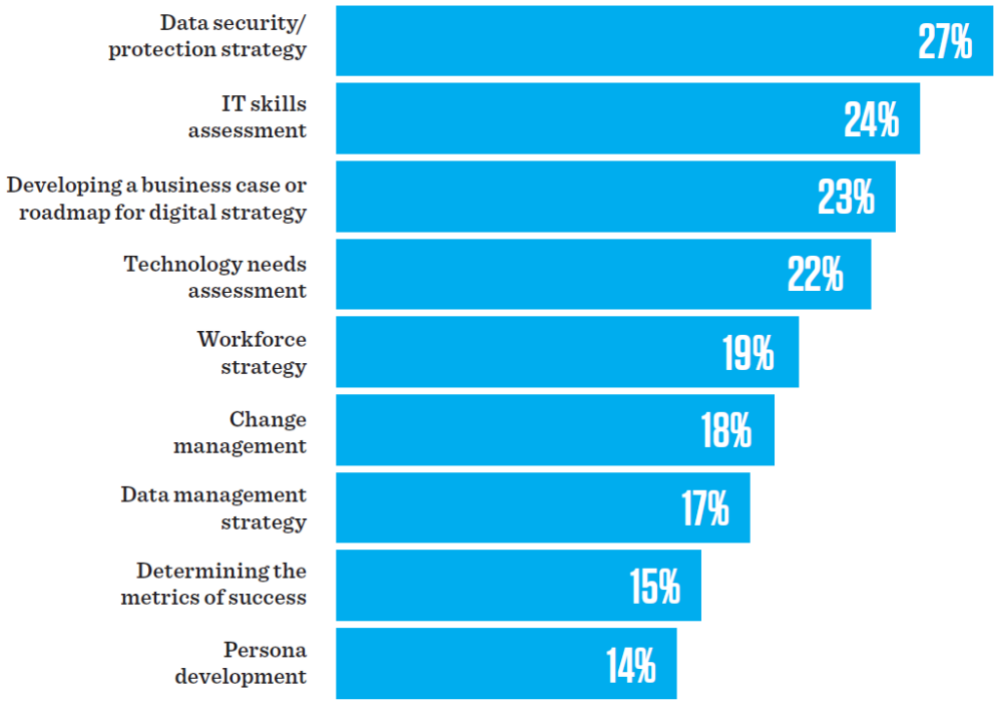
Fuente: (ISACA, 2017)

También se puede apreciar en la Figura N° 2 que la condición de riesgo es relevante para la tecnología, un 67% de los lideres digitales lo señalan según el

estudio de (ISACA, 2017), es decir es uno de los factores relevantes para el éxito del proceso.

En un estudio realizado por (IDG, 2018), donde consultaron por los pasos que seguían las organizaciones para caminar hacia un negocio digital, los resultados fueron los siguientes (Figura N°3)

Figura N° 3: Cuales son los pasos de una organización para convertirse en un negocio digital



Fuente: (IDG, 2018)

Para convertirse en un negocio totalmente digital, hay pasos necesarios y acciones que las organizaciones deben completar. El ritmo de la gestión del cambio organizacional para la mayoría de las organizaciones en transformación digital.

Más de la mitad de las organizaciones ya tiene datos, análisis, tecnología móvil y nube privada implementada en su organización y más de la mitad están probando o investigando Inteligencia artificial e internet de las cosas.

Sin embargo, solo el 27% ha implementado una estrategia de protección y de seguridad de los datos (Data Security/Strategy protection), las organizaciones aún están en el proceso de determinar roles y responsabilidades mientras adaptan a la cultura de la organización al nuevo entorno digital, en la Figura N°3 se pueden apreciar los porcentajes de empresas en cada ámbito de los pasos relevantes para una conversión digital. (IDG, 2018)

7.1.2 Seguridad Digital

El uso de las Tecnologías de la Información y de la Comunicación se ha incorporado de forma general a la vida cotidiana de las personas. Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero, al mismo tiempo, conlleva serios riesgos y amenazas que pueden afectar a empresas y personas.

Varios son los factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio. La rentabilidad que ofrece su explotación en términos económicos, políticos o de otro tipo, la facilidad y el bajo coste de empleo de las herramientas utilizadas para la consecución de ataques, y la facilidad de ocultación del atacante hacen posible que estas actividades se lleven a cabo de forma anónima y desde cualquier lugar del mundo, con impactos transversales sobre los sectores público y privado y los propios ciudadanos.

Variados pueden ser los impactos de un problema de Seguridad Digital, desde a afectar a personas como también pueden afectar al normal funcionamiento de una empresa o un país.

La interdependencia cibernética impulsa el riesgo global

Según el World Economic Forum 2017, la creciente interdependencia cibernética de las redes de infraestructura es uno de los principales factores de riesgo del mundo. El Informe de riesgos globales de WEF 2017 (World Economic Forum, 2017) descubrió que los ataques cibernéticos, las fallas en el software y otros factores podrían provocar fallas sistémicas que "se propagan a través de las redes y afectan a la sociedad de maneras imprevistas".

El reciente informe de tendencias mundiales del Consejo Nacional de Inteligencia e USA (Office of the Director National Intelligence, 2018) advirtió de manera similar que la sociedad enfrenta un riesgo "inminente" de disrupción cibernética - potencialmente a gran escala con "consecuencias letales" -debido a la vulnerabilidad de la infraestructura crítica. Los estudios de casos de desastres no cibernéticos dan muestra que los eventos en cascada a menudo comienzan con la pérdida de potencia y muchos sistemas se ven afectados instantáneamente o en un día, lo que significa que generalmente hay un tiempo precioso para abordar el

problema inicial antes de que caiga en cascada. Las interdependencias entre redes críticas y no críticas a menudo se ven inadvertidas hasta que ocurra un problema.
Muchas personas en todo el mundo -particularmente en Japón, Estados Unidos, Alemania, el Reino Unido y Corea del Sur- están preocupadas por los ataques cibernéticos de otros países. (PEW Research Center, 2017)

Las herramientas para llevar a cabo ciberataques están proliferando en todo el mundo. Las naciones más pequeñas pretenden desarrollar capacidades como las que usan los países más grandes. Y la filtración de las herramientas de piratería de la Agencia Nacional de Seguridad (NSA) de Estados Unidos ha hecho que las capacidades altamente sofisticadas estén disponibles para hackers maliciosos. (PWC, 2018)

Cuando se producen ataques cibernéticos, la mayoría de las empresas victimizadas dicen que no pueden identificar claramente a los culpables. Según (PWC, 2018), solo el 39% de los encuestados afirma tener mucha confianza en sus capacidades de atribución.

Estrategia de Seguridad Digital

Según (PWC, 2018), se comenta que la frecuencia de organizaciones que poseen una estrategia general de Seguridad Digital es particularmente alta en Japón (72%), donde los ciberataques se consideran la principal amenaza de seguridad nacional, y Malasia (74%), que obtuvo una muy buena calificación en el índice de ciberseguridad de la ONU. Ambos países se encuentran en el este de Asia y el Pacífico, una región donde el Foro Económico Mundial dice que los ciberataques se encuentran entre los cinco principales riesgos comerciales. (Worl Economic Forum, 2018).

La alta preparación no significa necesariamente bajo riesgo. El Índice Global de Ciberseguridad 2017 de la ONU ubicó a Estados Unidos entre los estados miembros más comprometidos con la seguridad cibernética, solo superado por Singapur. Pero la infraestructura de los Estados Unidos sigue siendo vulnerable a lo que el Foro Económico Mundial considera el principal riesgo comercial en América del Norte: "ciberataques a gran escala o malware que causan grandes daños económicos, tensiones geopolíticas o una pérdida generalizada de confianza en Internet". (World Economic Forum, 2017)

El Departamento de Seguridad Nacional de los EE. UU. Identificó más de 60 entidades en infraestructura crítica de los EE. UU. Donde el daño causado por un solo incidente cibernético podría generar razonablemente $ 50 mil millones en

daños económicos o 2.500 muertes inmediatas o una grave degradación de la defensa nacional de EE. UU. (Congress GOV USA, 2018)

Para muchas personas, el riesgo es real. Una encuesta del Pew Research Center descubrió que una gran mayoría de los estadounidenses esperan grandes ataques cibernéticos en los próximos cinco años en la infraestructura pública de los EE. UU. O en los sistemas bancarios y financieros. La mayoría de los profesionales de la seguridad de la información creen que la infraestructura crítica de EE. UU. Sufrirá un ataque cibernético dentro de los próximos dos años. (BlackHat USA , 2017)

Responsabilidad corporativa de la Seguridad Digital

Que se dice de la responsabilidad corporativa en Seguridad Digital, ¿este tema debería estar en los directorios? Según (PWC, 2018), la mayoría de los directorios corporativos no están modelando de manera proactiva las estrategias de Seguridad Digital o los planes de inversión de sus compañías.

Sólo el 44% de los encuestados (PWC, 2018) dice que sus juntas corporativas participan activamente en la estrategia general de seguridad de sus empresas. **"Muchas juntas aún lo ven como un problema de TI",** dijo Matt Olsen, cofundador y presidente de desarrollo comercial y estrategia para IronNet Cybersecurity y ex jefe del Centro Nacional de Contraterrorismo de Estados Unidos.
Según las encuestas de directores de empresas públicas y privadas de la Asociación Nacional de Directores Corporativos para 2016-2017, pocos miembros de la junta se sienten muy seguros de que sus empresas estén debidamente protegidas contra ataques cibernéticos. (NACD Director's Handbook on Cyber-Risk Oversight, 2018).

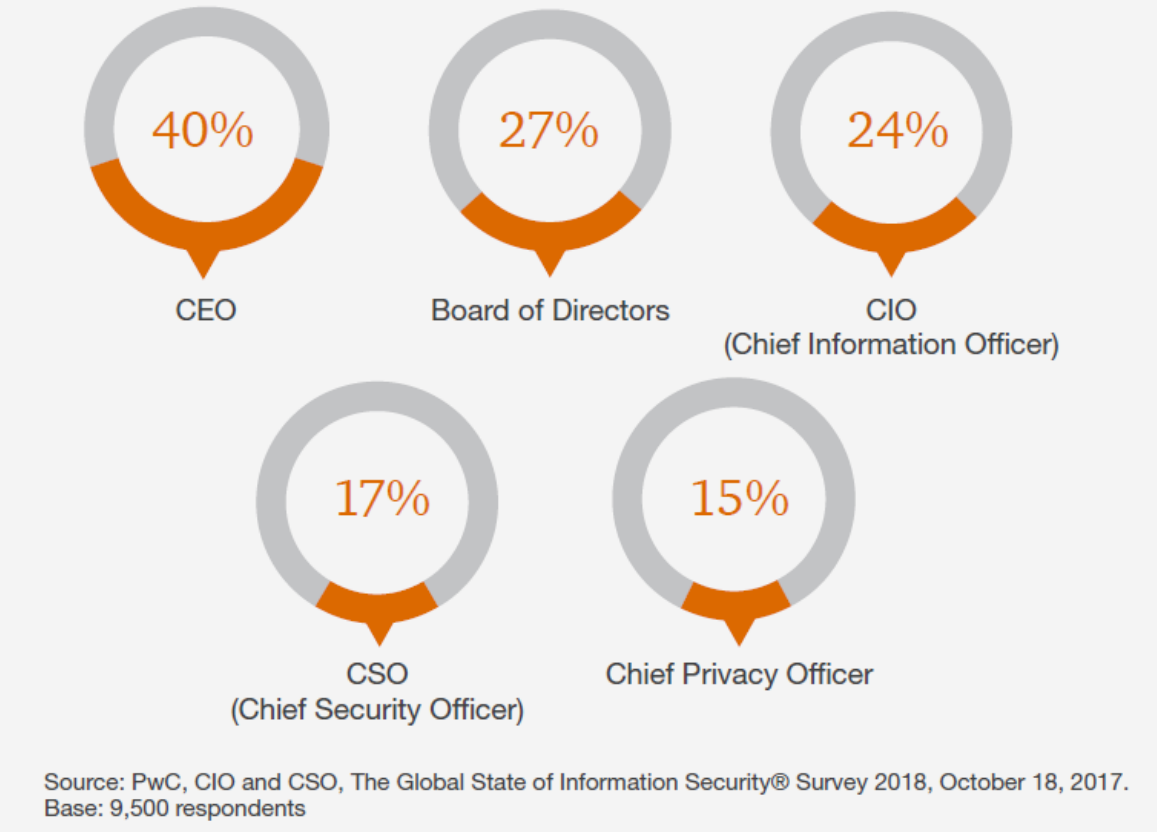
Poco menos de la mitad de todos los encuestados de (PWC, 2018) están de acuerdo en que el riesgo por sí solo impulsa el gasto en seguridad. Alrededor del 30% no está de acuerdo, y el resto está en la mira.

La mayoría de los encuestados (PWC, 2018) (66%) dicen que el gasto de seguridad de sus organizaciones está alineado con los ingresos de cada línea de negocios, pero un resto considerable (34%) dice que no es el caso o no están seguros. El director de Seguridad Digital (CISO) es cada vez más importante.

En las compañías que entienden de alguna manera la problemática de la seguridad digital, cuentan con un ejecutivo responsable de la Seguridad Digital, este ejecutivo es el CISO (Chief Information Security Officer) o el CSO (Chief

Security Officer), en la encuesta (PWC, 2018), se consultó a quien reporta este ejecutivo, los resultados en la Figura N°4.

Figura N° 4: ¿A quién reporta directamente el CISO o CSO o el ejecutivo equivalente?



Fuente: (PWC, 2018)

Según el (PWC, 2018), es más común que el CISO o el director de seguridad digital de una compañía informe directamente al CEO o al consejo de administración que al director de información. "El CISO debe ayudar a la junta a entender dónde se encuentra la compañía para proporcionar seguridad cibernética a las redes de la compañía", dijo Keith Alexander, fundador y CEO de IronNet Cybersecurity, quien anteriormente dirigió el cibercomando de Estados Unidos y la Agencia de Seguridad Nacional como general de cuatro estrellas. . "La información provista debe incluir cualquier ataque cibernético que haya ocurrido, así como fallas en el entrenamiento, el equipo y las herramientas en el dominio cibernético. El CISO debe resaltar las deficiencias para que la junta pueda ejecutar sus responsabilidades para comprender y abordar los riesgos que

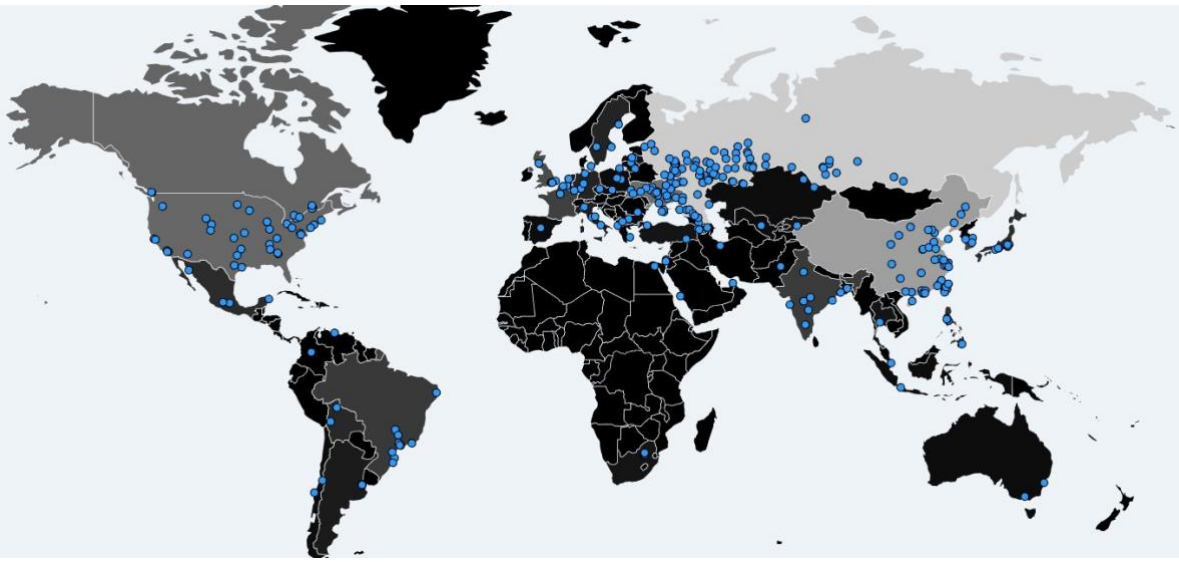
enfrenta la compañía". (NACD Director's Handbook on Cyber-Risk Oversight, 2018)

Estado de las amenazas de Seguridad Digital

Las amenazas a nivel mundial han ido en claro aumento, uno de los desarrollos más importantes en el panorama de ataque en 2017 fue la evolución del ransomware (malware que encripta computadores y solicita un rescate). Los ataques de gusanos ransomware basados en red eliminan la necesidad del elemento humano para infectar computadores. Para algunos atacantes, el premio no es un rescate, sino la destrucción de sistemas y datos. (CISCO, 2018).

Wannacry (Ransomware) uno de los ataques más impresionante de las últimas décadas, aproximadamente 30-40 empresas de nombre público entre los miles que probablemente fueron impactado por este ransomware. Los ejemplos incluyen el Ministerio del Interior ruso, Telefónica (España compañía de telecomunicaciones más grande) y FedEx. El Servicio Nacional de Salud del Reino Unido (NHS), con 16 de los 47 fideicomisos del NHS afectados, y la cirugía de rutina y citas con el médico siendo cancelado a medida que el servicio se recuperaba. Hay informes de que en China más de 40,000 organizaciones fueron afectadas, incluyendo más de 60 instituciones académicas. (Ernst & Young, 2017)

Figura N° 5: Mapa de Infecciones de Wannacry mayo 2017



Fuente: Malware Tech Blog

https://twitter.com/MalwareTechBlog/status/863054943632187392

Existen una serie de amenazas que a diario las empresas y personas están enfrentados, se exponen números globales del tipo de amenazas que afectan al mundo digital en el Anexo 1 y Anexo 2.

7.1.3 Transformación Digital en Chile

"El crecimiento económico alto, sostenido e inclusivo, depende que seamos capaces de enfrentar la transformación digital en conjunto con nuestras empresas, con un Estado como socio". Así lo afirmó el ministro de Economía, Jorge Rodríguez Grossi, en la apertura del seminario "El desafío de la Transformación Digital en Chile", organizado por el Ministerio de Economía, Fomento y Turismo, el Banco Interamericano de Desarrollo (BID) y la Sociedad de Fomento Fabril (Sofofa). (Ministerio Economía Chile, 2018)

Bernardo Larraín, presidente de SOFOFA, destacó que "La transformación digital es una oportunidad tanto para el sector público como privado y en ambos mundos, debemos reconocer que tenemos brechas, no cabe la autocomplacencia en esta materia y debemos desafiarnos a profundizar y acelerar el camino de la digitalización", agregando que "en el sector público, se pueden elaborar mejores políticas públicas a través de Big Data, para identificar cuáles son los segmentos de la población que pueden ser objeto de una política pública y evaluarla posteriormente". Y agregó que "en el mundo privado, por supuesto que tenemos el desafío de estar conectados con lo que está pasando en el perímetro de nuestras respectivas industrias, para poder abrazar cambios tecnológicos que, si los abrazamos serán una oportunidad, pero que si los dejamos pasar por el lado, pueden representar una amenaza para el negocio principal de una empresa". (Revista Trend TIC, 2018).

"Lo primero que las personas se preguntan es si esta transformación digital es real. La verdad es que, para un país como Chile, con industrias como la minería, el vino y la agroindustria, este fenómeno es bastante real. Hoy el 75% de las empresas chilenas están en vías de una transformación digital", aseguró Joseph Pucciarelli, Vicepresidente del Grupo & Asesor ejecutivo de TI en IDC Mundial, quien agregó que "el proceso no ha sido fácil, pues los principales obstáculos han sido la falta de visión y la falta de competencias para saber cómo aplicar la tecnología". (Trend TIC, 2018)

Predicciones de Transformación Digital en Chile

Según un estudio realizado por (IDC Chile, 2017), las predicciones para el mercado chileno son las siguientes:

1. El gasto promedio en cloud para 2017 crecerá 17%

Durante este año continuará el crecimiento en la adopción de tecnología en la nube, aumentando 17% con respecto a 2016, mientras que sus principales ***inhibidores seguirán siendo la seguridad y la privacidad de los datos***. (IDC Chile, 2017)

2. Se proyecta un crecimiento de 25% del mercado de IoT

Chile crecerá en Internet de las Cosas un 25%, quedando 10 puntos arriba de Latinoamérica, que lo haría en promedio 15%. Las industrias con mayor proyección en implementación de soluciones de IoT serán Retail, Manufactura y Transporte, todos con crecimiento sobre el 20%. (IDC Chile, 2017)

3.- El amanecer digital de las organizaciones tendrá un impacto en los hogares

Junto a la transformación digital de las organizaciones se producirá un impacto en los hogares. Los consumidores continuarán expandiendo y modificando la mezcla de dispositivos y aparatos que utilizan cotidianamente y de esta forma incluirse en la nueva economía digital. (IDC Chile, 2017)

4.- Inversión en Big Data & Analytics aumentará en 18% hasta los US$ 500 millones

Big Data & Analytics es una de las tendencias más importantes en industrias como el retail y la banca. (IDC Chile, 2017)

5.- Se espera que el 65% de los chilenos compre este año (2017) por e-commerce

La constante búsqueda por proveer una mejor experiencia de compra a los clientes, llevará a las empresas a desarrollar espacios y modelos de negocios digitales que impulsarán este canal. Hoy cerca del 52% de los chilenos ha adquirido algún producto o servicio a través de e-commerce, y se proyecta que este año subiría a 65%, con un consumo concentrado en ropa, dispositivos electrónicos y compra de pasajes y paquetes turísticos. (IDC Chile, 2017)

Se puede apreciar que en Chile, al igual que en el resto del mundo está en proceso de Transformación Digital, el gobierno y el mercado entienden que la digitalización es un proceso de negocio que trae consigo beneficios y también desafíos, de hecho en el estudio de (IDC Chile, 2017), mencionan que la Seguridad Digital y las privacidad de los datos es un inhibidor, es decir el proceso de Transformación Digital se podría ver limitado, detenido por la Seguridad Digital, se puede concluir que no puede haber proceso de Transformación Digital sin pensar en Seguridad Digital.

7.1.4 Seguridad Digital en Chile

En el gobierno de la presidenta Michelle Bachelet, como una manera de proveer una estrategia de Seguridad Digital que proteja a los usuarios públicos y privados contra posibles acciones de violación de fuentes de datos, junto con la protección de la privacidad de los ciudadanos, el 27 de abril de 2015 crea el Comité Interministerial sobre CiberSeguridad (CISC), a través del decreto supremo N° 533 de 2015. De acuerdo al artículo primero de dicho decreto, la misión de esta comisión asesora del Presidente de la Republica es proponer una política nacional de ciberseguridad y asesorar en la coordinación de acciones, planes y programas de los distintos actores institucionales en esta materia. (Derechos Digitales & Global Partners Digital, 2017)

El 27 de abril de 2017 en una ceremonia encabezada por la Presidente de la República, Michelle Bachelet, el Gobierno de Chile lanzó oficialmente la Política Nacional de Ciberseguridad primer instrumento de política pública del Estado que orientará la acción del país en la materia, con el objetivo de contar con un ciberespacio libre, abierto seguro y resiliente. (Subsecreatria de Defensa de Chile, 2018)

¿Por qué se requiere una política nacional de ciberseguridad?

a) Para resguardar la seguridad de las personas en el ciberespacio

Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad. (Gobierno de Chile, 2017 - 2022)

b) Para proteger la seguridad del país

Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos. (Gobierno de Chile, 2017 - 2022)

c) Para promover la colaboración y coordinación entre instituciones

Es necesario mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacional e internacional, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio. (Gobierno de Chile, 2017 - 2022)

d) Para gestionar los riesgos del ciberespacio

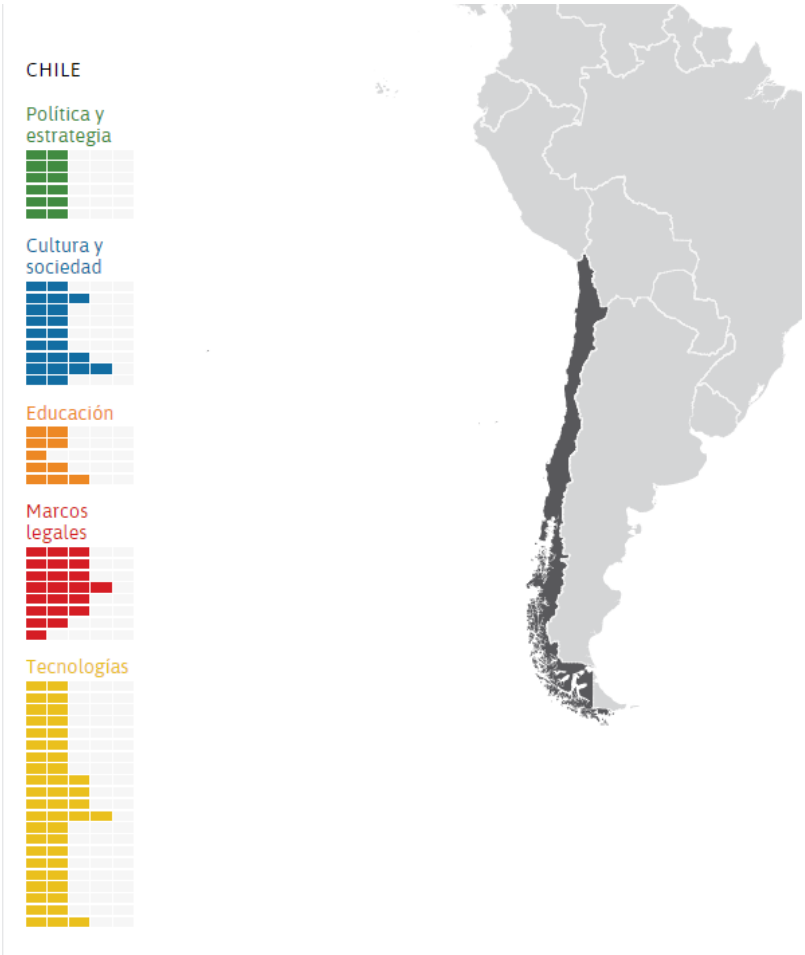
Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente. (Gobierno de Chile, 2017 - 2022)

Con esta política el Gobierno de Chile entrega una Visión de Estado, por lo tanto se puede inferir que la Seguridad Digital es un pilar fundamental en la digitalización de las empresas en Chile, donde el mismo Gobierno lidera un proyecto de Seguridad Digital para el país, para detalles al respecto pueden ser revisados en (Comité Interministerial sobre CiberSeguridad, 2018).

Cómo está preparado Chile en Seguridad Digital

En un estudio realizado por el (Banco Interamericano de Desarrollo & Organization of American States, 2016), evaluó a Chile en una serie de competencias del punto de vista de la Seguridad Digital, un resumen de sus resultados a continuación (Figura N° 6):

Figura N° 6: Grado de madurez de Chile en Seguridad Digital resumen



Fuente: (BID & Organización de los Estados Americanos, 2018)

De la Figura N° 6 se puede concluir que Chile está poco preparado para contrarrestar la amenaza del CiberCrimen, si bien se tiene conectividad se está recién definiendo la estrategia a nivel de gobierno, sin duda que la industria como la financiera está más avanzada en comparación con otras industrias, pero a nivel país queda mucho por hacer.

Figura N° 7: Grado de madurez de Seguridad Digital de Chile

	Chile
Política y estrategia	
Estrategia nacional de seguridad ciberné oficial o documentada	
Desarrollo de la estrategia	2
Organización	2
Contenido	2
Defensa cibernética	
Estrategia	2
Organización	2
Coordinación	2

Fuente: (BID & Organización de los Estados Americanos, 2018)

De la figura N° 7 se pueden apreciar los resultados para el análisis de este estudio, en una escala de 1 a 5, siendo 1 menor nivel de madurez y 5 mayor nivel, el resto de las competencias descritas en la Figura N°6 se pueden revisar en el Anexo 2, a continuación la explicación en detalle de los resultados de la Figura N° 7.

Política y Estrategia

Estrategia de Seguridad Digital oficial o documentada

Desarrollo de la estrategia*:* Se ha articulado un esquema de una estrategia nacional de seguridad cibernética construido sobre la base de la consulta del gobierno; se han establecido procesos de consulta para los grupos de interés clave, posiblemente con asistencia internacional.

Organización: Se ha diseñado y difundido un programa de seguridad cibernética coordinado; los presupuestos todavía pueden estar distribuidos; aún es limitada la

Cooperación interdepartamental. Es necesario comentar que al momento de la realización de este estudio no existía aún la Política Nacional de CiberSeguridad (Subsecreatria de Defensa de Chile, 2018), por lo que el resultado en este punto hubiera sido 3

Contenido: El contenido incluye vínculos entre las prioridades nacionales de riesgo y la seguridad cibernética, pero en general son ad hoc y no están detallados.

Defensa Cibernética

Estrategia: Han sido identificadas amenazas específicas a la seguridad nacional en el ciberespacio, tales como actores de amenazas externas, amenazas internas, Vulnerabilidades del sistema de suministro y amenazas a la capacidad operativa Militar, pero aún no existe una estrategia de respuesta coherente.

Organización: Las unidades de operación de defensa cibernética se incorporan a las diferentes ramas de las fuerzas armadas, pero no existe una estructura central de mando y control.

Coordinación: Se acuerdan los requisitos de capacidad de defensa cibernética entre el sector público y privado con el fin de minimizar la amenaza a la seguridad nacional.

Según el (Banco Interamericano de Desarrollo & Organization of American States, 2016) El Ministerio del Interior y Seguridad Pública, la Secretaría General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen la política de seguridad cibernética a nivel gubernamental. El país ha emitido una estrategia nacional de seguridad cibernética (Comité Interministerial sobre CiberSeguridad, 2018), la sensibilización entre las instituciones gubernamentales es generalizada. La infraestructura gubernamental presenta tecnología de seguridad actualizada y las partes interesadas pertinentes regularmente analizan los activos y vulnerabilidades de la Infraestructura Crítica Nacional. El Estado también coordina la planeación de gestión de crisis y ha puesto en marcha medidas de redundancia.

Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control. Uno de los principales desafíos de Chile de cara al futuro es el fortalecimiento de su capacidad de respuesta a incidentes: el CSIRT-CL que se encuentra en funcionamiento desde 2004 ofrece respuesta a incidentes para los sitios web del gobierno pero no está institucionalizado formalmente a nivel nacional para abordar todo tipo de violaciones.

Chile ha establecido un marco jurídico global para hacer frente a los delitos cibernéticos. El Decreto Supremo nº 1299 describe las normas y define los roles para el manejo de la delincuencia cibernética, la Ley nº 19.223 introduce los delitos informáticos al Código Penal y la Ley nº 19.628 cubre la privacidad y protección de datos. Aunque el sector privado no está obligado por ley a divulgar las violaciones, el gobierno trabaja en estrecha colaboración con las empresas para informar y responder a incidentes cibernéticos. De acuerdo con las autoridades de Chile, la suplantación de identidad (phishing), malware y piratería informática son los tipos más frecuentes de ataques cibernéticos en el país. El Departamento de Investigación de Organizaciones Criminales (OS-9) y el Laboratorio de Criminalística de los Carabineros (LABOCAR), la policía nacional de Chile, llevan a cabo investigaciones y análisis forense digital respectivamente. Estas unidades han detenido con éxito numerosos criminales cibernéticos en los últimos años. Por último, los tribunales tienen una capacidad adecuada para manejar evidencia electrónica.
La mentalidad de seguridad cibernética es inconsistente en la sociedad chilena. En 2013, para crear conciencia, el Ministerio de Educación inició la campaña de Internet Segura para educar a los jóvenes sobre la privacidad y el uso seguro de Internet. También está en marcha una campaña, llamada Consumidor Digital, para que los ciudadanos tengan cuidado de los riesgos del comercio electrónico y para que entiendan sus derechos como consumidores. La Universidad de Chile ofrece títulos avanzados en seguridad cibernética y también están disponibles diversos cursos en línea y capacitación para empleados. Comparativamente, el sector privado se ha vuelto cada vez más consciente de los riesgos de seguridad cibernética y ha puesto en marcha planes para abordarlos. (Banco Interamericano de Desarrollo & Organization of American States, 2016)

Se puede apreciar que Chile si bien es cierto no está avanzado en Seguridad Digital si hay lineamientos generales, existen iniciativas en diferentes ámbitos, pero aún queda bastante camino por recorrer y estandarizar, poder establecer un nivel de requerimientos mínimos para afrontar los riesgos de Seguridad Digital, dentro de otras iniciativas, que están por ejemplo en la Política Nacional de Ciberseguridad (Gobierno de Chile, 2017 - 2022)

A nivel mundial la industria que está más avanzada es la industria financiera y Chile no es la excepción al respecto, de hecho en un estudio realizado por Accenture donde se entrevistó a más de 250 ejecutivos de Seguridad de Bancos a nivel mundial, el 78% de ellos confía en su estrategia de Seguridad Digital, a pesar de sufrir entre dos y tres ataques al mes. (Trend TIC, 2018)

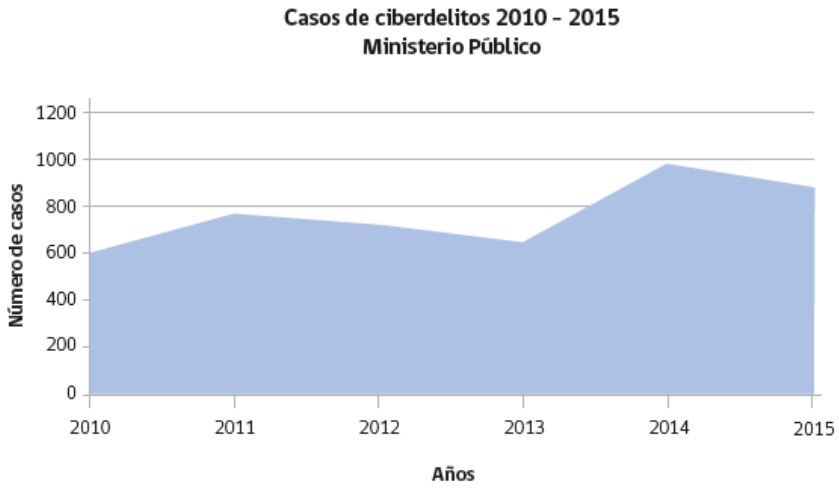
Algo que es importante entender es que la Seguridad Digital no es solo un tema tecnológico, es un esfuerzo conjunto de la compañía en total, empleados y directivos. (Trend TIC, 2018)

Estado de las amenazas de Seguridad Digital en Chile

A nivel regional, países que han registrado el mayor número de ciberataques en Latinoamérica fueron Brasil, Argentina, Colombia, México y Chile. Los accesos o robo de información desde un ordenador infectado -denominados botnets- predominaron en la región. (Gobierno de Chile, 2017 - 2022)

Del punto de vista de los CiberDelitos de acuerdo con el Ministerio Público, en relación con el cibercrimen, entre los años 2010 y 2015, el número de casos ingresados bajo el rótulo “delito informático” fue de 4.648 casos, distribuidos como se indica en la Figura N°8

Figura N° 8: Ciberdelitos 2010-2015 Ministerio Público

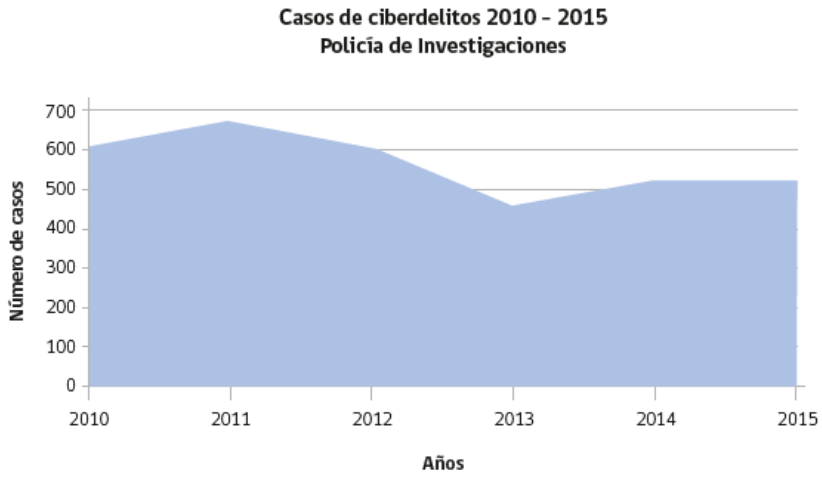


Casos ingresados por ciberdelitos 2010 - 2015 por Ministerio Público, referidos sólo a las figuras reguladas en la Ley N°19.223 (Fuente: ULDDECO, Ministerio Público, 2016[18]).

Fuente: (Gobierno de Chile, 2017 - 2022)

Según los datos aportados por la Policía de Investigaciones (PDI), durante el periodo 2015, se realizaron un total de 3.370 investigaciones, ver Figura N°9.

Figura N° 9: Ciberdelitos 2010-2015 PD



Fuente: (Gobierno de Chile, 2017 - 2022)

Según (Kaspersky Lab, 2018) el 51% del malware detectado en Chile en el primer semestre de 2017 provino de herramientas utilizadas en software piratas. En segundo lugar se ubicaron las URLS maliciosas con 12%, y el acceso remoto a dispositivos con un 10% de las detecciones. En Chile se registran 1.120 ataques diarios de Phishing.

Respecto de WannaCry, el ransomware que en mayo 2017 se propagó rápidamente entre más de 200 mil computadores basados en el sistema operativo Microsoft Windows, afectando a más de 150 países, Kaspersky Lab develó que el virus fue el responsable del 22% de todos los ataques de ransomware que se han perpetrado en Chile en el primer semestre del 2017. (Kaspersky Lab, 2018).

Las cifras muestran que Chile no está para nada ajeno a la problemática de Seguridad Digital, por lo que se hace necesario que las empresas aborden una estrategia al respecto, que vaya de la mano con la estrategia corporativa.

8. Análisis de modelos de Seguridad Digital

8.1 Consideraciones generales de los modelos

8.1.1 Qué tipo de empresas deberían usar un modelo de Seguridad Digital

Un Modelo de Seguridad Digital es para organizaciones de todos los tamaños, sectores y madurez.
Si bien los modelos son diseñados teniendo en cuenta la Infraestructura Crítica, son extremadamente versátiles.
Con los mecanismos de personalización incorporados (es decir, Niveles, Perfiles y Núcleos todos pueden ser modificados), el modelo puede ser personalizado para que lo use cualquier tipo de organización.
Debido a que el modelo está guiado por los resultados y no ordena cómo una organización debe lograr esos resultados, permite la escalabilidad.
Una pequeña organización con un bajo presupuesto de Seguridad Digital, o una gran corporación con un gran presupuesto, puede abordar el resultado de una manera que sea factible para ellos.
Es esta flexibilidad la que permite que un modelo sea utilizado por organizaciones que recién están comenzando a establecer un programa de seguridad digital, que al tiempo que les proporcionara valor a las organizaciones con programas maduros. (NIST GOV, 2018)

8.1.2 Por qué utilizar un modelo de Seguridad Digital

Un modelo proporciona un lenguaje común y una metodología sistemática para gestionar el riesgo de Seguridad Digital. El núcleo del modelo incluye actividades que se incorporarán en un programa de Seguridad Digital que se puede adaptar para satisfacer las necesidades de cualquier organización. Un modelo está diseñado para complementar o crear un programa de Seguridad Digital.
Un proceso de creación de Perfiles de un Modelo brinda a las organizaciones la oportunidad de identificar áreas donde los procesos existentes pueden fortalecerse o donde se pueden implementar nuevos procesos. Estos perfiles, cuando se combinan con el lenguaje fácil de entender del modelo, permiten una comunicación más sólida en toda la organización.
Un plan de implementación permite que una organización aproveche al máximo el modelo al permitir la priorización rentable y la comunicación de las actividades de mejora entre las partes interesadas de la organización, o establecer expectativas con proveedores y socios. Además, los planes de implementación asociados se

pueden aprovechar como elementos relevantes para demostrar la debida atención requerida.
Los niveles de Implementación del Modelo pueden ayudar a las organizaciones proporcionando un contexto sobre cómo una organización considera la gestión de riesgos de Seguridad Digital. (NIST GOV, 2018)

8.1.3 Beneficios de la utilización de un modelo

Existen muchos beneficios en la implementación de un modelo. Al ser neutrales, ampliamente aplicables, un modelo puede reducir el tiempo y los gastos de iniciar un programa de seguridad digital y también reducir el riesgo dentro de los programas actuales mediante la identificación de áreas de mejora.

A continuación se muestra un resumen de los beneficios de la implementación de un modelo (IT Governance, 2018)

Asegura la información en todos sus formatos: Ayuda a proteger todas las formas de información, incluida la propiedad digital, en papel, propiedad intelectual, secretos de la empresa, datos en dispositivos y en la nube, copias impresas e información personal.

Aumenta la resiliencia a los ataques de Seguridad Digital*: Implementar* y mantener un modelo aumentará significativamente la preparación de la organización frente a ataques de seguridad digital.

Proporciona un marco administrado de manera centralizada: Proporciona un marco para mantener segura la información de su organización y administrarla adecuadamente.

Ofrece protección para toda la organización: Protege a toda la organización de los riesgos basados en tecnología y otras amenazas comunes, como personal poco capacitado o procedimientos ineficaces.

Ayuda a responder a las amenazas de seguridad digital en evolución: Constantemente se adapta a los cambios del entorno como dentro de la organización, un modelo reduce la amenaza de riesgos en continua evolución.

Reduce los costos asociados con la seguridad de la información: Gracias al enfoque de evaluación y análisis de riesgos de un modelo, las organizaciones pueden reducir los costos de las capas de tecnología defensiva que no podría funcionar.

Protege la confidencialidad, disponibilidad e integridad de los datos: Un modelo ofrece un conjunto de políticas, procedimientos y controles técnicos y

físicos para proteger la confidencialidad, disponibilidad e integridad de la información.

Mejora la cultura de la empresa: El enfoque holístico de un modelo cubre a toda la organización, no solo a tecnología, abarca a la personas y procesos. Esto permite a los colaboradores comprender rápidamente los riesgos y adoptar controles de seguridad digital como parte de sus prácticas cotidianas.

8.1.4 Cuáles son los modelos más utilizados

Muchas organizaciones deben cumplir con una combinación de regulaciones de seguridad digital, empresas estatales, industriales e internacionales.

Según el estudio de tendencias de adopción de modelos de seguridad digital de (Tenable, 2018), el 84% de las empresas en Estados Unidos utiliza algún tipo de Modelo, mientras que el 44% de las empresas utilizan más de un modelo.

Según el estudio de (Tenable, 2018) los modelos más ampliamente utilizados son:

- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
- Payment Card Industry Data Security Standard (PCI DSS)
- Center for Internet Security Critical Security Controls (CIS)
- ISO/IEC 27001/27002 (ISO)

Para finales del 2016, la adopción del CSF era de un 43%, el CIS con un 44% y la ISO un 44%. (Tenable, 2018)

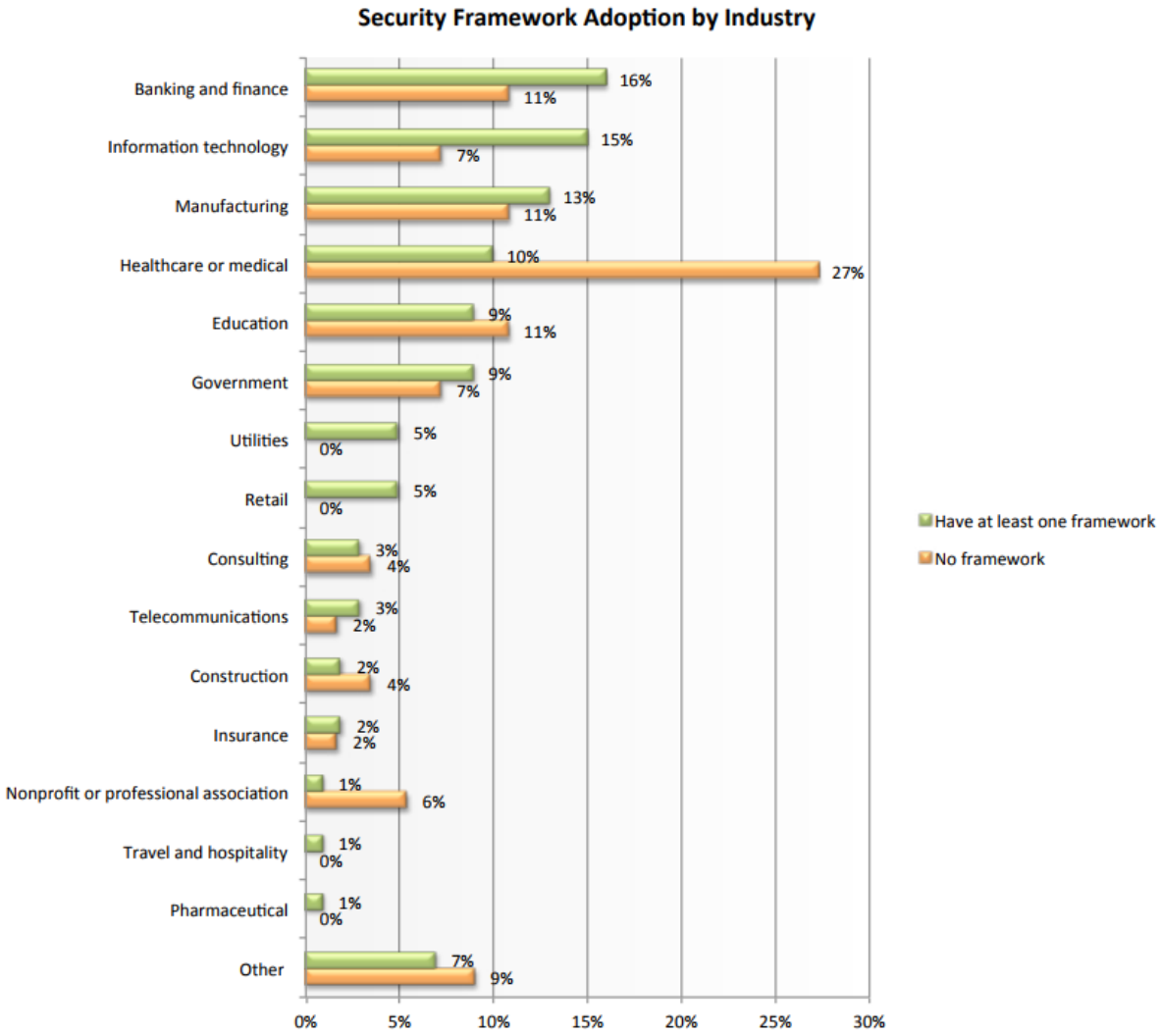
En otro estudio más reciente la adopción de los mismos modelos es el siguiente:

- PCI DSS (47%)
- ISO 27001 (35%)
- CIS (32%)
- NIST CSF (29%)

Fuente: (IT GOVERNANCE, 2018)

Las empresas con más de 10,000 empleados tienen una probabilidad levemente mayor de haber adoptado un marco de seguridad (90%), pero incluso las empresas más pequeñas con menos de 1,000 empleados informan tasas de adopción significativas (77%) (IT GOVERNANCE, 2018)

Figura N° 10: Adopción de modelos por industria



Fuente: (Tenable Network Security, 2016)

De los 4 modelos mencionados anteriormente se procederá a analizar el NIST CSF y la ISO/IEC 27001/27002, debido a que son modelos para cualquier tipo de empresa, el PCI DSS (Payment Card Industry Data Security Council Standard) es específico para empresas que trabajan con tarjetas de crédito (redbanc, transbank, bancos, etc.) y se encarga muy particularmente de los procesos asociados a la tarjeta de crédito, el CIS (Critical Security Controls) es un modelo específico muy técnico para controles tecnológicos de seguridad digital, materia donde el NIST CSF cumple el mismo objetivo y con mayor amplitud.

8.2 NIST Framework for improving Critical Infrastructure Cybersecurity

Fuente: (NIST GOV, 2018)

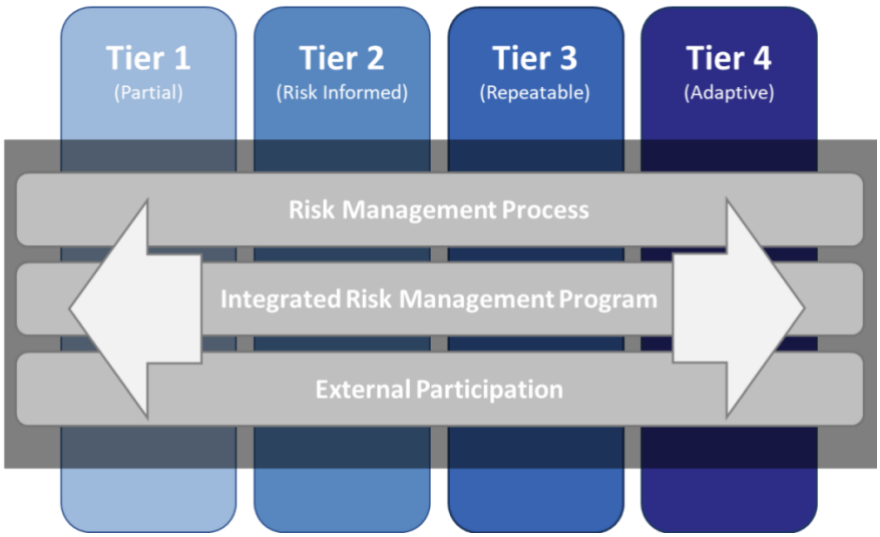
Este modelo consiste en estándares, directrices y mejores prácticas para gestionar el riesgo relacionado con la Seguridad Digital. Un enfoque prioritario, flexible y rentable del Modelo de Seguridad Digital ayuda a promover la protección y la resiliencia de infraestructura crítica y otros sectores importantes para la economía y la seguridad nacional. (NIST, 2018)

8.2.1 Componentes del Modelo

Niveles de implementación

Los niveles describen el grado de administración de la gestión de riesgo de seguridad digital de una organización. Los niveles varían desde Parcial (Nivel 1) hasta Adaptativo (Nivel 4) y describen un grado creciente de rigurosidad y significan qué tan bien se toman las decisiones de riesgo y también considera el grado en que la organización comparte y recibe información de seguridad. Los niveles no representan necesariamente niveles de madurez. Las organizaciones deben determinar el nivel deseado, asegurando que el nivel seleccionado cumpla con los objetivos de la organización, reduciendo el riesgo de seguridad digital a niveles aceptables, siendo factible de implementar.

Figura N° 11: Niveles de implementación de gestión de riesgo de Seguridad Digital



Fuente: (NIST GOV, 2018)

En la Figura N° 11 se aprecia, cada uno de los niveles Tier 1 a 5 representan un objetivo de la organización a alcanzar, para más detalles de los cuatro niveles revisar el (NIST GOV, 2018).

El núcleo del Modelo

El núcleo es un conjunto de actividades y resultados de seguridad digital deseados organizados en categorías y alineados con referencias informativas. El Núcleo del modelo está diseñado para ser intuitivo y actuar como una capa de traducción para permitir la comunicación entre equipos multidisciplinarios mediante el uso de un lenguaje simplista y no técnico. El núcleo consta de tres partes: funciones, categorías y subcategorías. El Núcleo incluye cinco funciones de alto nivel: Identificar, Proteger, Detectar, Responder y Recuperar. Estas 5 funciones no sólo son aplicables a la gestión de riesgos de seguridad digital, sino también a la gestión de riesgos en general. En la figura N° 12 las 23 categorías que se dividen en cinco funciones, se pueden apreciar las categorías del Núcleo del Modelo por cada función.

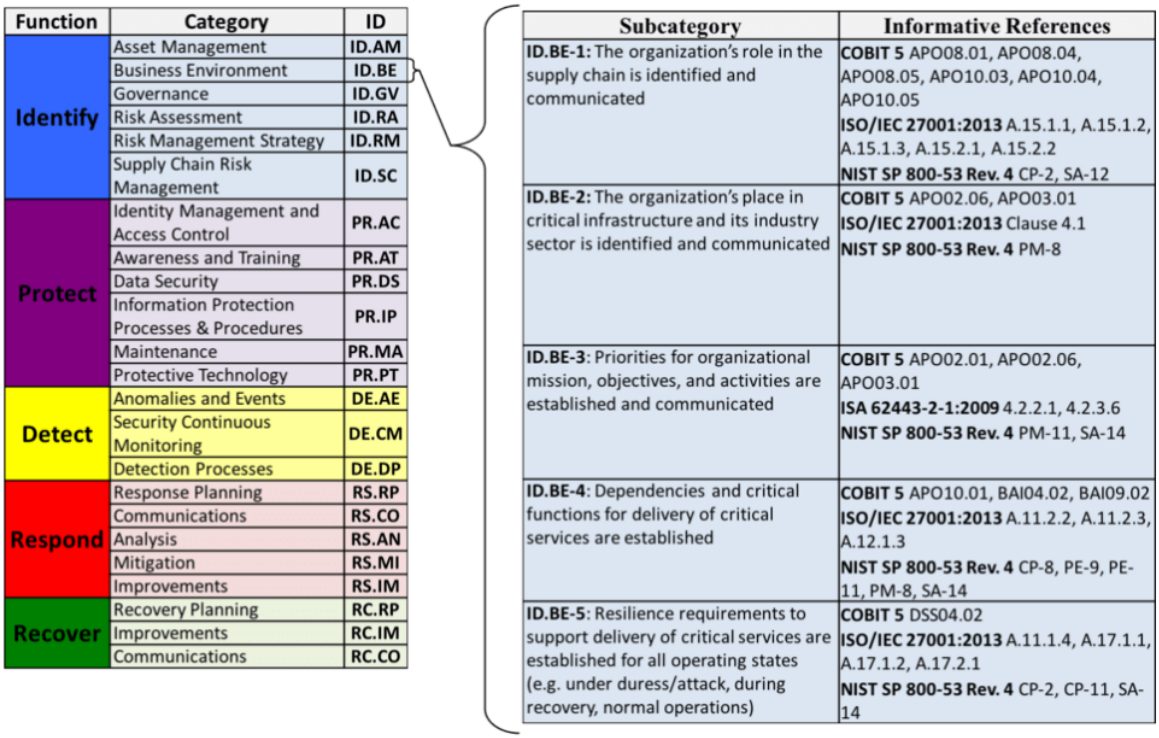
Figura N° 12: Funciones y categorías del núcleo del NIST

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Fuente: (NIST GOV, 2018)

Las categorías fueron diseñadas para cubrir la amplitud de los objetivos de seguridad digital para una organización, sin ser demasiado detalladas. Cubre temas de cibernética, física y personal, con un enfoque en los resultados de negocio. Las subcategorías son el nivel más profundo de abstracción en el Núcleo. Hay 108 subcategorías, que son declaraciones basadas en los resultados que proporcionan consideraciones para crear o mejorar un programa de seguridad digital. Debido a que el modelo se basa en los resultados y no impone cómo una organización debe lograr esos resultados, permite implementaciones basadas en riesgos que se personalizan según las necesidades de la organización.

Figura N° 13: Categorías del núcleo del NIST y ejemplo de Subcategoría.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Fuente: (NIST GOV, 2018)

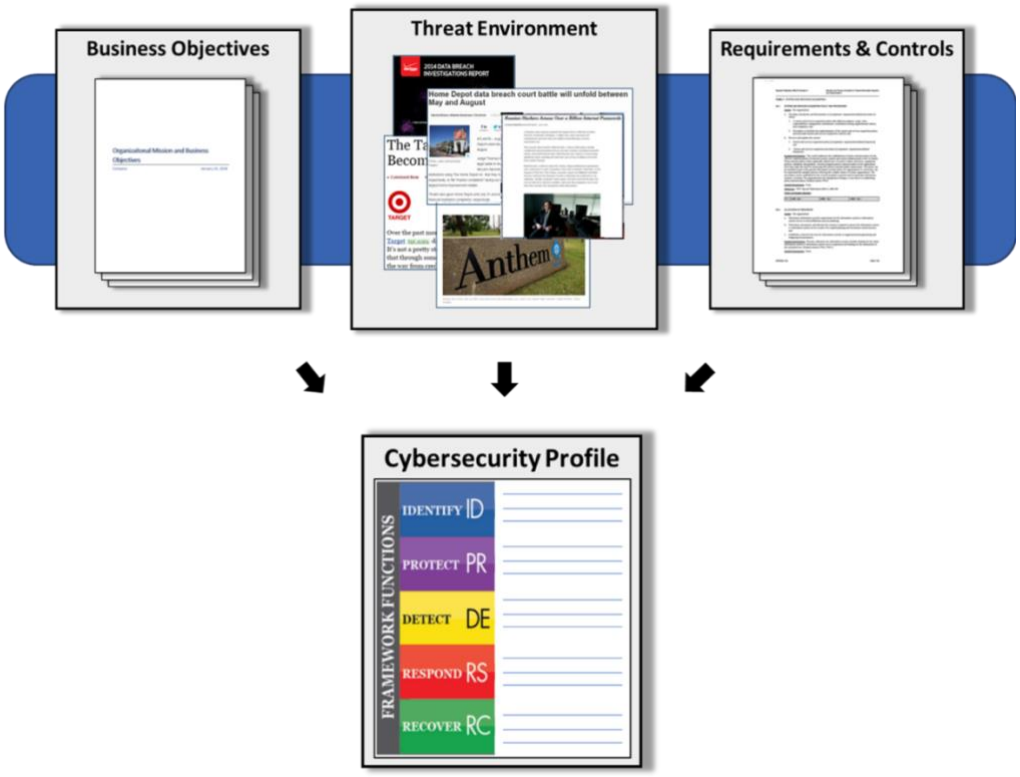
Las cinco subcategorías representadas en la categoría de entorno empresarial (ID.BE) proporcionan un ejemplo de las declaraciones centradas en los resultados que se encuentran en todo el núcleo. La columna a la derecha, Referencias informativas apoyan al Núcleo proporcionando amplias referencias que son más técnicas que el modelo mismo. Las organizaciones pueden desear utilizar algunas, ninguna o todas estas referencias para informar las actividades que deben emprender para lograr el resultado descrito en la Subcategoría, para más detalles

De todas las categorías y subcategorías revisar el Anexo 3.

Perfiles del Modelo

Los perfiles son la alineación de los requisitos de una organización y sus objetivos, el apetito por el riesgo y recursos en comparación con los resultados deseados del modelo. Los perfiles se pueden usar para identificar oportunidades para mejorar el nivel de seguridad digital comparando un perfil "actual" con un perfil "objetivo" o futuro.

Figura N° 14: Objetivos de Negocio, escenario de amenaza, requerimientos y controles, da como resultado un perfil objetivo.



Fuente: (NIST GOV, 2018)

Los perfiles tratan de optimizar el modelo de seguridad digital para acomodarse de mejor manera a la organización. Una forma de acercarse a los perfiles es que una organización trace un mapa de sus requisitos de seguridad digital, objetivos, misión y metodologías operacionales, junto con las prácticas actuales contra las

subcategorías del modelo de trabajo del modelo para crear un Perfil de estado actual. Estos requisitos y objetivos se pueden comparar con el estado operativo actual de la organización para comprender las brechas entre ambos, en la Figura N° 15 se aprecia un ejemplo de lo mencionado.

Figura N° 15: Ejemplo de un perfil objetivo

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

Fuente: (NIST GOV, 2018)

La creación de estos perfiles y el análisis de brechas permiten a las organizaciones crear un plan de implementación priorizado. La prioridad, el tamaño de la brecha y el costo estimado de las acciones correctivas ayudan a las organizaciones a planificar y presupuestar las actividades de mejora de la seguridad digital.

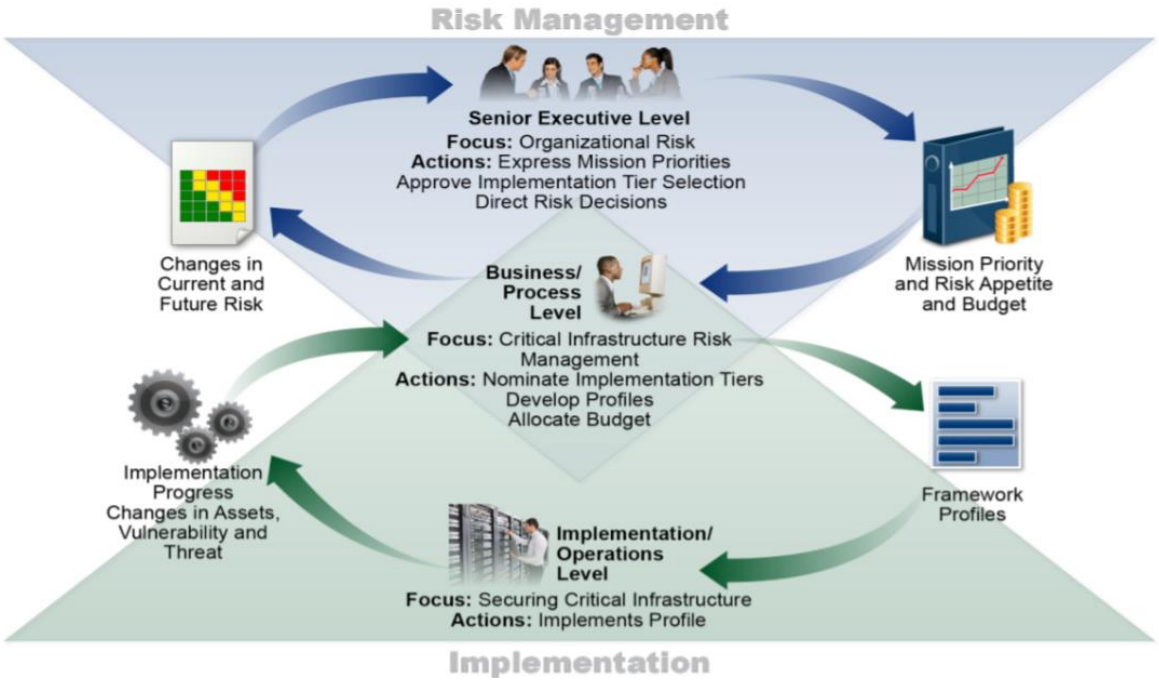
8.2.2 Gestión de riesgo con el modelo NIST

El modelo ayuda a guiar los puntos claves de decisión sobre las actividades de gestión de riesgos a través de los distintos niveles de una organización, desde los ejecutivos superiores hasta el nivel de negocio y proceso, y también la implementación y las operaciones.
Como se muestra en la Figura N° 16, el diagrama y la explicación demuestran cómo el Marco permite las comunicaciones de administración de riesgos de extremo a extremo en toda la organización.

El nivel ejecutivo comunica las prioridades de la misión, los recursos disponibles y la tolerancia al riesgo al nivel de negocio / proceso. El nivel de negocio / proceso utiliza la información como entradas en el proceso de gestión de riesgos, y luego formula un perfil para coordinar las actividades de implementación / operación. El nivel de implementación / operación comunica el progreso de la implementación del perfil al nivel de negocio / proceso. El nivel de negocio / proceso usa esta información para realizar una evaluación de impacto. La administración de nivel de

negocios / procesos informa los resultados de esa evaluación de impacto al nivel ejecutivo para informar el proceso general de gestión de riesgos de la organización y el nivel de implementación / operaciones para el conocimiento del impacto en el negocio.

Figura N° 16: Proceso de Gestión de Riesgos con NIST



Fuente: (NIST GOV, 2018)

8.2.3 Las cinco funciones

El núcleo del modelo contiene cinco funciones, que representan la estrategia a seguir con el modelo, las funciones se pueden apreciar en la Figura N° 17.

Figura N° 17: Cinco funciones del núcleo del NIST

Fuente: (NIST GOV, 2018)

Identificar

La Función de Identificación ayuda a desarrollar una comprensión organizacional para administrar el riesgo de seguridad digital, para sistemas, personas, activos, datos y capacidades. Es necesario comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de seguridad digital relacionados, permiten a una organización enfocarse y priorizar sus esfuerzos, de manera de ser consistente con su estrategia de gestión de riesgos y sus necesidades de negocio.

Proteger

La función de protección describe las salvaguardas apropiadas para garantizar la entrega de servicios de infraestructura crítica. La función de protección admite la capacidad de limitar o contener el impacto de un posible evento de Seguridad Digital.

Detectar

La función de detección define las actividades apropiadas para identificar la ocurrencia de un evento de seguridad digital. La función de detección permite el descubrimiento oportuno de eventos de ciberseguridad.

Responder

La función Responder incluye actividades apropiadas para tomar medidas con respecto a un incidente detectado de ciberseguridad. La función Responder soporta la capacidad de contener el impacto de un posible incidente de seguridad digital.

Recuperar

La función de recuperación identifica las actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o servicios que se vieron afectados debido a un incidente de seguridad digital. La función de recuperación admite la recuperación oportuna a las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

Nota:
La parte de implementación del modelo se cubrirá en la propuesta de solución de este trabajo, en el punto 9.

8.3 ISO 27001

Fuente:(BSI GROUP, 2018)

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz para minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio.

8.3.1 Cómo funciona la ISO 27001

Fuente: (Advisera, 2018)

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará

relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

8.3.2 Donde interviene la gestión de seguridad de la información en una empresa

Fuente: (Advisera, 2018)

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información, tal como se aprecia en la Figura N° 18.

Figura N° 18: La gestión de riesgo es el centro del proceso

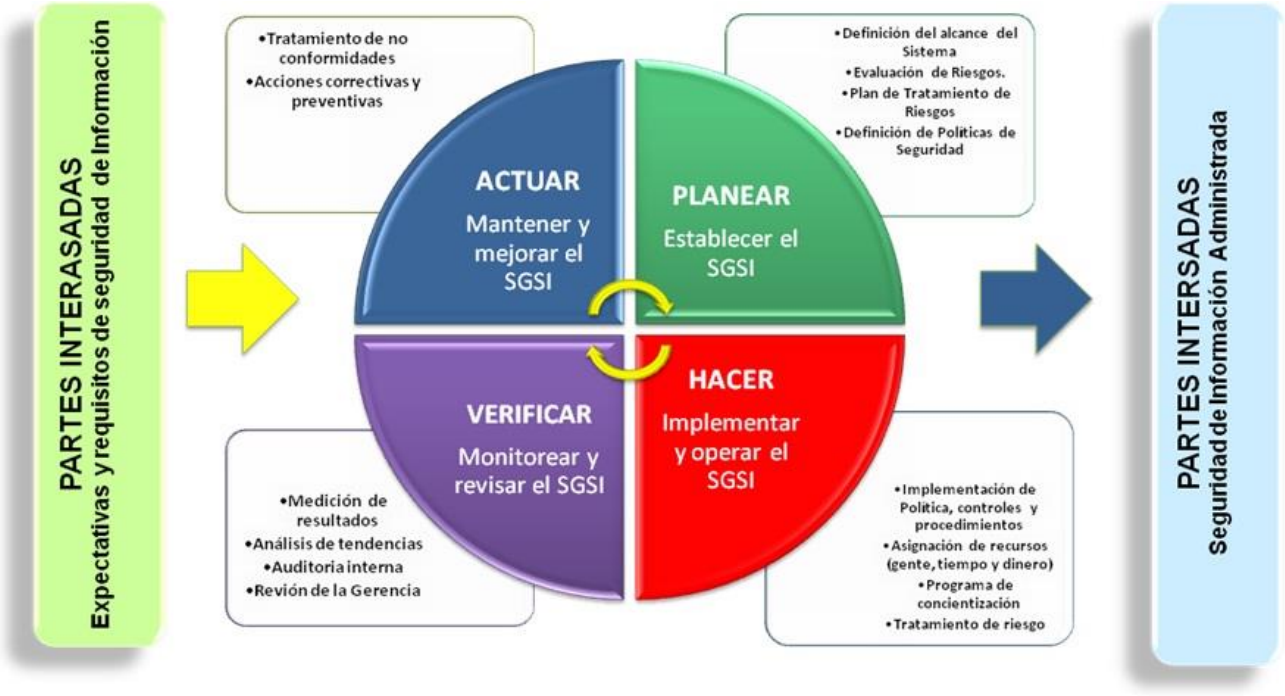
Fuente: (Advisera, 2018)

8.3.3 Estructura de la ISO 27001:2013

Fuente: (ISO ORG, 2018)

La estructura de la ISO 27001 está basada en un ciclo de mejorar continua PDCA (Planear, hacer, verificar y actuar), de acuerdo a la Figura N° 19.

Figura N° 19: Ciclo PDCA ISO 27001:2013



Fuente: (TODDLE, 2018)

Estructura de la ISO 27001:2013

Planear

- ✓ Contexto de la organización: Se identifican los problemas internos y externos que rodean a la organización:
  - Se intuyen todos los requisitos para definir el contexto del SGSI sin importar el tipo de empresa que sea y el alcance que tenga.
  - Se introduce una nueva figura como un elemento primordial para definir el alcance del SGSI
  - Se establece la prioridad de identificar y definir todas las necesidades de las partes interesadas con relación a la seguridad de la información y las expectativas creadas por el Sistema de Gestión

de Seguridad de la Información, ya que esto determinará las políticas de Seguridad de la Información y todos los objetivos a seguir para el proceso de gestión de riesgos.

- ✓ Liderazgo: Se realiza un ajuste de la relación y las responsabilidades de la gerencia de la organización con respecto al **Sistema de Gestión de Seguridad de la Información**, destacando como se deberá demostrar el compromiso, como por ejemplo:
  - Garantizar que los objetivos del **SGSI** y la política de seguridad de la información, antes se conocía como la política del SGSI
  - Se debe garantizar la disponibilidad de todos los recursos para la implantación del SGSI.
  - Se garantiza que los roles y las responsabilidades para la seguridad de la información se asignan y se comunican de forma adecuada.

- ✓ Planeación: En este apartado de la norma ISO 27001:2013 se enfoca a la definición de los objetivos de seguridad como un todo, los cuales deben estar claros y se debe contar con planes específicos, se pueden presentar grandes cambios con la evaluación de riesgos.
  - La metodología se enfoca con el objetivo de identificar todos los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información.
  - El nivel de riesgos se determina con base a toda probabilidad de que ocurra un riego y las consecuencias generadas, si el riesgo se materializa.

- ✓ Soporte: Los requisitos del soporte para el establecimiento de la implementación y mejora del SGSI.
  - Recursos
  - Personal competente
  - Conciencia y comunicación de todas las partes interesadas

Hacer

- ✓ Operación: Establece todos los requisitos del Sistema de Seguridad de la Información, todas las expectativas de la gerencia y de la organización y la retroalimentación sobre estas.
  Además la organización plantea y controla las operaciones y los requisitos de seguridad, el pilar de este proceso se centra en realizar las evaluaciones de riesgos de seguridad de la información de forma periódica por medio de un programa elegido, que dará origen a la implementación de los controles de la **ISO 27002: 2013,** tomando en consideración los riesgos más altos como prioridad.

Verificar

- ✓ Evaluación de desempeño: La base para realizar la identificación y la medición de la eficiencia y el desempeño que realiza el SGSI, es decir las auditorías internas y revisiones al sistema de gestión.
  Se tiene que considerar el estado en que se encuentran los planes de acción para poder atender las no conformidades como es debido, además se establecer la necesidad de definir quién y cuándo realiza las evaluaciones, además de quien tiene que analizar la información que se ha recolectado.

Actuar

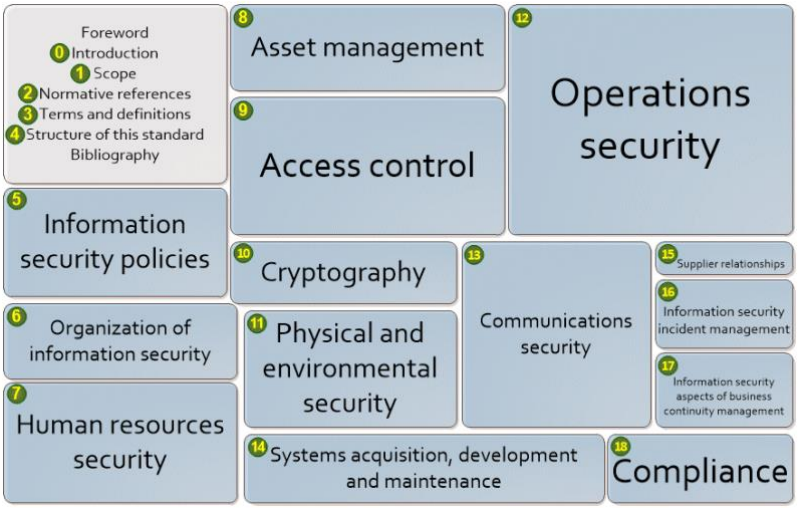
- ✓ Mejora: El principal elemento del proceso son las no conformidades, las cuales tienen que contabilizarse y compararse con las acciones para asegurar de que no se repitan y que las acciones correctivas que se realicen sean efectivas.

8.3.4 Objetivos de control ISO 27002:2013

Fuente: (ISO 27001 Security, 2018)

Cuando el proceso de gestión de riesgos está realizado en la etapa de operación y se tiene claridad de la condición de riesgo de la organización, se procede a implementar los controles de la ISO 27002:2013, de acuerdo a la condición de riesgo y requerimientos del negocio, el mapa de objetivos de control se puede apreciar en la Figura N° 20 color celeste.

Figura N° 20: Mapa objetivos de control ISO 27002:2013



Fuente: (ISO 27001 Security, 2018)

Política de seguridad de la información

- ✓ Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una **adecuada política de seguridad**, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

Organización de la Seguridad de la Información

- ✓ Los controles indicados en este capítulo buscan estructurar un marco de seguridad eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles.

Seguridad relativa a los recursos humanos

- ✓ Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar **el nivel de seguridad adecuándolo a las características** de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

Gestión de activos

- ✓ Se centra en la atención en la **información como activo** y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la **seguridad y en la alteración no deseada**.

Control de acceso

- ✓ Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo no todas las **personas de una organización** necesitan acceder para realizar su actividad diaria a todos los datos, sino que se tienen roles que **necesitan un mayor acceso** y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, **gestión de los privilegios de acceso**, etc. siendo algunos de los controles que se incluyen en este apartado.

Criptografía

- ✓ En el caso de estar tratando la información sensible o crítica puede ser interesante utilizar diferentes técnicas criptográficas para proteger y garantizar su autenticidad, confidencialidad e integridad.

Seguridad Física y del entorno

- ✓ La seguridad no es solo a nivel tecnológico sino también físico, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles, por parte del personal externo los documentos con los que se están trabajando no sólo nos permitirán gestionar de forma adecuada la seguridad sino que se **acabarán convirtiendo en hábitos que nos aportan eficiencia** en la gestión.

Seguridad de las operaciones

- ✓ Tiene un marcado componente técnico concentrado en todos los **aspectos disponibles como la protección** del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

Seguridad de las comunicaciones

- ✓ Partiendo de la base de que la gran mayoría de los intercambios de información y de datos en distintas escalas **se llevan a cabo mediante las redes sociales y/o similares**, garantizar la seguridad y proteger de forma adecuada los medios de transmisión de estos datos clave.

Adquisiciones, desarrollo y mantenimiento de los sistemas de información

- ✓ La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, es general, **abarca toda la organización** y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del desarrollo de aplicaciones de software desde un inicio.

Relaciones con proveedores

- ✓ Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben **establecer medidas de seguridad** pudiendo ser muy recomendable e incluso necesario en determinados casos.

Gestión de Incidentes de Seguridad Digital

- ✓ No se puede hablar de **controles de seguridad** sin mencionar un elemento clave, los incidentes en seguridad. Y es que, estar preparados para cuando

estos incidentes ocurran, dando **una respuesta rápida y eficiente** siendo la calve para prevenirlos en el futuro.

Aspectos de seguridad de la información para la gestión de la continuidad de negocio

- ✓ No se sabe que se necesita un dato hasta que se ha perdido. Sufrir una pérdida de **información relevante y no poder recuperarla** de alguna forma puede poner en peligro la continuidad de negocio de la organización.

Cumplimiento

- ✓ Legislación, normas y políticas aplicables que **se encuentre relacionadas con este campo** y con las que conviven en las organizaciones. Se debe tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben **garantizar que se cumple** y que están actualizados con los últimos cambios siendo esencial para no tener sorpresas desagradables.

Nota: Para mayores detalles de los controles de cada objetivo de control de la ISO 27002:2013 referirse al Anexo 4.

8.4 Comparativa entre ISO 27001 y NIST CSF

En los puntos 8.2 y 8.3 se aprecia una descripción de lo más relevante de la ISO 27001 y el NIST CSF, ambos modelos tienen varias cosas en común, ambos aportan una metodología sobre cómo implementar la seguridad digital en una empresa, se podría utilizar cualquiera de ellos, ambos son tecnológicamente neutros, ambos son aplicables a cualquier tipo de organización, ambos tienen el propósito de generar beneficios comerciales mientras se observan requisitos regulatorios y legales, considerando también los de las partes interesadas.
La mayor similitud que tienen es que ambos modelos están basados en la gestión de riesgos, lo que significa la implementación de controles depende de este importante proceso.
Sin embargo tienen algunas diferencias que se pueden apreciar mejor en la tabla N° 1.

De la tabla N° 1 se puede concluir que a pesar de sus similitudes sus diferencias están en dos ámbitos principales, el ámbito de la estrategia, donde la ISO 27001 del punto de vista de su visión más amplia, más holística, es más clara para poder identificar y entender lo que se debe hacer en términos del gobierno del proceso de seguridad digital, también es más simple poder identificar claramente la documentación necesaria y los registros necesarios, dentro de las exigencias que tiene la ISO 27001 cuenta con una serie de directrices claras en la implementación de la estrategia dentro en una compañía, el NIST CSF a pesar que conecta la

estrategia con la ejecución y operación no queda tan claro como conformar y ejecutar la estrategia.
El segundo ámbito donde son diferentes es en la implementación de controles, a pesar que la ISO 27001 entrega los lineamientos de la implementación de los controles a través de la ISO 27002 (punto 8.3.2), el NIST CSF es mucho más claro al respecto, donde es posible entender a la perfección el objetivo que se busca (punto 8.2.3) con la implementación de cada control, además de mapearlo con los controles de los otros modelos que se utilizan, por lo tanto la implementación, que es la ejecución de las directrices de la estrategia es más simple.

Tabla N° 1: Comparación entre ISO 27001 y NIST CSF

Tabla comparativa entre NIST CSF e ISO 27001/27002	ISO 27001 ISO 27002	NIST CSF
Voluntario de implementar	√	√
Cuenta con una metodologia de Implementación	√	√
Es neutral en cuanto a la tecnología	√	√
Aplicable a cualquier organización y a cualquier area	√	√
Contempla requerimientos regulatorios	√	√
Se basa en la gestión de riesgos	√	√
Mas clara estructura de planificacion e implementación de controles	x	√
Perfiles de implementación	x	√
Facil entendimiento	x	√
Certificable	√	√
Mejor cobertura en protección de activos no digitales	√	x
Mejor claridad en la documentación y resgistros	√	x
Mejor enfoque de gestión de estratégica	√	x
Controles mapeados con otros modelos	x	√
Reconocimiento Internacional	√	√

Fuente: Propia

9. Propuesta de solución de un Modelo de Seguridad Digital para la empresa.

La propuesta final es utilizar los dos modelos descritos anteriormente, ISO 27001 y NIST CSF, con la ISO se tiene una estructura de gobierno de cómo administrar el proceso de manera corporativa dentro de un ciclo de mejora continua y con el NIST CSF se tiene la ventaja de una implementación de controles más específicos y focalizados en seguridad digital, propuesta que se describe en detalle a continuación.

9.1 Conectando con la estrategia de la empresa

Para poder definir una adecuada estrategia, como primer punto se debe tener en cuenta que esta debe estar alineada con los objetivos estratégicos de la compañía, es decir debe existir una conexión directa entre los objetivos de negocio y los objetivos de seguridad digital, esta definición será diferente para cada empresa, dado que los objetivos de cada empresa son diferentes, lo relevante es poder conectar ambas estrategias, de manera que las acciones de seguridad digital soporten los objetivos estratégicos, siendo un aporte real para los objetivos de la compañía.

Una forma de conectar estos objetivos estratégicos es mediante el mapeo de objetivos estratégicos del Mapa Estratégico de la compañía, con los objetivos de seguridad digital, para el caso se tomará como ejemplo un mapa estratégico genérico figura N° 21.

Figura N° 21: Marco del BSC, Cuadro de Mando Integral Genérico.

Fuente: (P.Norton, 2004)

Se puede apreciar en la Figura N° 21 las diferentes perspectivas del BSC (Balanced Score Card), este mapa estratégico es diferente en cada empresa, sin embargo para poder dar un ejemplo, se considera un BSC genérico, existen perspectivas donde poder conectar con la estrategia corporativa, en primer lugar la perspectiva del cliente, donde las características del producto o servicio, características como la calidad, la confidencialidad, la disponibilidad de una

plataforma digital, están directamente relacionados con la seguridad digital y obviamente estos indicadores se pueden ver afectados negativamente con un ataque de estas características.

Del punto de vista de la perspectiva financiera el indicador Valor sostenido por los accionistas, si una empresa sufre un incidente de seguridad digital, el valor de la acción pudiera verse afectado, como fue el caso de las acciones de Facebook que cayeron por el escándalo de la filtración de datos durante la campaña electoral en EEUU (INFOBAE, 2018), por lo tanto la perspectiva financiera también se ve afectada por los incidentes de seguridad digital.

Al revisar la perspectiva proceso interno, donde se tiene Gestionar Innovación por ejemplo, si este proceso de innovación se refiere a un proceso de Transformación Digital, claramente la seguridad digital está directamente relacionada a ese proceso, por lo tanto se tiene otra conexión al mapa estratégico.

Se han dado algunos ejemplos de cómo conectar la seguridad digital con la estrategia corporativa, generalmente la forma simple de conectar es con algún indicador del producto o servicio, en una empresa digital, varias de las características del producto se pueden ver afectadas por un problema de seguridad digital, o lo que sería mejor y recomendable, que la seguridad digital fuera una más de sus características principales consideradas en el BSC.

Se recomienda también trabajar en la construcción de un BSC de Seguridad Digital, donde se puedan apreciar los diferentes indicadores que son relevantes en este proceso, apoyando con ello el logro de la misión de la organización.

9.2 Responsable de la estrategia corporativa de Seguridad Digital

Al contar con el mapeo de los objetivos estratégicos de Seguridad Digital con los objetivos estratégicos de la compañía, es necesario contar con un ejecutivo responsable de gestionar la estrategia de seguridad digital.

Este ejecutivo es el CISO que viene del inglés Chief Information Security Officer, que castellanizado viene siendo el Gerente de Seguridad Digital o Director de Seguridad Digital, este ejecutivo debe ser de primera línea, para tener canal directo y reportar a la directriz principal de la compañía, trabajando en conjunto y apoyando los objetivos estratégicos de la compañía.

En este mismo punto y reforzando el párrafo anterior, es importante señalar que la seguridad digital es un tema estratégico en las compañías y no un tema únicamente tecnológico, eso refuerza que el ejecutivo debe ser de primera línea y

no debe estar reportando a áreas de tecnología o similar, es parte de la estrategia corporativa como cualquier otro gerente o gerencia de primera línea.

En empresas pequeñas podrá ser un ejecutivo que tenga este rol en conjunto con otro, en empresas más grandes será un rol único e independiente, si se trata de una empresa pequeña, la recomendación es que este rol no sea juez y parte de la misma estrategia, es decir, es ideal que sea independiente de las áreas que generan riesgos de seguridad digital.

Principales responsabilidades del ejecutivo responsable:

- Responsable de diseñar e implementar la estrategia de seguridad digital.
- Tiene a su cargo el desarrollo inicial de las políticas de seguridad de primer nivel y el control de su implementación y velar por su correcta aplicación.
- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- Comunicar y difundir la Política de Seguridad a la compañía.
- Dar el apoyo metodológico para evaluar los riesgos asociados a la Seguridad de la Información, seguridad digital y tecnológica.

9.3 Definición de la estrategia corporativa de Seguridad Digital

En el punto 8 se analizaron dos modelos para definir una estrategia de seguridad digital, la ISO 27001 y el NIST CSF, se puede apreciar también en la tabla N° 1 una comparativa entre ambos modelos, estos modelos son los más ampliamente utilizados a nivel mundial (punto 8.1.4), pero como existen diferencias entre ellos la estrategia que se propone es una mezcla de ambos, de acuerdo a la tabla N° 1, la ISO 27001 tiene mayor fortaleza en lo que es la ejecución de la estrategia, el gobierno del proceso de seguridad digital, como también todo lo que tiene que ver con la documentación y registros necesarios, sin embargo en la implementación de la estrategia de controles de seguridad digital el NIST CSF tiene ventajas en comparación con la ISO 27001, es más simple entender y enfocar los esfuerzos en objetivos claros de seguridad digital, es por este motivo que se emplearán ambos modelos.

Como la estrategia será en base a estos dos modelos, será la ISO 27001 la que definirá el gobierno del proceso, mediante la creación de lo que se llama un **“Sistema de Gestión de Seguridad de la Información”**, conocido por sus siglas **SGSI**, que corresponde a la implementación del modelo.

Se hace el hincapié como se vio en el punto 8 este Sistema de Gestión se puede utilizar en cualquier tipo de empresa independiente de la industria.

9.1 Documentando la estrategia corporativa de Seguridad Digital

El primer paso en la construcción del SGSI, es documentar los objetivos de seguridad digital, un documento que sea conocido por todos los integrantes de la empresa, que sea la carta de navegación, lo que la empresa quiere conseguir implementando la estrategia de seguridad digital, a este documento se le llama “Política de Seguridad Digital”, donde se documentan las principales directrices de seguridad digital para la compañía, en este documento se deberán definir al menos lo siguientes puntos:

- **Objetivos:** Qué se quiere lograr con la estrategia, donde se quiere llegar, como se alinea con la estrategia corporativa, etc.
- **Alcance:** Qué áreas de la empresa se rigen por estos objetivos, debería ser toda la compañía, pero podría ser implementado primeramente en un área y después en toda la compañía.
- **Mapa estratégico:** Descripción de cómo la estrategia de seguridad digital se alinea con la estrategia corporativa (punto 9.1)
- **Partes Interesadas:** Descripción de las partes interesadas por parte de la estrategia, quienes son relevantes en este proceso, va depender del tipo de empresa y en el entorno en el que se desempeña.
- **Organización interna:** Descripción de la organización de la empresa, las gerencias que la componen y su objetivo.
- **Factores internos y externos:** Qué factores afectan a la seguridad digital, tanto externos como internos.
- **Gestión de riesgo:** Metodología de gestión de Riesgo (punto 9.6)
- **Organización de la Seguridad:** Cómo estará organizada la seguridad en la compañía.(punto 9.2 y 9.5)
- **Funciones del NIST CSF:** En este punto se debe incorporar algo muy similar a lo del punto 8.2 pero con un nivel detalle mayor, incorporando también información del anexo N°3.

Este documento debe ser de simple entendimiento, que la organización pueda leer y entender perfectamente las directrices, dado que se necesita encarecidamente que la organización se haga parte y contribuya.

Esta política pasa a ser el principal registro de la estrategia, define los principales lineamientos de seguridad digital, este documento debiera ser revisado cada año en conjunto con las cambios de estrategia de la compañía, si existe un cambio de rumbo pudiera reflejar un cambio de rumbo o modificación de la estrategia de seguridad digital también.

La política de seguridad como principal registro de la estrategia, también se emplea para efectos de demostrar a una entidad externa, una auditoria o similar, que la compañía está trabajando en un proceso de seguridad digital y que por lo tanto se está haciendo cargo de la problemática.

9.2 Comité responsable y de apoyo

Una vez definido los principales lineamientos de seguridad digital para la compañía, se debe crear un comité de seguridad, que va a depender de como esté organizada la empresa si es un comité particular para el tema, será parte de un comité general donde se discutan diferentes tópicos o algún otro tipo de organización.

Es relevante que este comité esté compuesto por todos los altos directivos de la compañía, comenzando por el Gerente General. Dependiendo también de cómo se organiza la empresa y si cuenta con un directorio, el comité también puede estar formado por directores, para este tipo de organización no existe una regla, la idea es que con una periodicidad definida este comité de altos ejecutivos se reúna y se discutan los diferentes temas de seguridad digital, proyectos asociados, iniciativas, aprobación de directrices, conocimiento de los riesgos detectados y sus planes de mitigación, etc.

Principales responsabilidades del Comité de Seguridad:

- Conocer y aprobar las políticas de seguridad.
- Conocer los riesgos relevantes asociados a la Seguridad Digital.
- Velar por la implementación del Sistema de Gestión de la Seguridad de la Información.
- Monitorear el cumplimiento de cada uno de los aspectos señalados en la Política.
- Conocer y aprobar las excepciones permanentes a la Política.
- Apoyar al CISO en la implementación de directrices y gestión del SGSI.

9.3 Proceso de Gestión de Riesgo.

Una vez conformada el proceso de gobierno de seguridad digital, la designación del ejecutivo responsable, la conformación del comité, la definición de la estrategia, corresponde pasar a uno de los procesos más relevantes, la Gestión de Riesgos.

¿Por qué es tan relevante?, la respuesta es simple, debido que las organizaciones no cuentan con recursos infinitos, debido que existen prioridades dentro de la organización que considerar, por lo tanto el proceso de gestión de riesgos ayuda a resolver estas restricciones de la implementación, este proceso debe encargarse de identificar los principales problemas, riesgos de seguridad digital que la empresa cuenta, es relevante conocer el estado actual en el que se encuentra la empresa, para poder focalizar los recursos a mejorar los procesos y servicios que la empresa tiene en mayor riesgo, donde un incidente le pueda traer graves consecuencias, consecuencias que pueden ir desde generar trastornos en su oferta ser servicios, hasta dejarlos completamente fuera de línea, o no disponibles.

El entregable de este proceso, es una priorización de los riesgos de mayor a menor, información que debe ser conocida por los altos ejecutivos, también debe ser conocida por el comité de seguridad. Este proceso dará origen a la generación de los presupuestos necesarios para seguir avanzando, pondrá al tanto a los ejecutivos de la real situación de la tecnología digital en función del riesgo, pudiendo gatillar en algunos casos, cambios de timón del punto de vista de la estrategia, debiendo ser un proceso que sirva de apoyo fundamental en la toma de decisiones de la empresa en este ámbito.

9.3.1 Metodología de gestión de riesgo

Existen varias metodologías para trabajar un proceso de gestión de riesgo, muchas empresas pueden ya contar con un proceso corporativo de riesgo, en tal caso la tarea es sumarse a este proceso, seguir los lineamientos y trabajar en la identificación de los riesgos de seguridad digital, sin embargo para empresas que no cuenten con un proceso corporativo a continuación se realiza una recomendación de cómo se debe trabajar este proceso.

Gestión de riesgo ISO 31000: 2018

ISO 31000:2018 es la norma internacional que proporciona principios y directivas eficaces para el tratamiento y la gestión de riesgos. Esta norma ayuda a las organizaciones a identificar, analizar, evaluar y tratar sus riesgos.

ISO 31000:2018 aporta sus beneficios a organizaciones públicas o privadas, es posible aplicarla a todo tipo de actividades o negocios.

Esta metodología está basada en la detección de riesgos por proceso de negocio, tanto a nivel estratégico como a nivel operativo, donde en su etapa final los riesgos son registrados en un mapa de riesgos.

La descripción de la metodología se realiza en dos fases:

I. La estructura recomendable para el gobierno del proceso.
II. Los pasos a seguir para la gestión de riesgo.

I. Estructura recomendable para el gobierno de la gestión de riesgos

La estructura más recomendable para la gestión de riesgos, es alinear el proceso a un ciclo de mejora: planificar, hacer, verificar, actuar, los puntos relevantes son los siguientes:

Parte 1: Existencia de un compromiso de la alta dirección.

Parte 2: Diseño del marco de trabajo de la gestión de riesgo.

- Compresión de la organización y de su contexto.
- Establecimiento de la política de gestión del riesgo.
- Integración en los procesos de la organización.
- Recursos necesarios.

Importante para este proceso como para cualquier otro proceso de implementación de un modelo ISO, es que la empresa debe contar con un mapa de procesos corporativos, donde este claramente identificado cada proceso estratégico, gestión, operativo y táctico, dado que para el caso, la gestión de riesgos se basa en identificar riesgos de los procesos de negocio.

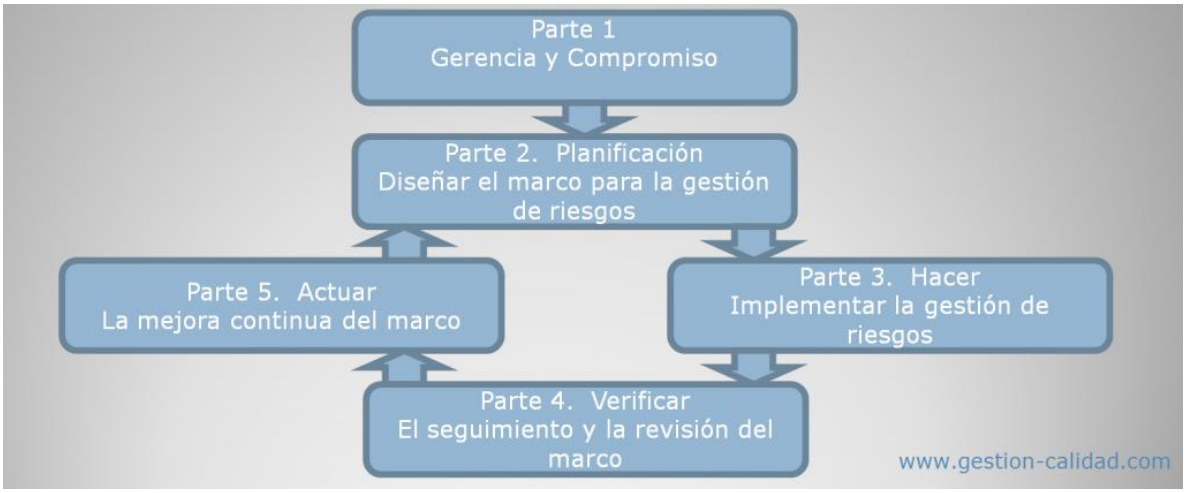
Parte 3: Implementación del proceso de gestión de riesgo

Parte 4: Seguimiento y revisión del marco de trabajo

Parte 5: Mejora contínua del marco de trabajo.

En la figura N° 22, se puede apreciar el ciclo PDCA de gestión de riesgo.

Figura N° 22: PDCA Gestión de riesgos



Fuente: (Gestion Calidad, 2018)

II. Los pasos a seguir para la Gestión de riesgo ISO 31000:2018

La norma ISO 31000:2018 “Gestión del riesgo” recomienda un proceso, paso a paso, para la gestión efectiva de riesgos.

El proceso de la gestión del riesgo es una parte integral de la gestión y de la toma de decisiones y se debe integrar en la estructura, las operaciones y los procesos de la organización. Puede aplicarse a nivel estratégico, operacional, de programa o de proyecto.

Aunque el proceso de la gestión del riesgo se presenta frecuentemente como secuencial, en la práctica es iterativo, se describe a continuación:

1. Comunicación y consulta

El propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas.

2. Alcance, contexto y criterios.

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos externo e interno.

3. Evaluación del riesgo.

Identificación del riesgo.

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

Análisis del riesgo.

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

Valoración del riesgo.

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecido para determinar cuándo se requiere una acción adicional.

4. Tratamiento del riesgo.

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo, generalmente las acciones de tratamiento son: aceptar, mitigar, transferir y eliminar los riesgos.

5. Seguimiento y revisión.

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

6. Registro e informe en el Mapa de Riesgos.

El resultante final del proceso de gestión de riesgos es el mapa de riesgos, el cual permite comprender las amenazas y facilitar la toma de decisiones a través de la prevención de los posibles riesgos que se le pueden plantear a la organización.

El mapa en si se trata de una representación gráfica de los objetivos estratégicos de la organización, donde se sitúan cada uno de los riesgos más representativos para la empresa.

El mapa cuenta con dos variables, probabilidad e impacto, del punto de vista cualitativo y cuantitativo, permitiendo de esta manera determinar un mapa de calor, que tiene relación con el apetito de riesgo, definiendo ambos conceptos se tiene:

Probabilidad: posibilidad de que en un determinado riesgo pueda ocurrir en el desarrollo de la actividad, cuan frecuente es.

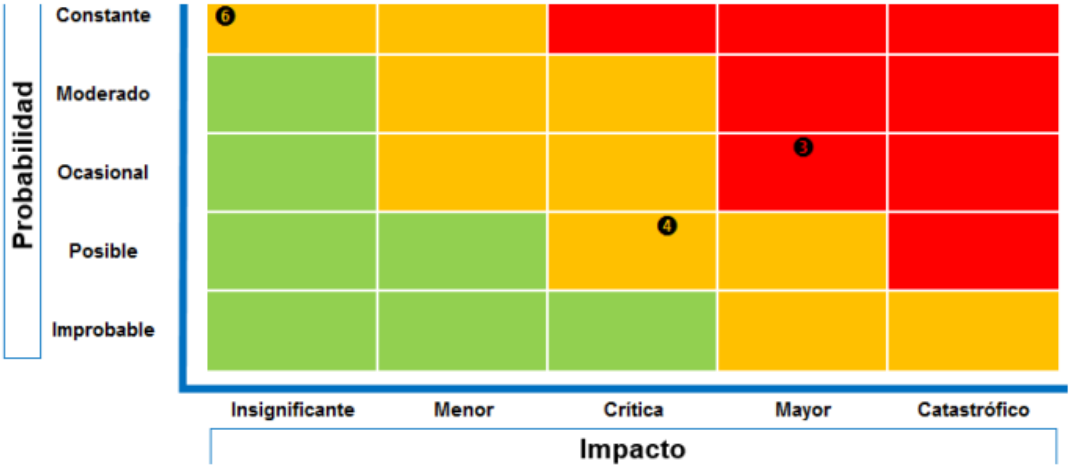
Impacto cuantitativo y cualitativo: efecto económico, operacional, imagen corporativa, de la materialización del riesgo.

Este tipo de representaciones gráficas contribuyen a que los altos directivos de las empresas comprendan de un modo visual cual es la situación de la compañía. Las organizaciones aceptan, mitigan o transfieren esos riesgos dependiendo de la probabilidad de que se produzcan y de su impacto,

Por lo tanto en esta misma línea todos aquellos riesgos que la estrategia sea **mitigarlos,** pasan a ser el foco principal de la implementación de controles de seguridad digital, es decir mediante esta metodología, se tiene la priorización de los esfuerzos y recursos necesarios para poder comenzar a implementar.

En la figura N° 23 se puede apreciar un mapa de calor.

Figura N° 23: Mapa de riesgos, mapa de calor.



Fuente: (EALDE BUSINESS SCHOOL, 2018)

Se puede apreciar en la Figura N° 23, que existen 3 diferentes niveles de riesgo, en color verde los de nivel bajo, en color amarillo los de nivel medio, en color rojo los de nivel alto, cuando se habla de apetito de riesgo, se refiere al nivel de riesgo del mapa de calor que la organización está dispuesta a aceptar, una organización con un proceso de gestión de riesgo maduro, generalmente su apetito de riesgo debería aceptar riesgos bajos únicamente, por consiguiente tratar riesgos de nivel medio y alto, sin embargo en una organización que este comenzando a trabajar en un proceso como este, se recomienda un apetito de riesgo, donde se acepte los riesgos bajos y medios, es decir se traten o mitiguen únicamente los riesgos altos, esto para poder priorizar y también dosificar los recursos necesarios.

En la figura N° 24, se puede apreciar un esquema del proceso descrito en su conjunto.

Figura N° 24: Proceso ISO 31000: 2018

Fuente: (SPC Consulting Group, 2018)

Cuáles son los Beneficios de ISO 31000 (ISO TOOLS ORG, 2018)

- Mejora la eficiencia operativa de la organización en forma proactiva, y fomenta el liderazgo de la Alta Dirección.
- Construye confianza entre las partes interesadas, que se ven beneficiadas con la prevención de los riesgos.
- Aplica controles de Sistema de Gestión al análisis de riesgos para minimizar su impacto negativo.
- Mejora el rendimiento y la sostenibilidad de otros Sistemas de Gestión, como el de la calidad.
- Se adapta fácilmente a los cambios y las modificaciones de forma eficaz, sobre todo en la medida en la que la organización se expande.
- Optimización de los recursos utilizados por la organización en la prevención de riesgos.
- Reducción de costos, gracias a la disminución de incidentes o eventos generadores de riesgos.
- Aprovechamiento de nuevas oportunidades.
- Mejora de la planificación y reducción de incidentes generadores de pérdidas inesperadas.

9.4 Gestión corporativa del cambio

Con el proceso de gestión de riesgo finalizado, como se comentó anteriormente, se tiene la prioridad y el foco de donde están los problemas, los mayores riesgos de seguridad digital, sin embargo, como en el proceso de seguridad digital se trabaja con personas de la organización, un proceso que es necesario considerar es la gestión del cambio.

La gestión del cambio busca facilitar y conseguir la implementación exitosa de los procesos de transformación, lo que implica trabajar con y para las personas en la aceptación y asimilación de los cambios y en la reducción de la resistencia, facilitando la aceptación y asimilación de los cambios, producto de una nueva forma de operación. (KPMG, 2018).

El proceso de gestión de cambio cuenta con 3 fases o estados: Estado Presente, Estado de Transición y Estado Futuro, ver Figura N° 25

Figura N° 25: Estados de la Gestión de Cambio.

Fuente: (EXEVI, 2018)

Existen diferentes metodologías para implementar la gestión del cambio la interior de una organización, en la Figura N° 26 se puede apreciar la metodología de (KPMG, 2018).

Figura N° 26: Metodología de gestión de Cambio

Fuente: (KPMG, 2018)

9.5 Concienciación de los colaboradores

¿Quién gestiona la información en la empresa? Los empleados son los encargados de gestionar, procesar, almacenar, modificar, transmitir y eliminar la información en una empresa. Son el engranaje principal para el buen funcionamiento, pero ¿conocen los riesgos en materia de Seguridad Digital? (INCIBE, 2018)

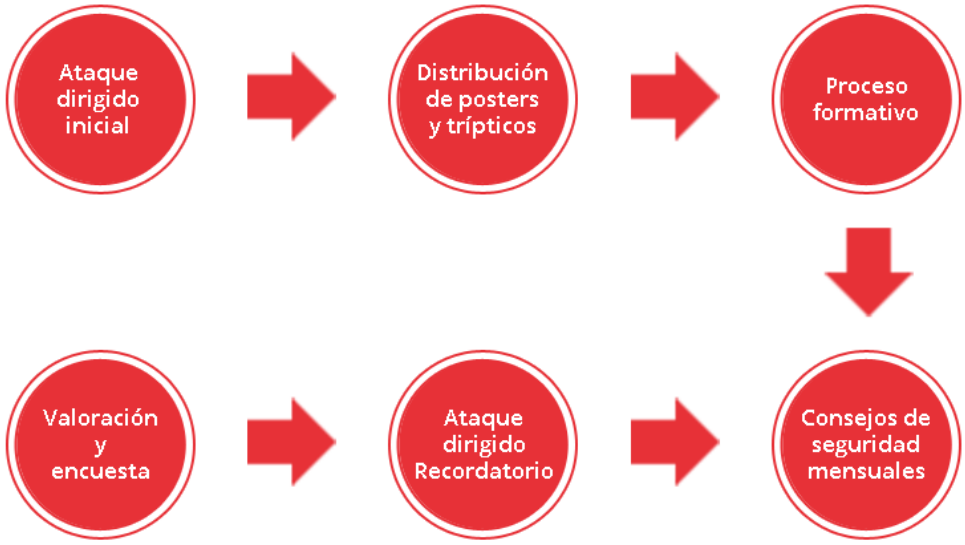
Puede haber riesgos por desconocimiento y desinformación que sitúen a la empresa en una situación crítica. Por lo tanto es necesario formar a los empleados por medio de la concienciación en materia de Seguridad Digital. (INCIBE, 2018)

Existen tres aspectos claves para que la concienciación en Seguridad Digital del personal funcione (PMG SSI, 2018):

- Demostrar convincentemente que las brechas de seguridad no solo afectan negativamente a la organización, sino que también puede dañar a los empleados de manera individual.
- Se debe enfocar y **reforzar constantemente** los fundamentos de una fuerte práctica de seguridad.
- Debe ser atractiva para los empleados haciendo hincapié en la importancia que tiene para ellos.

El Instituto Nacional de CiberSeguridad de España INCIBE, propone una atractiva metodología de concienciación, consiste en lo siguiente (INCIBE, 2018):

Figura N° 27: Etapas de concienciación de colaboradores



Fuente: (INCIBE, 2018)

Ataques Dirigidos: La conciencia empieza con uno o dos ejercicios que van a permitir evaluar el nivel de concienciación en seguridad de los empleados a la vez que se despierta su interés por aprender más. Estos ejercicios toman la forma de ataques sorpresa.

Pósteres y Trípticos: Después de lanzar un ataque dirigido se debe distribuir en lugares de paso frecuente dos tipos de materiales: pósteres y trípticos.

Proceso Informativo: Una vez despertado el interés, se plantea realizar un proceso formativo combinado con la distribución de material para su lectura y visualización son la opcional organización de charlas. Esta fase consta de cuatro bloques temáticos: la información, los soportes, el puesto de trabajo y los dispositivos móviles.

Consejos de seguridad mensuales: Consejos temáticos para reforzar lo aprendido, este tipo de material puede ser enviado por correo electrónico, publicado en una intranet o distribuirse de manera impresa.

Valoración: Cuando haya terminado la concienciación en la empresa puede realizar una prueba online, un set de preguntas o volver a enviar nuevamente un

ataque dirigido y así sucesivamente se debe ir reforzando este proceso de manera constante, se debe considerar que existe la rotación de personal y también que las personas pueden olvidar lo aprendido.

Para mayor detalle se puede dirigir al sitio web de (INCIBE, 2018) y descargar el **Kit de concienciación**.

9.6 Implementación del NIST CSF

Del punto 9.1 al punto 9.8 está creada la estructura de gobierno del proceso de Seguridad Digital, considerando además procesos relevantes como la gestión del cambio y la concienciación de los empleados, el proceso central del modelo es la gestión de riesgos punto 9.6, al finalizar este proceso ya se tiene claridad cuáles son los riesgos más altos presentes en la empresa, por lo tanto se sabe dónde se deben destinar los recursos necesarios, se tiene claro cuál es el foco de la implementación.

Del punto de vista de la gestión de riesgo, NIST presenta una primera clasificación, los niveles los Tier siendo del 1 al 4 (punto 8.2.1 niveles de implementación), este nivel va depender exclusivamente de cómo esta implementado el proceso de gestión de riesgo en la compañía, siendo Tier 1 para empresas que estén comenzando a trabajar en este proceso, como Tier 3 o Tier 4 para empresas que ya llevan un tiempo con este proceso de manera corporativa. Idealmente mientras más maduro está el proceso de gestión de riesgo, más sólida será la implementación y más acertadas serán las decisiones y destinación de los recursos para la implementación, para mayor detalle y descripción de los diferentes Tier y como clasificar a la empresa referirse al NIST (NIST, 2018).

Para comenzar a implementar el NIST en una compañía, primeramente se debe conocer cuál es el perfil actual de la empresa, el perfil viene siendo el nivel de implementación de controles que la empresa tiene actualmente sin haber implementado NIST, es decir es un levantamiento de cómo está la seguridad digital en comparación con las categorías y subcategorías del NIST (anexo 3), por lo tanto se deben realizar reuniones de levantamiento para obtener esta información, reuniones con los diferentes encargados, administradores, operadores, etc., para poder determinar, cual es el perfil actual de la empresa, con este levantamiento se sabrá también cual es el nivel de acuerdo a las 5 funciones del NIST (punto 8.2.3), con la creación de este perfil actual, se podrá saber también en cuál de las 5 funciones existe mayor debilidad y por ende cual requiere mayor foco.

Justamente en este momento cuando se crea el perfil actual es cuando interviene el proceso base que es la gestión de riesgos, al crear el perfil actual de la empresa, se podrá ver el gap o brecha en cada una de las funciones, categorías y

subcategorías, se pueden encontrar muchos controles inexistentes o no implementados, pudiendo parecer inalcanzable poder tener todos los controles funcionando en una empresa que está comenzando a trabajar el proceso de la seguridad digital. Diferente será en una empresa que ya tiene un nivel de madurez mejor en seguridad digital, donde el NIST entregará este gap, el cual será útil para poder identificar sus fortalezas y debilidades de acuerdo a la creación del perfil actual comparando con las cinco funciones, es decir que función esta mejor; identificar, detectar, proteger, recuperar, responder.

Por este motivo es que la gestión de riesgo es un proceso base, porque para el caso de la empresa que tenga un perfil con muchos gap en las cinco funciones, deberá analizar este resultado con el resultado de la gestión de riesgo y destinar o priorizar sus recursos, enfocándose en las categorías y subcategorías que representan un mayor riesgo al negocio, por lo tanto, el plan de implementación, deberá contar con este foco descrito.

Con el perfil actual en conjunto con los resultados de la gestión de riesgo, se procede a crear un perfil futuro, esto es, donde la empresa quiere llegar, cuales son las prioridades, cual es el presupuesto necesario para lograrlo.

Debido a que el presupuesto es una variable relevante en cualquier proyecto, la manera de apalancar el presupuesto es nuevamente con los resultados de la gestión de riesgo, la segunda lectura de la gestión de riesgo permite conocer el impacto de no implementar el perfil futuro definido, (en la figura N° 15 se puede revisar un ejemplo de un perfil futuro), cuales con las consecuencias de implementar un plan, que podría ocurrir o que ha ocurrido.

A continuación de acuerdo a una serie de supuestos, se da un ejemplo de un plan de implementación con las etapas previas.

9.6.1 Ejemplo de un plan de implementación del NIST CSF

A continuación se da un ejemplo de un resultado del proceso de gestión de riesgo, tomando en consideración un proceso de negocio, este es mapeado a la función del NIST correspondiente, su categoría y subcategoría, para posterior proponer un plan de implementación.

Supuestos a considerar:

Empresa: Se trata de una empresa que ofrece servicios financieros a través de su página web y aplicaciones Mobile.

Riesgo detectado: Se detectó que la empresa tiene fuertes debilidades en las soluciones tecnológicas para poder detectar proactivamente intentos o ataques de seguridad digital, entiéndase ataques, hackeos a su plataforma web o su plataforma mobile, por lo tanto su proceso de monitoreo no es el adecuado, de hecho se pudo identificar que esta empresa ya fue víctima de un ataque de esta índole, por lo tanto la probabilidad es constante y su impacto es mayor debido que le sustrajeron dinero ver Figura N° 24, por lo tanto el riesgo es registrado como "Deficiencias en el proceso de Monitoreo de Seguridad".

Apetito de riesgo: El apetito de riesgo de esta empresa, es tomar acciones sobre todos los riesgos altos detectados, es decir generar un plan de mitigación para los riesgos de nivel alto.

Resultados del análisis de riesgo: Al contar con un riesgo de probabilidad constante e impacto mayor, el riesgo es de nivel alto, debido a que el riesgo queda situado en el sector rojo del mapa de calor, ver figura N° 24.

Desarrollo del plan

De acuerdo al riesgo detectado y al revisar el NIST, coincide directamente sobre la función detección, la cual se despliega a continuación en la figura N° 28.

Figura N° 28: Función detección de NIST CSF

Detección	Anomalias y eventos	DE.AE
	Monitoreo Continuo de Seguridad	DE.CM
	Detección de procesos	DE.DP

Fuente: (NIST, 2018)

Se puede apreciar que la función detección cuenta con 3 categorías:

- Anomalías y eventos.
- Monitoreo continuo de Seguridad
- Detección de procesos

De acuerdo al riesgo detectado, el siguiente paso es identificar a que categoría de NIST corresponde el riesgo, para este caso es Monitoreo continuo de Seguridad, esta categoría es desplegada en la Figura N° 29.

Figura N° 29: Categoría Monitoreo continúo de Seguridad del NIST

Detección	Monitoreo Contínuo de Seguridad (DE.CM) Los sistemas de información y activos son monitoreados para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	DE.CM-1: La red es monitoreada para detectar eventos potenciales de ciberseguridad.
		DE.CM-2: El ambiente físico es monitoreado para detectar potenciales eventos de ciberseguridad.
		DE.CM-3: La actividad de personas es monitoreada para detectar potenciales eventos de ciberseguridad.
		DE-CM-4: El código Malicioso es detectado
		DE-CM-5: El código mobile no autorizado es detectado.
		DE-CM-6: La actividad de proveedores externos es monitoreada para detectar potenciales eventos de ciberseguridad.
		DE.CM-7: Monitoreo de personas no autorizadas, conexiones, dispositivos y software es desarrollada.
		DE-CM-8: Escaneos de vulnerabilidades son desarrollados.

Fuente: (NIST, 2018)

Se puede apreciar que en la Figura N° 29 la categoría de Monitoreo continuo de Seguridad cuenta con 8 subcategorías, a modo de ejemplo se toman dos subcategorías para desarrollar un plan, las siguientes:

- DE.CM-4: Código Malicioso es detectado
- DE.CM-8: Revisiones o Escaneos de vulnerabilidades son realizados.

En la Figura N° 29 se puede apreciar que la subcategoría tiene información de referencia, esto es muy útil dado que si el profesional a cargo del plan requiere de un mayor detalle del control, puede verificar la información del control en otro

modelo, esta funcionalidad del NIST es muy útil debido que permite medir el nivel de implementación con más de un modelo y para el caso de este análisis se puede comparar por ejemplo con la ISO 27001:2013.

En la Figura N° 30 se puede apreciar la información de ambos controles del NIST de acuerdo a la referencia de la ISO 27001:2013.

Figura N° 30: Equivalencia de controles de la Figura 29 NIST con la ISO 27001:2013

12.2	Protección contra el Malware
	Control para el malware es requerido, incluyendo la concienciación de los usuarios.
12.6	Administración Técnica de Vulnerabilidades
	Las vulnerabilidades técnicas deben ser remediadas y debieran existir reglas para el gobierno de la instalación de software por parte de los usuarios.

Fuente: (ISO 27001 Security, 2018)

En la Figura N° 30 se aprecia que el control DE.CM-4 de NIST de la figura N° 29, equivale al 12.2 de la ISO 27001:2013 y el control DE.CM-8 de la misma figura, equivale al control 12.6 de la ISO 27001:2013.

Plan de Mitigación

Plan 1:

Tomando como referencia el NIST se tiene el primer control DE.CM-4 de la Figura N° 29, que se refiere a protección contra el malware y también la concienciación de los empleados.

El plan a implementar consistirá en revisar la versión y nivel de actualización de la solución antimalware, verificar si la versión tiene la capacidad de detección temprana de malware, si cuenta con capacidades de machine learning para la detección de malware por comportamiento. Si la solución no cuenta con estas características, deberá realizar una evaluación técnica-financiera para migrar, cambiar o reemplazar la actual solución antimalware de la empresa.

Como segunda acción del plan, se procederá a crear un plan de concienciación con foco en los peligros de infección de malware para los empleados, tomando como ejemplo lo descrito en el punto 9.8.

Plan 2:

Tomando como referencia el NIST se tiene el segundo control DE.CM-8 del Figura N° 29, que se refiere a la revisión de vulnerabilidades de los sistemas. Se deberá crear un proceso de revisión de vulnerabilidades de los sistemas de manera periódica, para posterior, establecer un segundo proceso de parchado de las vulnerabilidades encontradas, proceso que deberá trabajar en un círculo de mejora continua, en paralelo se debe regular la instalación de software por parte de los empleados, el cual idealmente se deberán limitar los permisos para que los usuarios no tengan el privilegio de instalar software y de necesitarlo se deberá crear un requerimiento a la mesa de ayuda.

El punto 9.9.1 corresponde a un ejemplo de cómo proceder en el proceso de implementación, la cadena completa desde la detección de un riesgo en el proceso de gestión de riesgo hasta la generación del plan para su mitigación, este proceso deberá repetirse para cada riesgo detectado como prioridad, de acuerdo al apetito de riesgo definido.

Nota relevante:

Es necesario mencionar que una estrategia de la aplicación del modelo, en particular de la implementación de los controles, ideal sean aplicados, relevados, discutidos, en las etapas de diseño de los proyectos y no al final, se generan dificultades al implementar un control cuando el , producto-servicio o proceso está ya en operación, se generan impactos financieros y también operacionales, porque no se cuenta con ventanas de tiempo para detener el servicio, puede incluso generar una modificación mayor a la solución el revisarlo al final.

Por lo tanto se recomienda encarecidamente, que el proceso de seguridad digital se haga parte desde el diseño hasta la puesta en marcha de las diferentes soluciones digitales de las empresas, que sea un eslabón más como parte de la gestión de proyectos corporativos.

9.7 Proceso de auditoria

Una vez que el modelo ya está en funcionamiento, corresponde revisar el estado de la implementación, revisar cómo se han ido mitigando los riesgos, como está el nivel de controles de seguridad digital, la función del proceso de auditoria es generar observaciones y oportunidades de mejora como proceso de retroalimentación al modelo.

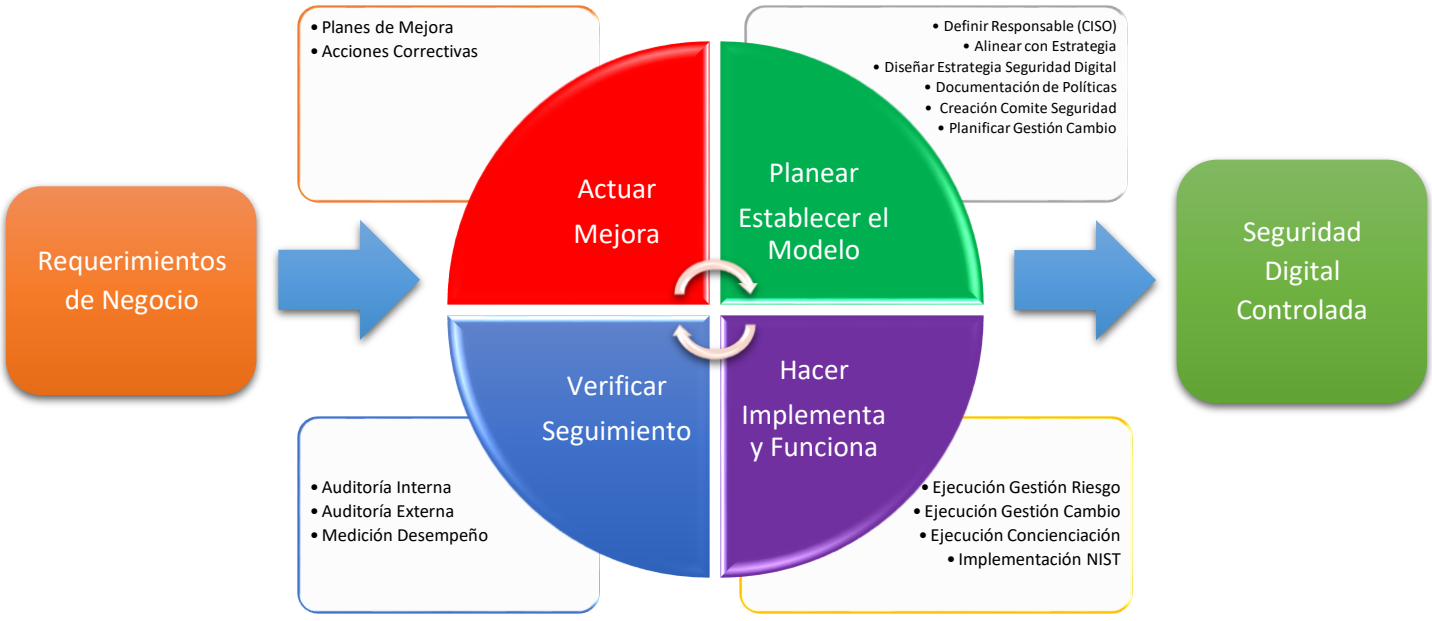
En empresas medianas o grandes, es probable que cuenten con un departamento o una gerencia de auditoria interna, área responsable de revisar el cumplimiento y

funcionamiento de procesos dentro de las empresas, detectando anomalías en pos de la generación de mejoras. Esta área es la encargada de revisar el estado de la implementación del modelo de seguridad digital, es ideal que este proceso sea realizado por una área que no sea la misma dueña del proceso, para poder contar con una opinión objetiva, de hecho también está la opción que una empresa auditora externa realice este proceso, una opinión totalmente independiente a la compañía, para el caso ambos procesos de auditorías se pueden realizar, va depender también el rubro de la empresa, respecto a la obligatoriedad respecto a procesos de auditorías, por lo tanto se recomienda como mínimo ejecutar el proceso de auditoría interna.

9.8 Resumen del modelo de Seguridad Digital

Hasta acá finaliza la propuesta de implementación del Modelo de Seguridad Digital, modelo que cuenta con una serie de etapas descritas en el punto 9, a continuación un diagrama en un ciclo de mejora continua de todo el modelo, ver Figura N° 31.

Figura N° 31: Modelo de Seguridad Digital en un ciclo de mejora continua.



Fuente: Propia

Como se puede apreciar en la Figura N° 31, el ciclo de mejora continua regula todo el proceso de Seguridad Digital, siguiendo el lineamiento de la ISO 27001:2013 para su gobierno, donde en el proceso “Hacer”, está la implementación del NIST y sus controles, dando correlación a la definición de estrategia definida en el punto 9.3, para posteriormente seguir con el proceso “verificar” donde está la auditoria interna que su resultado retroalimenta al modelo para la mejora continua de todo el proceso.

Ventajas de la utilización de este modelo

La principal ventaja de la utilización de este modelo es que cubre tanto la perspectiva estratégica como la perspectiva operacional, implementar únicamente la ISO 27001 se tiene cobertura estratégica sin la granularidad adecuada del punto de vista operacional, la ISO no contempla el ordenamiento de los controles en función de cómo establecer una estrategia táctica, que oriente a los responsables técnicos en el cómo enfrentar y organizarse frente a las amenazas cibernéticas, por el contrario ,implementar solo el NIST CSF se tiene una cobertura detallada y un enfoque muy claro de la perspectiva operacional de seguridad digital, pero claramente es indispensable la componente estratégica, por ese motivo este modelo mixto permite tener una cobertura total de la problemática. Además el modelo es súper claro en definir el liderazgo de esta estrategia, en general los modelos no son específicos en este aspecto, sin embargo, dada la problemática es necesario establecer un estándar y una directriz clara, la cual está completamente alineada con las leyes y regulaciones que se vienen por el lado del Gobierno de Chile, finalmente una gran diferencia de este modelo a cualquier otro en el mercado, es que este modelo aborda el cómo alinear la estrategia de seguridad digital con el logro de la misión de la organización, por lo tanto, cubre todos los ámbitos necesarios para enfrentar adecuadamente las amenazas cibernéticas actuales.

9.9 Conclusiones

La problemática de la seguridad digital al igual que los procesos de digitalización de los negocios llegaron para quedarse, queda demostrado que dentro de las múltiples variables a gestionar en este aspecto, la seguridad digital es indispensable, los impactos que puede tener un incidente de seguridad digital son

múltiples, van desde el daño de la imagen de la compañía hasta las pérdidas financieras acarreadas ya sea por temas operacionales o por efecto de los daños de imagen, por lo tanto es relevante que las compañías tomen conciencia de lo que significa y se hagan cargo de la problemática de manera preventiva.

Según los estudios de esta investigación queda de manifiesto que a nivel país tampoco las noticias son muy alentadoras, sin embargo a raíz de los incidentes ocurridos en el último tiempo en Chile (2018), el gobierno tomó acciones concretas y estableció un mapa de navegación, esta ruta crítica entrega luces de que el país, tiene la capacidad de mejorar para enfrentar las amenazas cibernéticas, al igual que la resiliencia para enfrentar las catástrofes naturales. Estas acciones del gobierno demuestran que es un tema preocupante del punto de vista de la economía digital, así como se daña la reputación de una empresa, también se puede dañar la imagen de un país y el país puede ser menos atractivo del punto de vista de la inversión extranjera.

Para poder enfrentar adecuadamente esta problemática cada empresa debe ser autosuficiente y autónoma en el cómo enfrentar este tipo de amenazas, las directrices de gobierno y regulaciones del país ayudan, pero al igual como cada empresa debe velar por su éxito en el mercado, debe velar también por no poner en juego el éxito de su empresa debido a amenazas cibernéticas.

Seguir la guía de los países desarrollados es el mejor norte de cómo enfrentar esta problemática, estos países son robustos en su contexto legal, en su entorno regulatorio, eso da un marco para que las empresas de manera independiente sigan estas directrices y es en esa línea donde nace la importancia de tener un modelo estratégico y operacional de cómo abordar la seguridad digital, se hace necesario un modelo que contemple ambas perspectivas, por sobre todo la perspectiva estratégica, durante mucho tiempo la seguridad digital era problema de las áreas de tecnología de las empresas, hoy en día, con la digitalización, con este cambio cultural y generacional, es impensable no tratar este tema a nivel estratégico, nivel donde se toman las decisiones, el modelo planteado en esta investigación cumple con esa necesidad y entrega las herramientas necesarias para poder cubrir estas dos perspectivas muy necesarias en este mundo digital, la cuarta revolución industrial.

Bibliografía

Advisera. (18 de junio de 2018). *27001 Academy*. Obtenido de 27001 Academy: https://advisera.com/27001academy/es/que-es-iso-27001/

AIG. (7 de mayo de 2018). *New Cyber Trends: U.S. & Latin America*. Obtenido de New Cyber Trends: U.S. & Latin America: https://www.aig.com/knowledge-and-insights/k-and-i-article-state-of-cybersecurity-us-latin-america

Banco Interamericano de Desarrollo & Organization of American States. (2016). *Observatorio de la CiberSeguridad en America Latina y el Caribe.* USA: Creative Commons IGO.

BID & Organización de los Estados Americanos. (07 de mayo de 2018). *Obeservatorio de la CiberSeguridad en America Latina y el Caribe*. Obtenido de Obeservatorio de la CiberSeguridad en America Latina y el Caribe: http://observatoriociberseguridad.org/graph/countries/cl/selected/cl/0/dimensions/1-2-3-4-5

BlackHat USA . (2017). *Portrait of an Inmminent Cyberthreat.* USA: Blackhat.

BSI GROUP. (18 de junio de 2018). *Sistema de gestión ISO/IEC 27001 de Seguridad de la Información*. Obtenido de Sistema de gestión ISO/IEC 27001 de Seguridad de la Información: https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

CISCO. (2018). *Annual CyberSecurity Report.* California: CISCO.

CNN Español. (15 de abril de 2018). *Sitio web CNN en español*. Obtenido de Sitio web CNN: http://cnnespanol.cnn.com/2018/04/10/mark-zuckerberg-en-el-congreso-el-momento-de-madurar-del-ceo-de-facebook/

Comité Interministerial sobre CiberSeguridad. (07 de mayo de 2018). *Ministerio del Interior y Seguridad Pública*. Obtenido de Ministerio del Interior y Seguridad Pública: http://ciberseguridad.interior.gob.cl/noticias/ciberseguridad-vision-de-estado/

Congress GOV USA. (27 de abril de 2018). *CYBERSECURITY INFORMATION SHARING ACT OF 2015*. Obtenido de CYBERSECURITY INFORMATION SHARING ACT OF 2015: https://www.congress.gov/congressional-report/114th-congress/senate-report/32/1

Cooperativa. (18 de junio de 2018). *Cooperativa Noticias*. Obtenido de Cooperativa Noticias: https://www.cooperativa.cl/noticias/pais/consumidores/banco-de-chile-mando-carta-a-sus-clientes-explicando-el-hackeo/2018-06-12/181814.html

Dávila, A. L. (Febrero de 2008). *Gestioópolis.com*. Obtenido de https://www.gestiopolis.com/sistemas-mrp-materials-requirement-planning/

Derechos Digitales & Global Partners Digital. (2017). *HACIA UN NUEVO MARCO NORMATIVO EN CHILE.* Santiago: Vladimir Garay y Patricio Velasco.

EALDE BUSINESS SCHOOL. (10 de julio de 2018). *GESTIÓN DE RIESGOS*. Obtenido de GESTIÓN DE RIESGOS: https://www.ealde.es/mapa-de-riesgos/

Ernst & Young. (2017). *Wannacry Ransomware Attack.* UK: EYGM Limited.

EXEVI. (10 de julio de 2018). *¿Cómo Gestionas el Cambio?* Obtenido de ¿Cómo Gestionas el Cambio?: https://www.exevi.com/como-gestionas-el-cambio/

FORRESTER. (2017). *Accelerating Digital Transformation with Technology.* USA: Forrester Research.

Fundación Telefonica. (2015). *La transformacion digital digital y movil de la comunicacion politica.* España: Ariel S.A.

Gestion Calidad. (10 de julio de 2018). *ISO 31000 (Gestión de Riesgos)*. Obtenido de ISO 31000 (Gestión de Riesgos): http://gestion-calidad.com/iso-31000-gestion-de-riesgos

Global Security Map. (7 de Mayo de 2018). *Global Security Map (Chile)*. Obtenido de Global Security Map (Chile): http://globalsecuritymap.com/#details/cl

Gobierno de Chile. (2017 - 2022). *Política Nacional de CiberSeguridad.* Santiago: Commons Atribución-CompartirIgual 4.0 Internacional.

IDC. (2017). *IDC FutureScape: Worldwide IT Industry 2018 Predictions.* USA: IDC Research.

IDC Chile. (07 de mayo de 2017). *IDC Predictions Chile 2017*. Obtenido de IDC Predictions Chile 2017: http://cl.idclatin.com/releases/news.aspx?id=2140

IDG. (2018). *State of Digital Business Transformation.* USA: IDG Communicatios, Inc.

INCIBE. (10 de julio de 2018). *Kit de concienciación*. Obtenido de Kit de concienciación: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

INFOBAE. (10 de julio de 2018). *Cayeron las acciones de Facebook por el escándalo de la filtración de datos durante la campaña electoral en EEUU*. Obtenido de Cayeron las acciones de Facebook por el escándalo de la filtración de datos durante la campaña electoral en EEUU: https://www.infobae.com/america/eeuu/2018/03/19/caen-las-acciones-de-facebook-por-el-escandalo-de-la-filtracion-de-datos-durante-la-campana-electoral-en-eeuu/

ISACA. (2017). *Digital Transformation Barometer.* USA: ISACA.

ISO 27001 Security. (19 de junio de 2018). *ISO/IEC 27002:2013*. Obtenido de ISO/IEC 27002:2013: http://www.iso27001security.com/html/27002.html#Section9

ISO 27002 ES. (19 de junio de 2018). *ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES*. Obtenido de ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

ISO ORG. (19 de junio de 2018). *ISO/IEC 27001:2013(en)*. Obtenido de ISO/IEC 27001:2013(en): https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO ORG. (19 de junio de 2018). *ISO/IEC 27002:2013(en)*. Obtenido de ISO/IEC 27002:2013(en): https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

ISO TOOLS ORG. (10 de julio de 2018). *La norma en Gestión de Riesgos ISO 31000 y sus beneficios*. Obtenido de La norma en Gestión de Riesgos ISO 31000 y sus beneficios: https://www.isotools.org/2017/10/15/gestion-de-riesgos-iso-31000-y-sus-beneficios/

IT Governance. (18 de junio de 2018). *The benefits of implementing an information security management system (ISMS)*. Obtenido de The benefits of implementing an information security management system (ISMS): https://www.itgovernance.co.uk/isms-benefits

IT GOVERNANCE. (22 de junio de 2018). *Top 4 cybersecurity frameworks*. Obtenido de Top 4 cybersecurity frameworks: https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks/

Kaspersky Lab. (8 de mayo de 2018). *Kaspersky Lab: 51% del malware detectado en Chile en Q1 de 2017 provino de software pirata*. Obtenido de Kaspersky Lab: 51% del malware detectado en Chile en Q1 de 2017 provino de software pirata: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-51-del-malware-detectado-en-chile-en-q1-de-2017-provino-de-software-pirata

KPMG. (10 de julio de 2018). *Gestión del Cambio*. Obtenido de Gestión del Cambio: https://home.kpmg.com/co/es/home/services/advisory/management-consulting/capitalhumano-y-gestion-del-cambio/gestion-del-cambio.html

Ministerio Economía Chile. (07 de Mayo de 2018). *Ministerio de Economía, Fomento y Turismo*. Obtenido de Ministerio de Economía, Fomento y Turismo: http://www.economia.gob.cl/2018/01/24/ministro-rodriguez-el-crecimiento-economico-depende-que-enfrentemos-la-transformacion-digital-en-conjunto-con-nuestras-empresas.htm

NACD Director's Handbook on Cyber-Risk Oversight. (27 de abril de 2018). *NACD.* Obtenido de National Association of Corporate Directors: https://www.nacdonline.org/cyber

NIST. (18 de Junio de 2018). *CYBERSECURITY FRAMEWORK*. Obtenido de CYBERSECURITY FRAMEWORK: https://www.nist.gov/cyberframework

NIST GOV. (18 de junio de 2018). *NIST*. Obtenido de National Institute of Standards and Technology: https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework

OEA. (2018). *Estado de la Ciberseguridad en el Sector Bancario en America Latina y el Caribe.* Canada: OEA (Organizacion de los Estados Americanos).

Office of the Director National Intelligence. (2018, abril 27). *Office of the Director National Intelligence*. Retrieved from Global Trends Main Report: https://www.dni.gov/index.php/global-trends/letter-nic-chairman

P.Norton, R. S. (2004). *Mapas Estratégicos.* Barcelona: Gestion 2000: Edicion Lengua Castellana.

PEW Research Center. (27 de abril de 2017). *Global Attitudes & Treds*. Obtenido de Global Attitudes & Treds: http://www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/

PMG SSI. (10 de julio de 2018). *ISO 27001 – Aspectos importantes en concienciación en Seguridad de la Información*. Obtenido de ISO 27001 – Aspectos importantes en concienciación en Seguridad de la Información: https://www.pmg-ssi.com/2014/06/iso-27001-concienciacion-seguridad-informacion/

PWC. (27 de abril de 2018). *Bold steps to manage geopolitical cyber threats*. Obtenido de Bold steps to manage geopolitical cyber threats: https://www.pwc.com/gx/en/issues/information-security-survey/geopolitical-cyber-threats.html

PWC. (2018). *Key findings from The Global State of Information Security® Survey 2018.* USA: PWC GSSIS.

Revista Trend TIC. (07 de mayo de 2018). *Revista Trend TIC*. Obtenido de Revista Trend TIC: http://www.trendtic.cl/2018/01/presidente-de-la-sofofa-la-transformacion-digital-es-una-oportunidad-tanto-para-el-sector-publico-como-privado/

SAP. (2017). *Viviendo la transformacion Digital (Estudio).* America Latina: Propia.

SPC Consulting Group. (10 de julio de 2018). *ISO 31000:2018 – Proceso para la gestión de riesgos*. Obtenido de ISO 31000:2018 – Proceso para la gestión de riesgos: https://spcgroup.com.mx/iso310002018-proceso-para-la-gestion-de-riesgos/

Subsecreatria de Defensa de Chile. (07 de mayo de 2018). *Una Política Nacional de CiberSeguridad para Chile*. Obtenido de Una Política Nacional de CiberSeguridad para Chile: http://www.ssdefensa.cl/n5427_27-04-2017.html

Symantec Corporation. (2018). *Internet Security Threat Report.* California: Symantec Corporation.

Tenable. (18 de Junio de 2018). *Survey Report: Trends in Security Framework Adoption*. Obtenido de Survey Report: Trends in Security Framework Adoption: https://www.tenable.com/whitepapers/trends-in-security-framework-adoption

Tenable Network Security. (2016). *TRENDS IN SECURITY FRAMEWORK ADOPTION.* USA: Dimensional Researh.

TODDLE. (19 de junio de 2018). *WP Content 2014*. Obtenido de http://toddleoutsourcing.es/wp-content/uploads/2014/04/sgsi_pdca.jpg: http://toddleoutsourcing.es/wp-content/uploads/2014/04/sgsi_pdca.jpg

TREND Micro. (2013). *Latin American and Caribbean Cybersecurity Trends and Government Responses.* Cupertino: TREND MICRO INCORPORATED.

Trend TIC. (07 de mayo de 2018). *78% DE BANCOS CONFÍA EN SU ESTRATEGIA DE CIBERSEGURIDAD, A PESAR DE SUFRIR ENTRE DOS Y TRES ATAQUES AL MES*. Obtenido de 78% DE BANCOS CONFÍA EN SU ESTRATEGIA DE CIBERSEGURIDAD, A PESAR DE SUFRIR

ENTRE DOS Y TRES ATAQUES AL MES: http://www.trendtic.cl/2017/05/78-de-bancos-confia-en-su-estrategia-de-ciberseguridad-a-pesar-de-sufrir-entre-dos-y-tres-ataques-al-mes/

Trend TIC. (07 de mayo de 2018). *CHILE: 75% DE LAS EMPRESAS ESTÁN EN VÍAS DE UNA TRANSFORMACIÓN DIGITAL*. Obtenido de CHILE: 75% DE LAS EMPRESAS ESTÁN EN VÍAS DE UNA TRANSFORMACIÓN DIGITAL: http://www.trendtic.cl/2017/09/chile-75-de-las-empresas-estan-en-vias-de-una-transformacion-digital/

Trend TIC. (7 de mayo de 2018). *EDGAR PÉREZ: "LA CIBERSEGURIDAD NO ES SOLAMENTE UN TEMA TECNOLÓGICO, SINO QUE ES UN CONJUNTO DE ESFUERZOS"*. Obtenido de EDGAR PÉREZ: "LA CIBERSEGURIDAD NO ES SOLAMENTE UN TEMA TECNOLÓGICO, SINO QUE ES UN CONJUNTO DE ESFUERZOS": http://www.trendtic.cl/2017/08/edgar-perez-la-ciberseguridad-no-es-solamente-un-tema-tecnologico-sino-que-es-un-conjunto-de-esfuerzos/

Worl Economic Forum. (27 de abril de 2018). *Shareable Infographics*. Obtenido de Shareable Infographics: http://reports.weforum.org/global-risks-2017/shareable-infographics/

World Economic Forum. (2017). *The Global Risk Report.* Suiza: World Economic Forum.

Yahoo Finance. (20 de abril de 2018). *Pagina de yahoo Financiero*. Obtenido de Sitio web Yahoo Finance: https://finance.yahoo.com/quote/FB?p=FB

Anexos

Anexo N° 1 - Amenazas y Vulnerabilidades 2017 en grandes números a nivel mundial

Amenazas WEB (Sitios web)

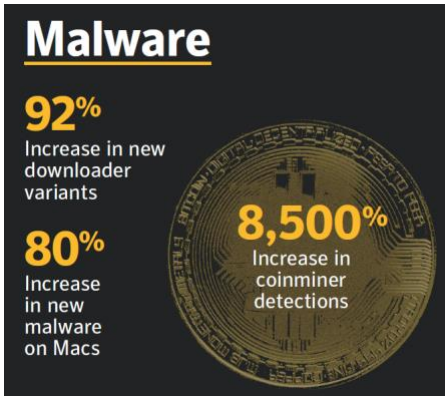
Figura N° 32: Web Threats

Fuente: (Symantec Corporation, 2018)

Según la figura N°5 más de 1 billón de requerimientos web analizados.

Malware (ataques de virus, gusanos, troyanos, etc.)

Figura N° 33: Malware

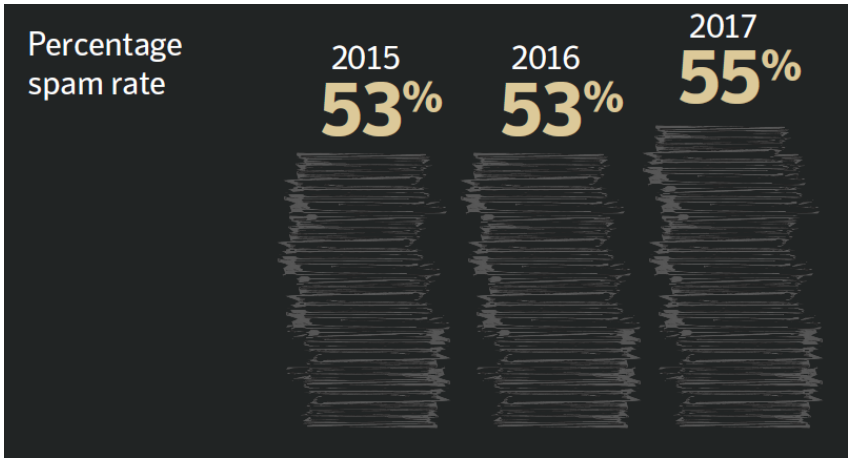


Fuente: (Symantec Corporation, 2018)

Un aumento del 92% en amenazas descargables, 80% de aumento de amenazas para MAC y 8500% de detecciones de minería de bitcoins.(figura N° 6)

Amenazas por Email (Principalmente SPAM)

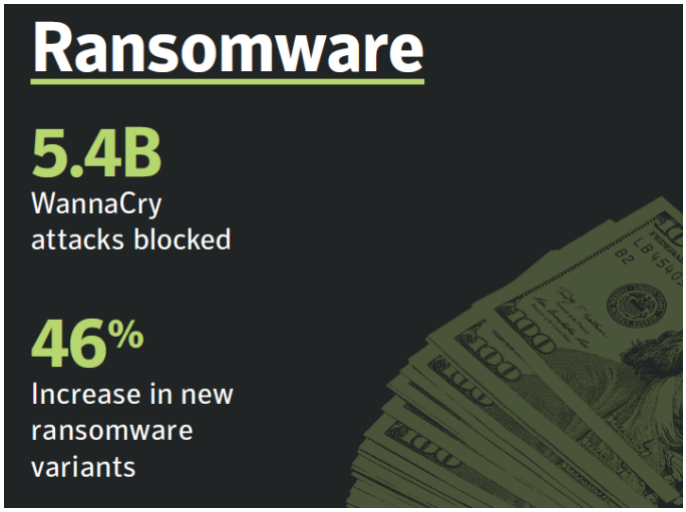
Figura N° 34: Tasa aumento en porcentaje de SPAM anuales



Fuente: (Symantec Corporation, 2018)

Ransomware (Malware que encripta computadores pidiendo un rescate)

Figura N° 35: Ataques de Ransomware

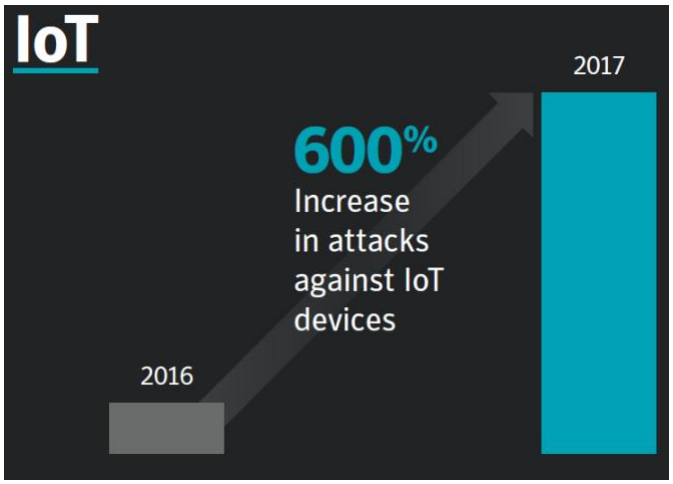


Fuente: (Symantec Corporation, 2018)

5.4 Billones de ataques se ransomware bloqueados y un 46% de incremente de amenazas de este tipo (Figura N° 8)

Internet de las cosas

Figura N° 36: Internet de las cosas

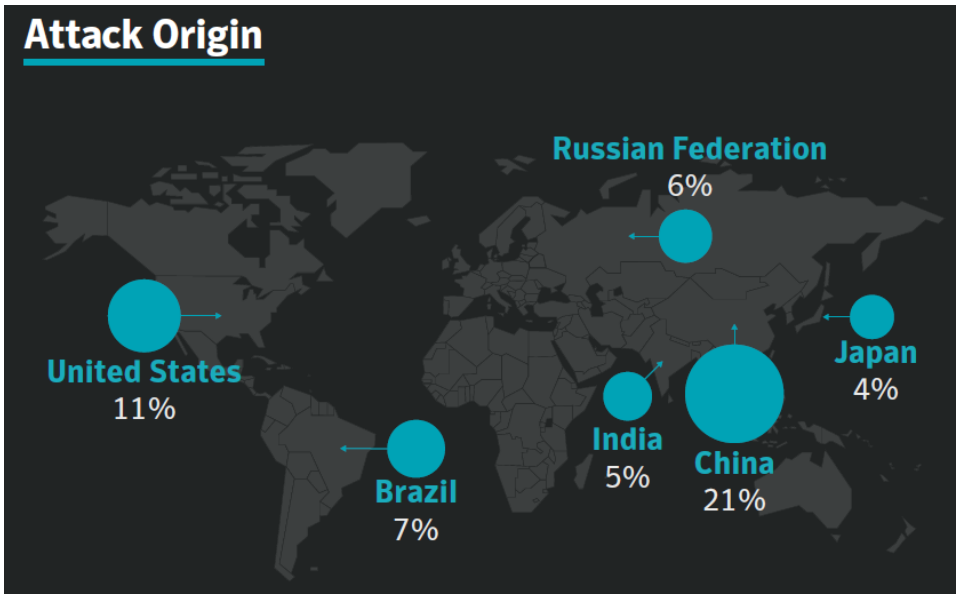


Fuente: (Symantec Corporation, 2018)

Un considerable aumento del 600% de ataques de IOT.

Orígenes de los ataques a nivel mundial

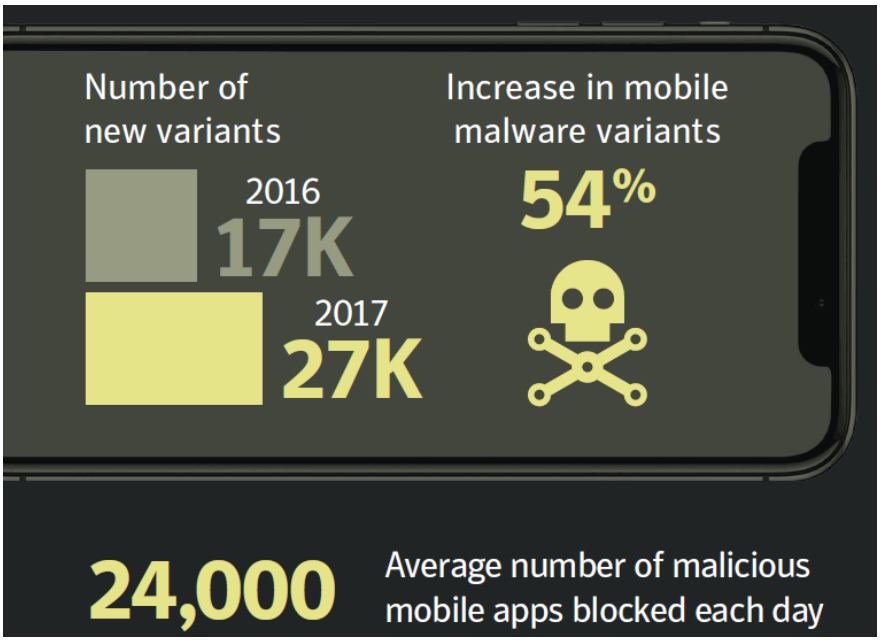
Figura N° 37: Porcentaje de incremente de los orígenes de los ataques a nivel mundial



Fuente: (Symantec Corporation, 2018)

Mobile

Figura N° 38: Incremento de ataques a plataformas mobile



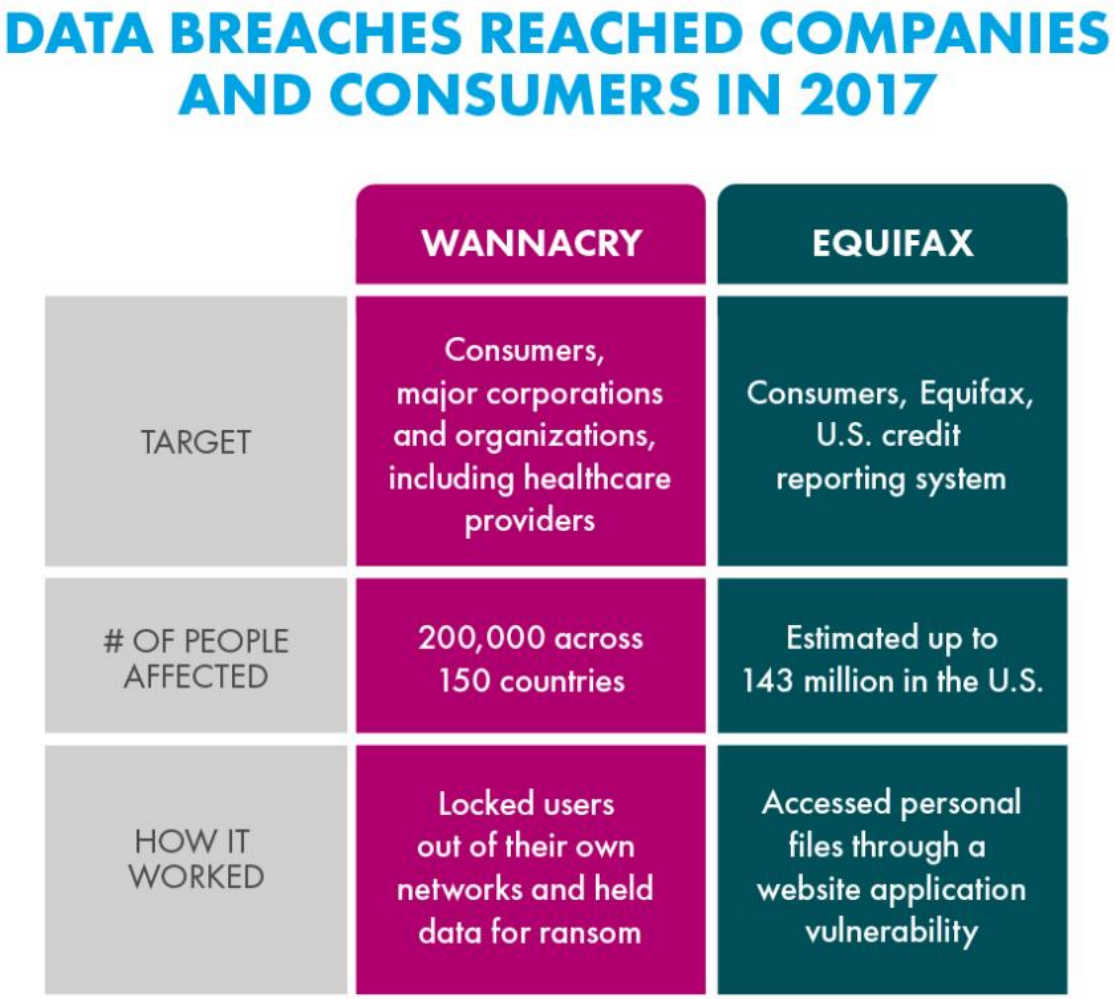
Fuente: (Symantec Corporation, 2018)

Vulnerabilidades

Figura N° 39: Incremento de Vulnerabilidades a nivel mundial en 2017

Fuente: (Symantec Corporation, 2018)

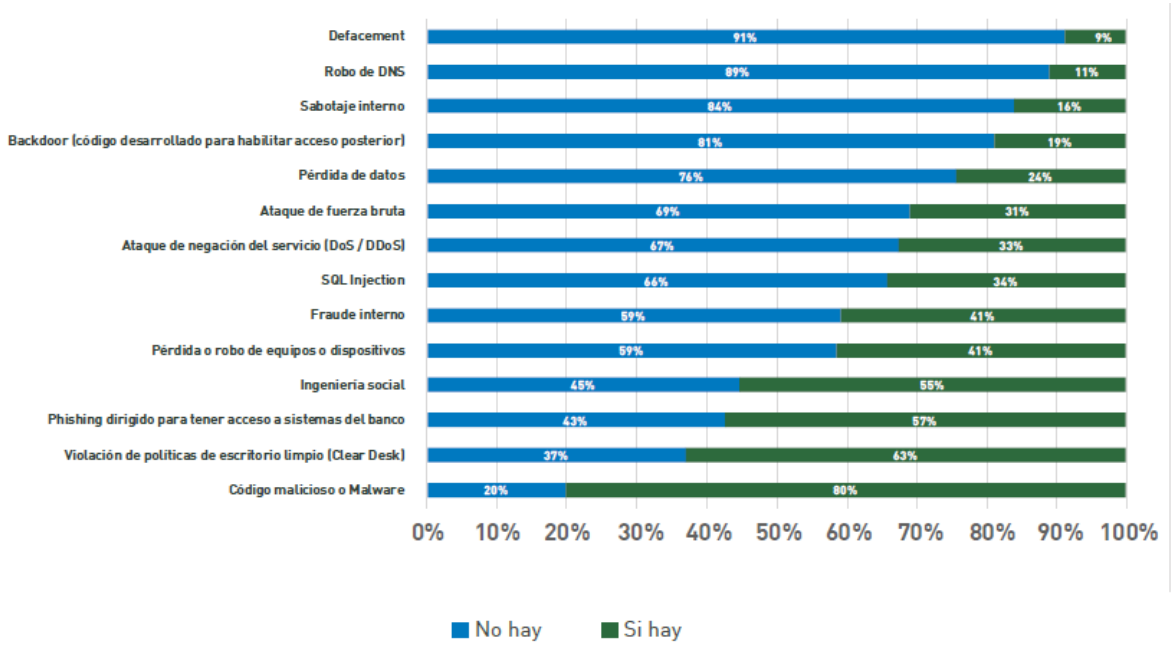
Figura N° 40: Violaciones de Datos 2017



Fuente: (AIG, 2018)

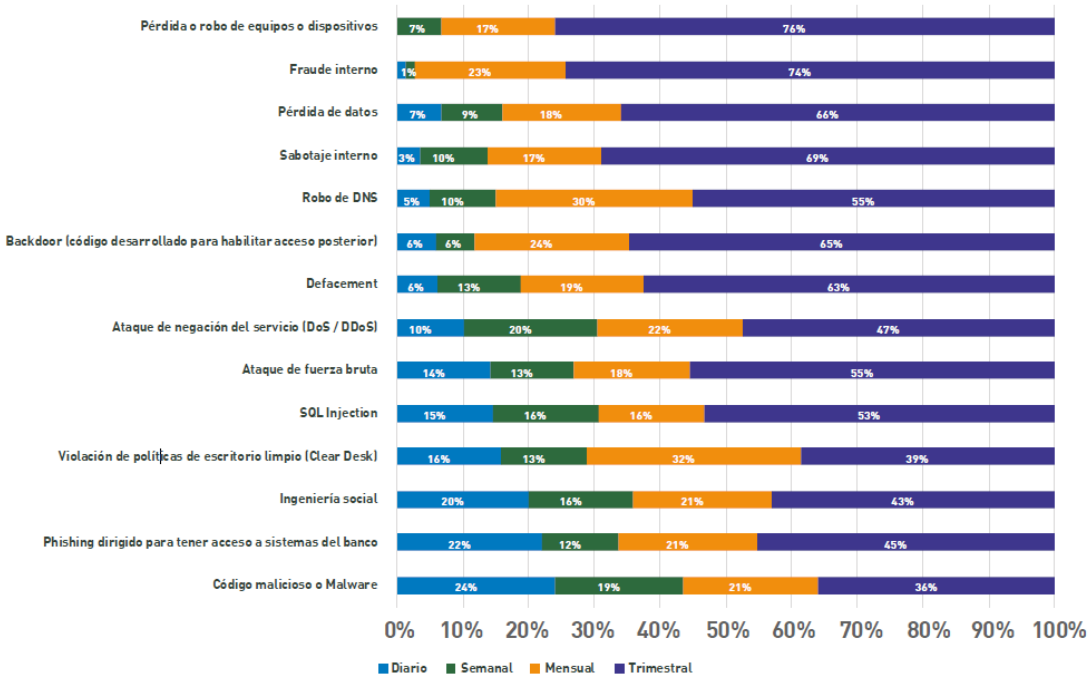
Anexo N° 2 – Eventos de Seguridad digital contra entidades bancarias que se han registrado en el periodo 2017 y su frecuencia (Industria Financiera)

Figura N° 41: Eventos de seguridad digital periodo 2017 en Latinoamérica.



Fuente: (OEA, 2018)

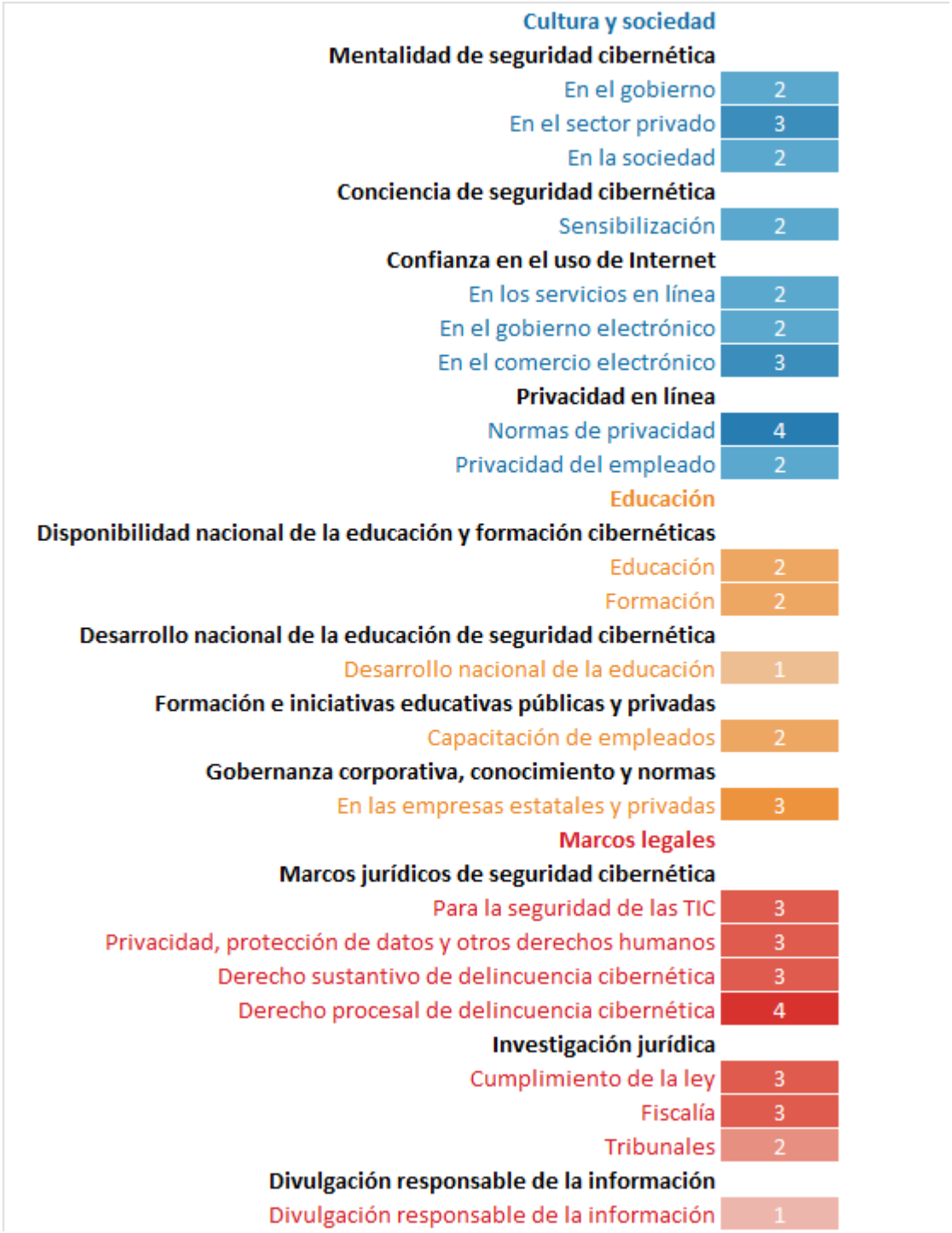
Figura N° 42: Frecuencia en la ocurrencia de eventos de seguridad digital contra las entidades financieras.



Fuente: (OEA, 2018)

Anexo N° 3 – Grado de Madurez de la Seguridad Digital de Chile

Figura N° 43: Madurez de Seguridad Digital de Chile

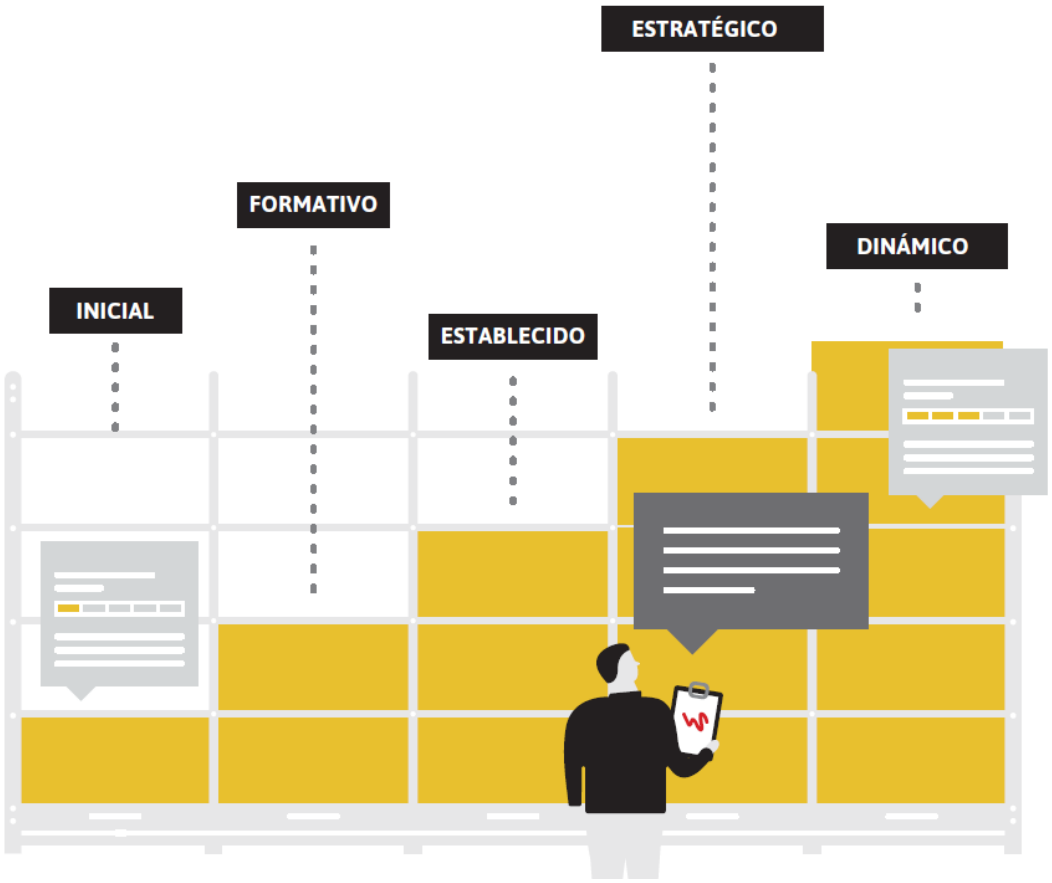


Fuente: (BID & Organización de los Estados Americanos, 2018)

Figura N° 44: Madurez de Seguridad Digital de Chile

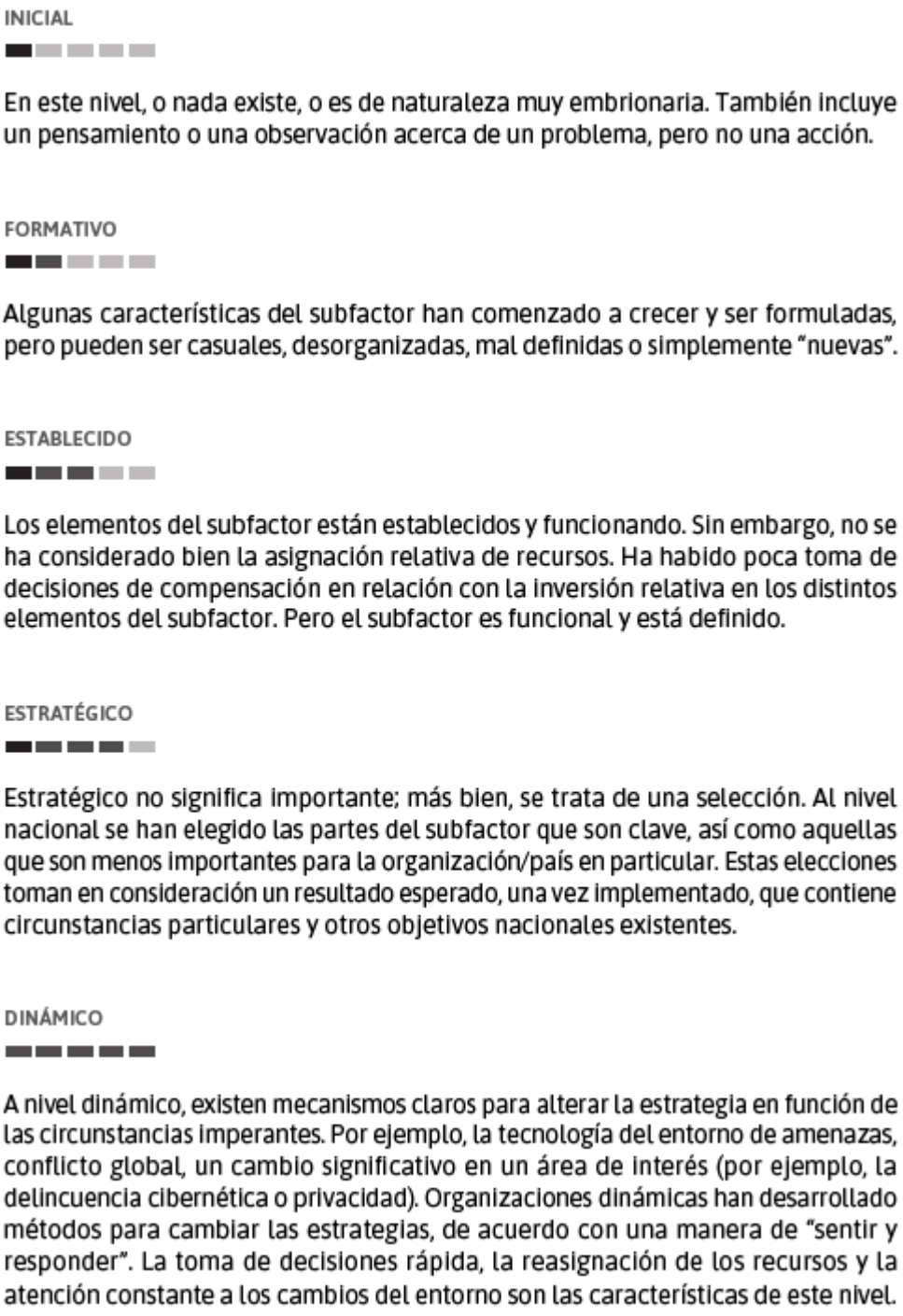
Fuente: (BID & Organización de los Estados Americanos, 2018)

Figura N° 45: Niveles de Madurez Figura N°20



Fuente: (BID & Organización de los Estados Americanos, 2018)

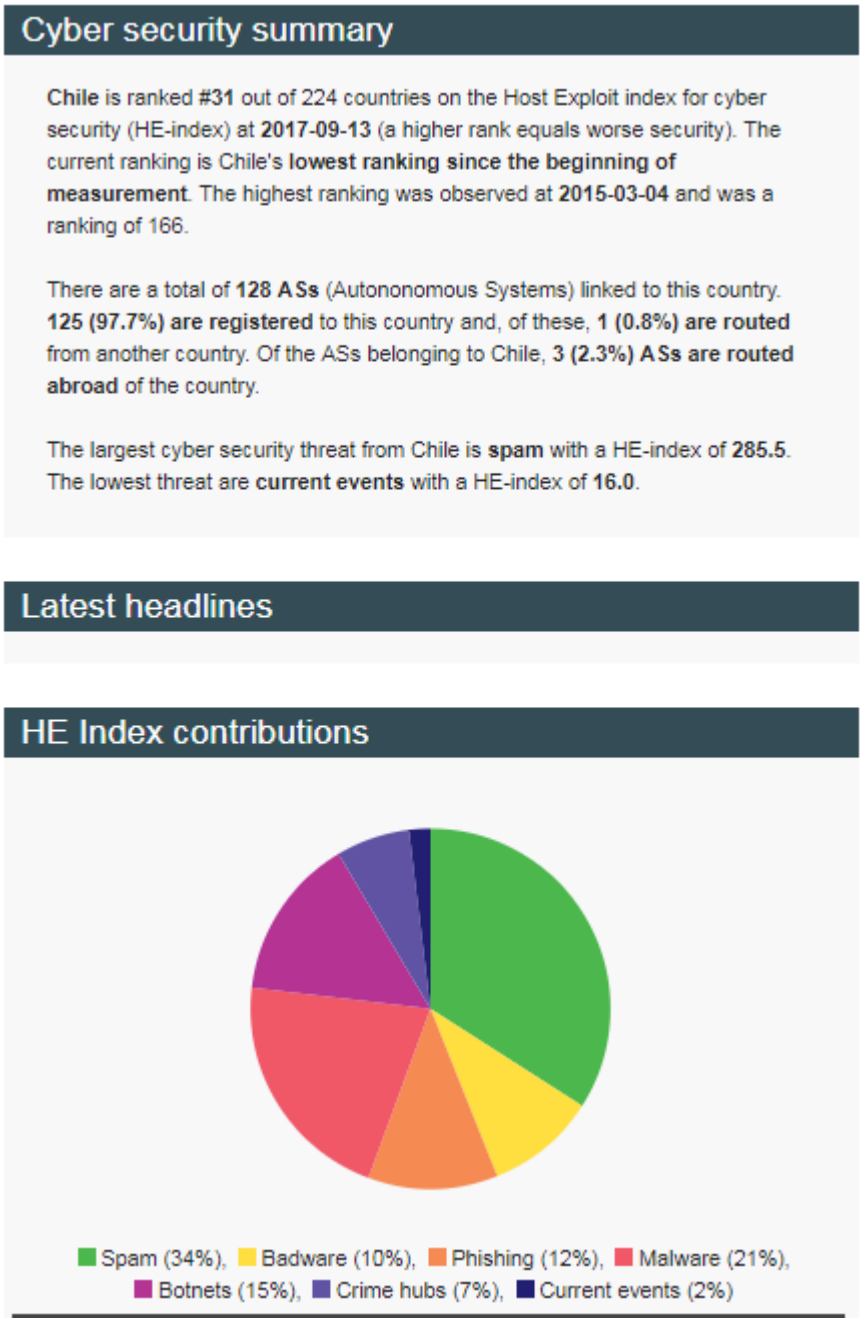
Figura N° 46: Descripción Niveles de Madurez Figura N°21



Fuente: (BID & Organización de los Estados Americanos, 2018)

Anexo N° 4 – Amenazas en Chile

Figura N° 47: Catalogación de Chile índice HE (host exploit)



Fuente: (Global Security Map, 2018)

Figura N° 48: Patrones de ataques de Seguridad Digital en Chile 2015

Cantidad de Registros	Descripción
58.375.435	Intentos de acceder a información de dispositivos de red mediante protocolo de administración SNMP
45.903.511	Escaneo de puertos de administración de dispositivos de la plataforma switch, router o seguridad.
19.745.086	Flujo web con traspaso de contraseñas en texto claro (sin cifrar)
7.805.544	Detección de actualizaciones dinámicas de DNS
5.570.661	Detección de flujo TFTP (transferencia de archivos) usando protocolo tftp
4.463.394	Detección de flujos portmap
3.359.194	Detección de trafico anómalo por el puerto de los DNS
2.479.277	Detección de flujos de escritorio remoto
2.077.435	Detección de consultas DNS por dominios reconocidos como de uso de malware
2.023.403	Detección de reconocimiento por PING
1.451.708	Escaneo de puertos de administración de dispositivos de la plataforma switch, router o seguridad.
1.428.461	Detección de acceso a wordpress (componentes claves)
1.400.697	Detección de malware MORTO
1.120.311	Detección de tráfico NO cifrado a través de puerto tradicionalmente utilizado para transmitir cifradamente (443)
1.106.303	Detección de acceso a zonas prohibidas de sitios web
1.025.252	Flujo de credenciales en texto claro de login wordpress (utilizando en sitios web de gobierno)

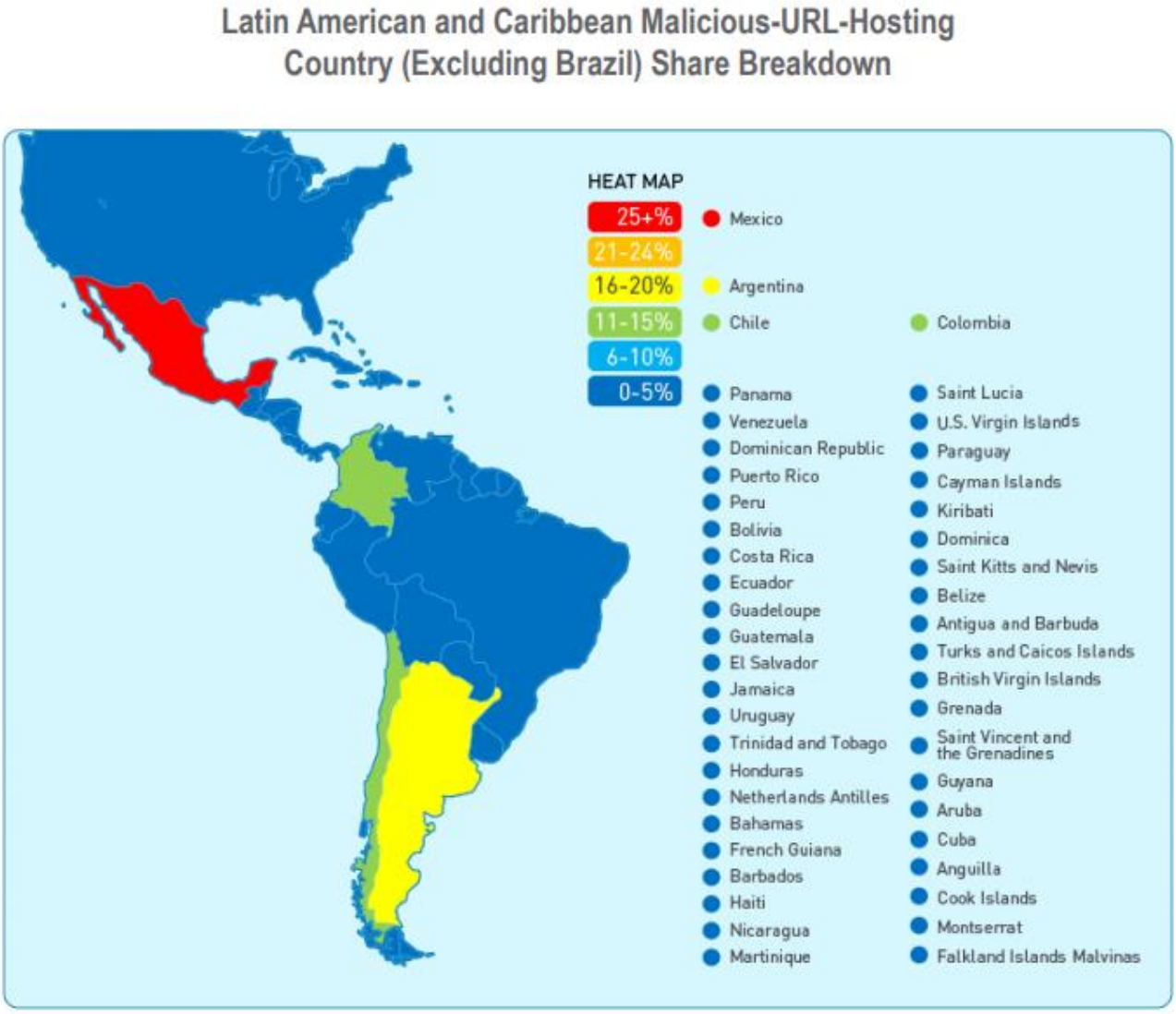
Patrones detectados en la Red de Conectividad del Estado (RCE) durante el período 2015
(Fuente: División Informática del Ministerio del Interior, año 2016)

Fuente: (Gobierno de Chile, 2017 - 2022)

Figura N° 49: Correo basura

Fuente: (TREND Micro, 2013)

Figura N° 50: URL Maliciosas



Fuente: (TREND Micro, 2013)

Figura N° 51: Hackeo Banco de Chile año 2018

El sábado, el Banco de Chile reconoció el ataque informático que afectó a la entidad en mayo pasado tenía como fin generar distracción y así poder sustraer 10 millones de dólares.

Ese dinero lo perdió la institución, **no sus clientes**, según detalló el gerente general de la entidad ligada al Grupo Luksic y Citibank, **Eduardo Ebensperger**.

Este martes, el banco le envió un mail a sus clientes del Banco de Chile y Edwards, explicando lo que pasó, con lujo de detalles.

Esta es la carta completa:

"En nuestro permanente interés por mantener informados a nuestros clientes, nos referimos al incidente de seguridad tecnológica que afectó a Banco de Chile y a las medidas adoptadas para resolverlo.

El día jueves 24 de mayo pasado **se detectó que terceros, delincuentes internacionales altamente sofisticados, a través de acciones ilícitas** sustrajeron desde cuentas propias de Banco de Chile en bancos corresponsales del exterior, una cifra aproximada **a US$10 millones**, dinero que corresponde a fondos del Banco y no de sus clientes. Respecto de dicha suma, el Banco inició las gestiones tendientes a obtener su recuperación.

Para facilitar la perpetración del delito, y para dificultar su detección, este grupo delictual introdujo un virus (**Malware Swapq**) que afectó algunos sistemas del Banco, impidiendo su normal funcionamiento.

Ante esta situación **se activaron nuestros protocolos de seguridad y el plan de contingencia, lo que permitió controlar el incidente**, continuar con la operación del Banco y asegurar la integridad de los datos e información, de manera que no se vieran perjudicadas las transacciones, registros, fondos y productos de nuestros clientes.

Lo anterior afectó principalmente la calidad de servicio en sucursales y banca telefónica, considerando especialmente que dentro de las medidas adoptadas se incluyó la desconexión de la mayoría de los terminales computacionales, quedando plenamente restablecidos nuestros servicios a comienzo de la semana siguiente.

Lamentamos profundamente los inconvenientes que generó esta situación que s**e reflejó en la lentitud operativa de nuestras sucursales (pagos de cheques y/o Vale Vistas, efectuar cambio de claves presenciales entre otros)**.

Sin embargo, estamos convencidos que **nuestra reacción permitió preservar la seguridad de sus datos, fondos y productos**".

Fuente: (Cooperativa, 2018)

Anexo N° 5 – Categorías y Subcategorías NIST

Figura N° 52: Núcleo del NIST, Categorías, Subcategorías y referencias de otros modelos.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Function	Category	Subcategory	Informative References
		third-party stakeholders (e.g., suppliers, customers, partners) are established	**ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families

Function	Category	Subcategory	Informative References
	management of cybersecurity risk.	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16

Function	Category	Subcategory	Informative References
		ID.RA-3: Threats, both internal and external, are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** PM-9

Function	Category	Subcategory	Informative References
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

Function	Category	Subcategory	Informative References
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

Function	Category	Subcategory	Informative References
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

Function	Category	Subcategory	Informative References
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

Function	Category	Subcategory	Informative References
		PR.IP-7: Protection processes are improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

Function	Category	Subcategory	Informative References
		PR.IP-12: A vulnerability management plan is developed and implemented	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected	**DE.AE-1:** A baseline of network operations and expected data flows for	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

Function	Category	Subcategory	Informative References
	and the potential impact of events is understood.	users and systems is established and managed	**ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Function	Category	Subcategory	Informative References
	the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Unauthorized mobile code is detected	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	**CIS CSC** 4, 20

Function	Category	Subcategory	Informative References
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15

Function	Category	Subcategory	Informative References
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Function	Category	Subcategory	Informative References
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

Fuente: (NIST, 2018)

Anexo N° 6 – ISO 27002:2013 Objetivos de control y controles

Figura N° 53: Estructura ISO 27001:2013

Section 5: Information security policies

5.1 Management direction for information security

Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall "information security policy" as specified in ISO/IEC 27001 section 5.2.

Section 6: Organization of information security

6.1 Internal organization

The organization should lay out the roles and responsibilities for information security, and allocate them to individuals. Where relevant, duties should be segregated across roles and individuals to avoid conflicts of interest and prevent inappropriate activities. There should be contacts with relevant external authorities (such as CERTs and special interest groups) on information security matters. Information security should be an integral part of the management of all types of project.

6.2 Mobile devices and teleworking

There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other Boys' Toys) and teleworking (such as telecommuting, working-from home, road-warriors, and remote/virtual workplaces). [I don't know how this ended up under section 6, but here it is.]

Section 7: Human resource security

7.1 Prior to employment

Information security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (*e.g.* through adequate job descriptions, pre-employment screening) and included in contracts (*e.g.* terms and conditions of employment and other signed agreements defining security roles and responsibilities, compliance obligations *etc.*).

7.2 During employment

Managers should ensure that employees and contractors are made aware of and motivated to comply with their information security obligations. A formal disciplinary process is necessary to handle information security incidents allegedly caused by workers.

7.3 Termination and change of employment

Security aspects of a person's departure from the organization, or significant changes of roles within it, should be managed, such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy and intellectual property laws, contractual terms *etc.* plus ethical expectations.

Section 8: Asset management

8.1 Responsibility for assets

All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization.

8.2 Information classification

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

8.3 Media handling

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Section 9: Access control

9.1 Business requirements of access control

The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted.

9.2 User access management

The allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (now called "secret authentication information") plus regular reviews and updates of access rights.

9.3 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls *e.g.* choosing strong passwords and keeping them confidential.

9.4 System and application access control

Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities and restricted access to program source code.

Section 10: Cryptography

10.1 Cryptographic controls

There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

Section 11: Physical and environmental security

11.1 Secure areas

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas *etc.* against unauthorized access. Specialist advice should be sought regarding protection against fires, floods, earthquakes, bombs *etc.*

11.2 Equipment

"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and air conditioning) and cabling should be secured and maintained. Equipment and information should not be taken off-site unless authorized, and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

Section 12: Operations security

12.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

12.2 Protection from malware

Malware controls are required, including user awareness.

12.3 Backup

Appropriate backups should be taken and retained in accordance with a backup policy.

12.4 Logging and monitoring

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

12.5 Control of operational software

Software installation on operational systems should be controlled.

12.6 Technical vulnerability management

Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

12.7 Information systems audit considerations

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

13 Communications security

13.1 Network security management

Networks and network services should be secured, for example by segregation.

13.2 Information transfer

There should be policies, procedures and agreements (*e.g.* non-disclosure agreements) concerning information transfer to/from third parties, including electronic messaging.

Section 14: System acquisition, development and maintenance

14.1 Security requirements of information systems

Security control requirements should be analyzed and specified, including web applications and transactions.

14.2 Security in development and support processes

Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled. Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled. System security should be tested and acceptance criteria defined to include security aspects.

Note: there is a typo in 14.2.8: the reference to section 14.1.9 should read 14.2.9. See the status update below, or technical corrigendum 2 for the official correction.

14.3 Test data

Test data should be carefully selected/generated and controlled.

15: Supplier relationships

15.1 Information security in supplier relationships

There should be policies, procedures, awareness *etc.* to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

15.2 Supplier service delivery management

Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled. [Exactly the same point applies to services delivered by internal suppliers, by the way!]

Section 16: Information security incident management

16.1 Management of information security incidents and improvements

There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.

Section 17: Information security aspects of business continuity management

17.1 Information security continuity

The continuity of information security should be planned, implemented and reviewed as an integral part of the organization's business continuity management systems.

17.2 Redundancies

IT facilities should have sufficient redundancy to satisfy availability requirements.

Section 18: Compliance

18.1 Compliance with legal and contractual requirements

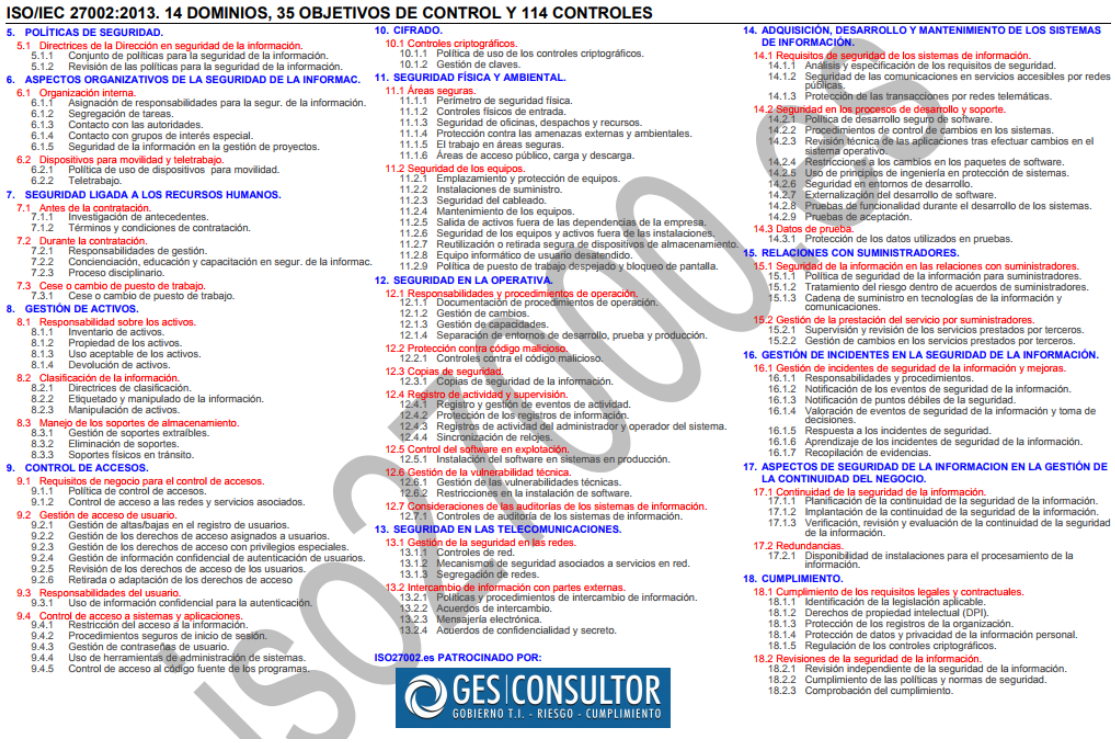
The organization must identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, [business] records, privacy/personally identifiable information and cryptography.

18.2 Information security reviews

The organization's information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employees' and systems' compliance with security policies, procedures *etc.* and initiate corrective actions where necessary.

Fuente: (ISO 27001 Security, 2018)

Figura N° 54: Estructura ISO 27001:2013 (español)



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:
GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

ISO27002

Fuente: (ISO 27002 ES, 2018)