Hacia un framework para la

Ciberseguridad

en la banca

creasys

Índice

Ir al Índice

Introducción

En la *era de la información* (Castells (2008 [1996]), las telecomunicaciones, los computadores y las redes, son determinantes para la forma en que se realizan los intercambios sociales y económicos, la manera en que se crea y obtiene conocimiento, el carácter del trabajo y la organización de la sociedad. Aquello que caracteriza a nuestra época es la *aplicación del conocimiento y la información sobre aparatos y procesos de generación de conocimiento y procesamiento de la información/comunicación*. Recursividad que fomenta la retroalimentación acumulativa permanente entre innovación, usos y desarrollo de nuevos campos, cuestión que asegura una expansión exponencial constante, en un contexto globalizado de descentralización de la producción facilitada por redes de información que liberan a las empresas y a las personas de las restricciones territoriales.

Hoy en día, la tecnología que permite, facilita y optimiza la generación de conocimiento es la principal fuente de productividad de las compañías. Esta potencia la gestión de información y la comunicación de símbolos, aplicándolos para mejorar permanentemente la generación de conocimiento y optimizar el procesamiento de información. Este nuevo paradigma productivo está basado en el desarrollo de tecnología de la información, cuyo principio estructurante es la acumulación de datos, información y conocimiento, el procesamiento y su aplicación en la búsqueda de mejorar los procesos y la productividad.

De hecho, según la CEPAL (2018: 27), la digitalización de la economía está impactando en la forma de producir y comercializar de bienes y servicios y en los modelos de negocio a nivel global, exigiendo el desarrollo de nuevas habilidades para desenvolverse con éxito en el nuevo entorno digitalizado. Cada vez más, los procesos productivos están incorporando tecnologías avanzadas y digitales en prácticamente todas las actividades, automatizando los procesos y la ejecución de diversas tareas.

En este contexto, el sector financiero en general y los bancos en particular están atravesando un proceso de modernización basado en la informatización y digitalización del negocio. De hecho, el Digital Banking Report 2018, finalizando la segunda década del siglo XXI, establece que la mayor parte de las prioridades estratégicas para la banca están relacionadas con la actualización tecnológica e innovación, tanto en sus procesos y operaciones como en sus plataformas y productos, en un marco en el cual el porcentaje de clientes que utilizan internet para acceder a canales de atención bancaria por computadoras o dispositivos móvil, a nivel mundial, supera el 90%.

En efecto, la transformación digital de la banca conlleva una optimización de los procesos productivos, por lo tanto, una modificación en la forma de ejecutarlos, y una consiguiente transformación en la relación de las compañías bancarias, al interior de estas, con sus clientes y proveedores. Pero también, al mismo tiempo, esta transformación, en tanto disrupción tecnológica, implica una serie de riesgos, uno de los más importantes es el relacionado con la seguridad de la información.

El riesgo cibernético no es nada nuevo. Su existencia subyace a las compañías. Por lo tanto, en lugar de poner continuamente medidas de seguridad, las empresas necesitan, para focalizar sus esfuerzos eficazmente, identificar sus activos comerciales más importantes y, sobre estos, diseñar y aplicar medidas de seguridad eficientes.

Con el objetivo de describir un panorama general de la seguridad de la información y los avances al respecto en el sector financiero chileno, a continuación, en primer lugar, se describirán los *beneficios de la seguridad de la información* a partir de los pilares de integridad, confidencialidad y disponibilidad. En el segundo apartado, nos referiremos a la protección de datos en base ciertos principios promovidos por la OCDE, que facilitan la protección de la privacidad y de las libertades individuales de las personas. En el tercer punto, abordaremos la importancia de implementar un Sistema de Gestión de Seguridad de la Información en las empresas, sus beneficios y las posibilidades que entrega la norma ISO diseñada para tales fines. Luego, en cuarto lugar, analizaremos la situación de la seguridad de la información en Chile y las políticas que se han implementado al respecto en el plano institucional. Posteriormente, en el quinto apartado del presente documento, describiremos las iniciativas del Sector Financiero nacional en materia de seguridad de la información, destacando el rol de la Comisión para el Mercado Financiero (CMF), las principales soluciones en materia de ciberseguridad promovidas por la banca y la descripción de los avances en tres de los principales bancos que operan en el país. Finalmente, nos referiremos a la importancia de la Ciber Resiliencia, asociada a los planes de continuidad y recuperación que tienen las empresas frente a potenciales desastres tecnológicos, destacando los aspectos que debe contemplar una organización que busca transformarse en ciber resiliente.

Ir al Índice

I. Beneficios de la Seguridad de la Información

Seguridad de la información, seguridad informática, garantía de la información, ciberseguridad, son terminologías utilizadas con frecuencia por las organizaciones indistintamente, aunque se diferencian en su enfoque, metodologías y zonas de concentración según las particularidades de cada una. Así, por ejemplo, el concepto de "seguridad de la información" está vinculado a la confidencialidad, integridad y disponibilidad de la información y de los datos relevantes para las organizaciones o empresas. Por otro lado, la "seguridad informática" hace referencia a un conjunto de mecanismos, características y prestaciones, cuya función es proteger la información que se administra. Y, finalmente, la "ciberseguridad" se relaciona con las amenazas que afectan a una entidad debido a la existencia de un ciberespacio global, excluyendo los peligros naturales, los errores personales o la seguridad física.

Ahora, específicamente, un *Sistema de Gestión de Seguridad de la Información* (SGSI), tiene como objetivo la protección de la información y de los sistemas de acceso, utilización, divulgación y destrucción no autorizada de la misma; estableciendo políticas, objetivos y procesos para lograr tales fines. Consiste en asegurar que los activos de una empresa se utilicen de la forma en que se ha decidido hacerlo, con acceso, control y modificación dentro de los límites que la propia organización ha definido[1]. En este sentido, un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una compañía, a fin de alcanzar los objetivos de negocio (ISO 27000: 2019). Para esto, un sistema de gestión establece y mantiene los procesos, los controles, los procedimientos y las políticas de seguridad que tienen por obligación el conservar aquello que se considera fundamental: los *tres pilares* de la seguridad de la información que a continuación definimos.

Integridad

Cualidad de la información para ser correcta, sin modificaciones, manipulaciones, ni alteraciones por parte de terceros no autorizados. Aquí, un aspecto relevante es la autenticación, cuestión que permite identificar al que accede, genera, modifica o elimina la información.

Confidencialidad

Se entiende como la propiedad de la información para no ser divulgada a personas o sistemas no autorizados. Es el atributo por el cual la información resultará accesible con la debida y comprobada autorización.

[1] Los activos de una empresa son la información (considerado el recurso de mayor valor), los equipos (hardware, software y la propia organización) y los usuarios (personas que hacen uso de las tecnologías).

Ir al Índice

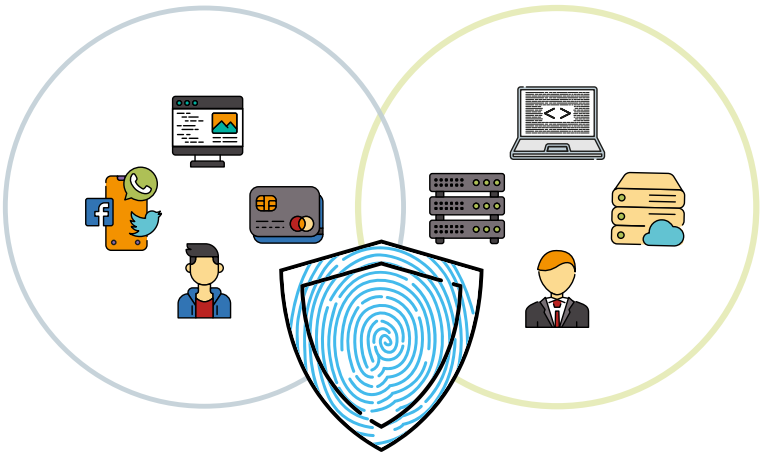
Disponibilidad

Característica, cualidad o condición de la información que se encuentra a disposición de quienes tienen los permisos para acceder, siendo estas personas, procesos o aplicaciones.

Independiente del formato que la contenga: electrónicos, físicos o digitales, la *información* debe ser *blindada*, para lo cual es necesario distinguir dos *dimensiones de la seguridad*. Por un lado, la lógica, que está relacionada con la aplicación de procesos y procedimientos que resguarden el acceso a los datos. Y, por otro lado, la física, vinculada a los equipos con los que se cuenta para almacenar información.

II. La Protección de los Datos

La ética es un tipo de saber que pretende orientar la acción humana en un sentido racional. Por lo tanto, es un saber esencialmente práctico, interesado por discernir qué debemos hacer y cómo debemos orientar nuestra conducta en virtud de obrar bien. A partir de la década de los 70 del siglo XX, en Estados Unidos surgió la *business ethics*, que se relacionó con la responsabilidad social empresarial. En palabras de Adela Cortina (2005[1994]: 89), la ética empresarial consistiría en el descubrimiento y la aplicación de los valores y normas compartidos por una sociedad pluralista en el ámbito peculiar de la empresa.



Cuando la ética se concretiza en la confidencialidad de los datos de parte de una organización empresarial y, por lo tanto, en el tratamiento seguro de éstos, su realización vincula a todas las partes interesadas (clientes, proveedores, colaboradores, socios e inversionistas) en torno a formas de actuar que promueven un tratamiento con estándares racionales sobre la información, que resguarden su privacidad, es decir, el derecho a estar libre de intrusiones o perturbaciones en la vida privada o en los asuntos personales; y protejan la integridad, calidad y disponibilidad, los tres de la seguridad de la información definidos anteriormente en este documento.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define ciertos principios básicos que complementados con otros estándares y medidas facilitan la protección de la privacidad y de las libertades individuales (OCDE, 2002:6).

Principio de limitación en la recolección de los datos

Deberán existir límites para la obtención de datos personales y cualquiera de éstos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.

Principio de calidad de los datos

Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.

Ir al Índice

Principio de especificación del propósito.

El propósito de la obtención de datos se deberá especificar a más tardar en el momento en que se produce dicha obtención, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

Principio de limitación de uso

No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el principio anterior, excepto si se tiene el consentimiento del sujeto implicado o por imposición legal o de las autoridades (por ejemplo, se puede disponer que los datos recopilados con fines de toma de decisiones administrativas puedan estar disponibles para investigación, estadísticas y planificación social).

Principio de salvaguardia de la seguridad

Se emplearán salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos. Los aspectos de seguridad y privacidad no son idénticos. Las limitaciones de uso y divulgación de los datos debieran ser medidas de seguridad reforzadas: físicas (por ejemplo, bloqueo de puertas, uso de tarjetas de identificación); organizacionales (por ejemplo, niveles de autoridad para acceder a los datos); en particular, en los sistemas informáticos (cifrado y seguimiento a amenazas de actividades inusuales y respuestas a ellas).

Principio de transparencia

Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien administra esos datos.

Principio de participación individual

Donde todo individuo tendrá derecho a que el administrador de datos u otra fuente le confirme que tiene datos sobre su persona; a que se le comuniquen los datos relativos a su persona en un tiempo razonable, a un precio –si existiese– que no sea excesivo, de forma razonable y de manera inteligible; a que se le expliquen las razones por las que una petición suya, según los puntos anteriores, haya sido denegada, así como poder cuestionar tal denegación; y, finalmente, a expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.

Ir al Índice

Principio de responsabilidad

Sobre toda administración de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

III. Importancia de Implementar un Sistema de Seguridad de la Información (SGSI) en las Empresas

La implementación y gobierno de un sistema de gestión de calidad, o cualquier otra certificación de excelencia, es clave para que una organización asegure que los servicios o productos que ofrece son fiables y cumplen con los estándares que exigen las normativas, así como la evidencia de una serie de procesos y procedimientos para la toma de decisiones apropiadas para la continuidad del negocio y la mejora continua del mismo.

Beneficios de la implementación de un SGSI

De entre todos los beneficios que se adquieren al implementar un SGSI, destacamos los siguientes:

- En los aspectos relacionados con la información, se cumple con la *protección o seguridad de los datos*, la privacidad y el control de las tecnologías de la información, determinando las metodologías necesarias para llevarlo a cabo eficientemente.

- La *ventaja competitiva* de disponer de un sistema de gestión conforme a los estándares internacionales, cuando la información que se manipula es altamente sensible.

- *Descenso de los gastos* derivados de los incidentes de seguridad, beneficio que supone una de las primeras preocupaciones en los directivos y la alta gerencia de las organizaciones. Este es uno de los principales motivos por los cuales se busca implementar un SGSI, aunque los beneficios no se aprecien de manera directa como una inversión, sino como el resultado de una reducción de los gastos directamente proporcional a la disminución de los incidentes relacionados con seguridad.

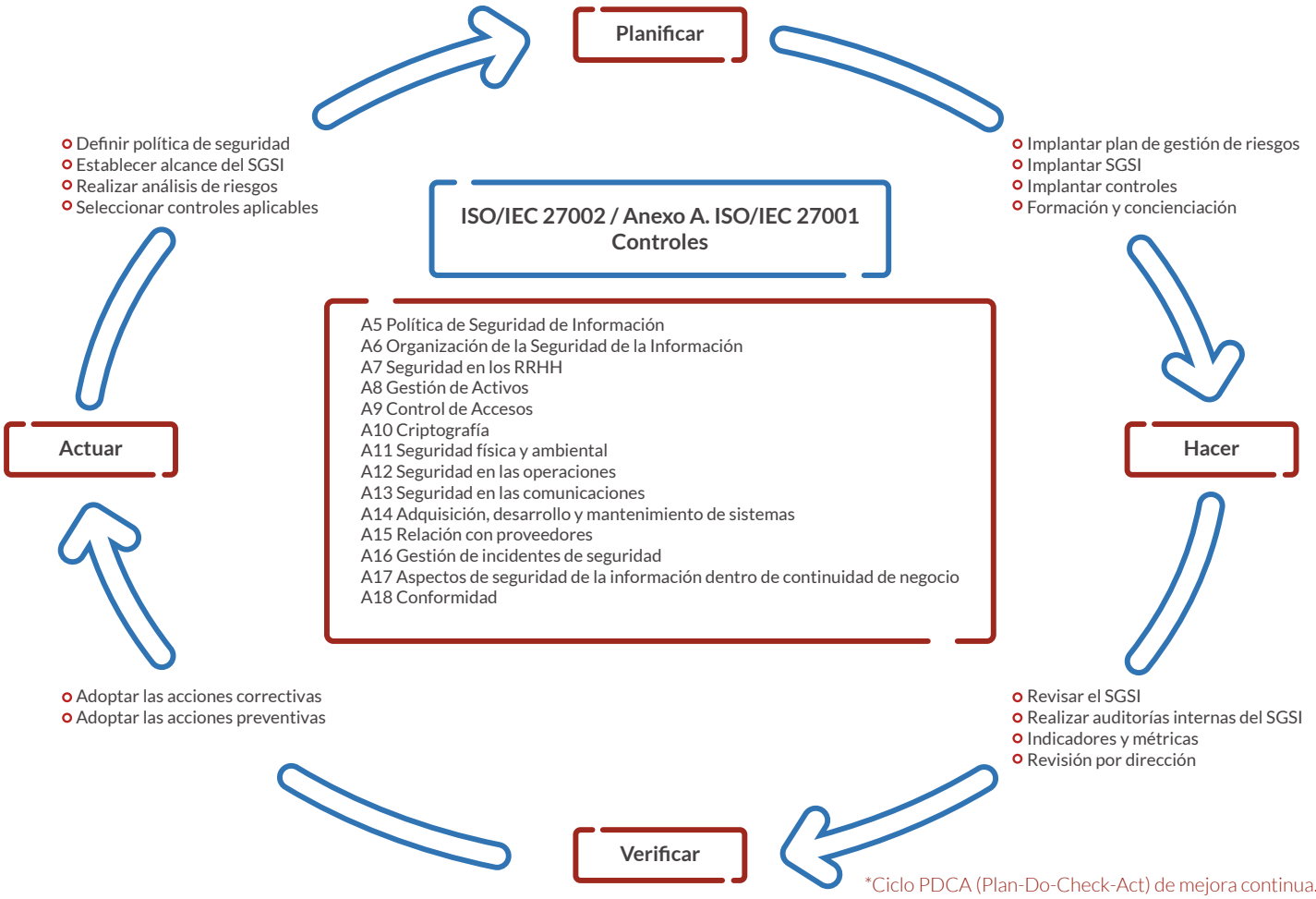
- La *organización* se fortalece con el establecimiento y la asignación de roles, responsabilidades y obligaciones, así como los alcances y objetivos, para un buen funcionamiento y desempeño.

Ir al Índice

La norma ISO 27001

Existe una gran cantidad de buenas prácticas aplicables al ámbito de la seguridad de la información en las empresas y, por consiguiente, relacionadas con la ciberseguridad. Las reconocidas mundialmente, corresponden a las de la familia ISO 27000 [2].

Específicamente, la propuesta de la norma ISO 27001 es un modelo para la definición, implementación, operación, revisión, mantenimiento y mejora de un SGSI. Permite generar una estructura de alto nivel que posibilita el reordenamiento de la seguridad de la información y de la ciberseguridad, en base a las necesidades y los riesgos propios de cada organización, centrada en la implementación de controles que permiten la gestión de los riesgos y el establecimiento de un enfoque de procesos que coadyuva a la mejora continua.



*Ciclo PDCA (Plan-Do-Check-Act) de mejora continua.

[2] La ISO (Organización Internacional de Normalización) es una institución no-gubernamental independiente, conformada por las organizaciones de normalización de sus 164 países miembros, siendo así el mayor desarrollador mundial de estándares internacionales, facilitando la creación de productos y servicios seguros, fiables y de calidad, maximizando productividad y minimizando errores y gastos.
En Chile, la Corporación de Fomento de la Producción (CORFO), el año 1973, creó el Instituto Nacional de Normalización (INN), constituido como una fundación de derecho privado sin fines de lucro. El INN es un organismo técnico en materias de la infraestructura de la calidad que fomenta la elaboración y el uso de normas chilenas, acreditando organismos de evaluación y certificación. Este organismo es fundador y miembro de la ISO y de la Comisión Panamericana de Normas Técnicas (COPANT), representando a Chile en tales espacios.
La red constituida por agentes públicos y privados, definida internacionalmente como "Infraestructura de la Calidad", es la encargada de la normalización: elaboración de normas técnicas nacionales; de la metrología: aseguramiento de la trazabilidad de las mediciones en el país; y de la acreditación: diseño, coordinación y ejecución de actividades de evaluación relacionadas con la conformidad, es decir, de certificación, ensayo e inspección.
En nuestro país, una parte importante de los elementos que componen la Infraestructura de la Calidad, han sido atribuidos y reconocidos como parte del quehacer del INN. Ello, sin prejuicio de las facultades reglamentarias y fiscalizadoras de la autoridad pública, que en muchos casos se apoya en la infraestructura de la calidad.

Ir al Índice

Este modelo facilita la implementación de los controles de seguridad de la información establecidos en el Anexo A de la norma y, en detalle, en la ISO 27002. Se estructura en torno a 14 dominios, 35 objetivos de control y 114 controles. Proporciona las directrices, el modelo de procesos y la mejora constante; entregando los lineamientos claves para la gestión de la continuidad de la seguridad de la información (ISO 22301), así como para la gestión de incidentes (ISO 27035).

Ecosistema Ciberseguridad

La ISO 27001 es el modelo sobre el cual se referencian diversos estándares para la seguridad de la información en las organizaciones, por ejemplo:

- COBIT, para el gobierno y gestión de las TIC.
- ITIL, para la gestión de servicios de TI.
- Marco de trabajo de ciberseguridad de NIST.
- El modelo de controles de NIST.

Ir al Índice

Los costos asociados a la implementación de la norma ISO 27001 se determinarán en función del tamaño, la madurez y las necesidades que tenga la organización, el negocio y la información administrada, así como su criticidad, tecnología utilizada en la gestión y las normativas aplicables en su orientación. Además, estos costos, están asociados a las siguientes dimensiones:

Formación

El implementar y gestionar un sistema relacionado con la metodología y forma de trabajo supone cambios. Por lo tanto, se vuelve imperativo capacitar a los empleados o colaboradores, entregando el material necesario y/o realizando actividades de formación acordes. También, en esta dimensión, se debe considerar la adquisición de la Norma para su disposición y consulta de todas las partes interesadas.

Asesoría externa

La capacitación del personal no es suficiente para la implementación y gobierno de un sistema de gestión. En el caso de no disponer de la formación o la experiencia, será preciso la asistencia externa de una asesoría experta, la cual debe trabajar en colaboración con los empleados para que el sistema funcione.

Inversión en tecnología

Como es regular no contar con la tecnología necesaria en la implementación de un sistema de gestión, ya sea software y/o hardware, se requiere de la optimización de la tecnología existente, así como aprender a administrarla en función de los nuevos requerimientos de seguridad de la información.

Costo temporal del personal

Los empleados van a dedicar tiempo a la implementación, el cual también se deberá considerar. La identificación de riesgos, mejora de los procedimientos y las políticas, si es que existiesen, o el desarrollo de nuevas políticas acorde a los objetivos organizacionales definidos, incluidos los tiempos que tome el capacitarse y asumir, en cada caso, las nuevas responsabilidades.

Certificación

Los costos asociados a la certificación, siempre que la organización desee obtenerla como ventaja competitiva en el mercado, deben considerarse. Esta distinción es concebida como un paso más dentro de la planificación de la implementación y los costos corresponden a la auditoría de certificación, estando directamente relacionados con el tiempo que demore a los auditores su realización.

Ir al Índice

IV. La Situación de la Seguridad de la Información en Chile

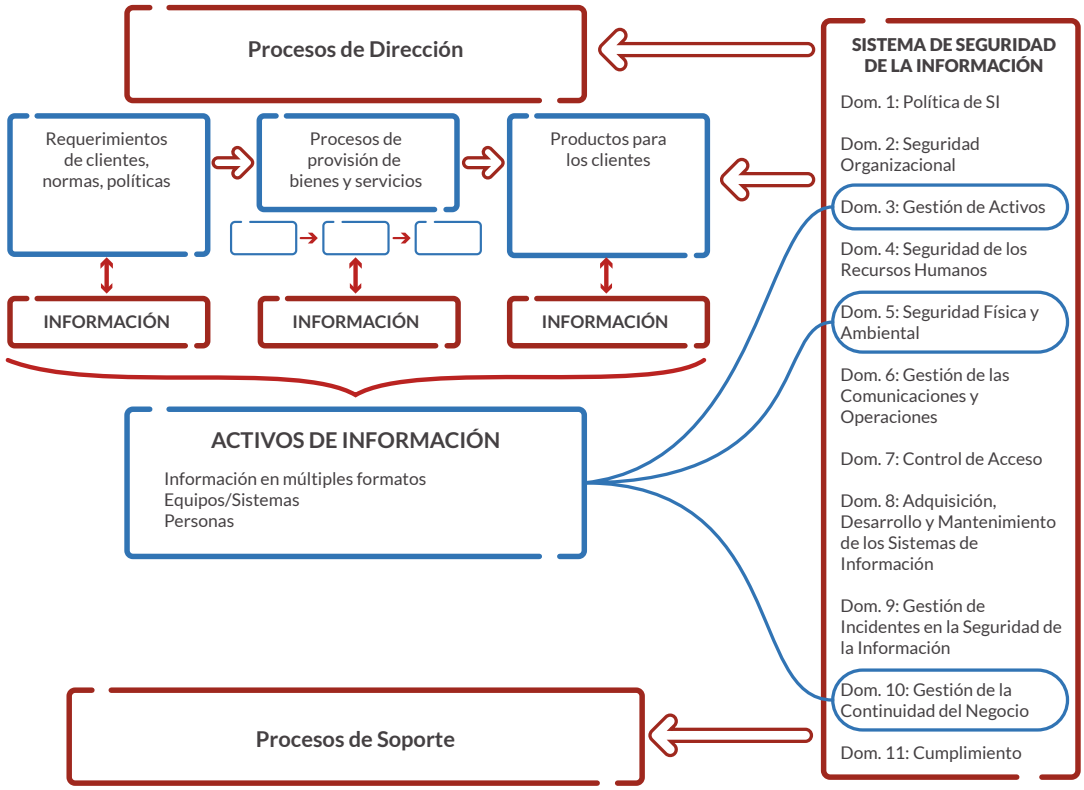
Los Programas de Mejoramiento de la Gestión (PMG) en los servicios públicos tienen su origen en la Ley 19.553 del año 1998, como parte de su proceso de Modernización del Estado, con el fin de aumentar la eficacia y eficiencia en el funcionamiento de las distintas instituciones que lo conforman. La "Seguridad de la Información" fue incorporada el año 2010 a los PMG y su asistencia técnica quedó a cargo de la Red de Expertos de la Secretaría y Administración General del Ministerio del Interior y de la Dirección de Presupuestos del Ministerio de Hacienda.

"*La información que es generada en la realización de los procesos de una institución pública es un activo que, como otros bienes de la organización, tiene gran valor y necesita ser protegida en forma apropiada. La Gestión de la Seguridad de la Información protege dicha información de una amplia gama de amenazas, con el fin de asegurar la continuidad de los procesos institucionales y la entrega de productos y servicios a sus usuarios / clientes / beneficiarios, minimizando el daño de la institución y maximizando la eficiencia y las oportunidades de mejora de la gestión organizacional*" (Ministerio de Hacienda, 2012: 3).

La información a la que hacen referencia puede ser impresa o escrita en papel, almacenada en formato digital, transmitida por correo o medios electrónicos, exhibida en películas o en una conversación.

A través de la Guía Metodológica, publicada el año 2012, se entregan una serie de requisitos técnicos, de manera detallada, sobre las distintas etapas que componen el Sistema de Seguridad de la Información, para verificar su cumplimiento con los objetivos comprometidos por los servicios públicos, asegurando así la calidad, disponibilidad y oportunidad de la información, mediante la ejecución de un adecuado conjunto de objetivos de control, traducidos en políticas, procedimientos, prácticas, estructuras organizacionales, elementos de infraestructura y funciones de software.

Dentro de sus objetivos, en la guía se declara la necesidad de "*contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional considerados relevantes, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios / clientes / beneficiarios*" (Ministerio de Hacienda, 2012:11), facilitando el identificar amenazas y vulnerabilidades que afecten los activos de información. Las definiciones y los métodos de implementación, así como la aplicación de dominios, son los indicados en la norma NCh-ISO 27001, que es la adaptación chilena realizada por el INN de la ISO 27001.



Ir al Índice

El año 2015 se creó el Comité Interministerial sobre Ciberseguridad (CICS), el cual tiene como objetivo esencial proponer una Política Nacional de Ciberseguridad, entendiéndola como "*una condición mínima de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, así como el conjunto de políticas y técnicas destinadas a lograr dicha condición*", según lo indican en el sitio oficial del comité. Este comité orientó la metodología y el cronograma de trabajo ejes temáticos relacionados con infraestructura de la información; prevención, persecución y sanción de ciberdelitos; sensibilización, formación y difusión; cooperación y relaciones internacionales; desarrollo industrial y productivo; e institucionalidad de la ciberseguridad.

V. Iniciativas del Sector Financiero Chileno en Materia de Seguridad de la Información

La *Comisión para el Mercado Financiero (CMF)* tiene, entre sus objetivos principales, el velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero nacional; y porque las personas o entidades fiscalizadas, entre ellas las entidades de los mercados de valores, seguros, bancos e instituciones financieras, cumplan con las leyes, reglamentos, estatutos y otras disposiciones que las rijan. En el año 2019, esta institución realizó una consulta relacionada con la normativa de *Gestión de la Seguridad de la Información y Ciberseguridad*, cuya aplicación comenzó a regir desde el 1 de marzo del 2020.

Esta norma establece una serie de lineamientos y mejores prácticas que deben ser consideradas por las entidades bancarias en sus procesos de gestión de la seguridad de la información y la ciberseguridad, preparándolos, frente a riesgos operacionales, en la administración, prevención y acción.

Específicamente, el capítulo de la Recopilación Actualizada de Normas (RAN) para Bancos, se divide en cuatro secciones:

- El rol del directorio para la adecuada gestión, así como su responsabilidad en la aprobación de estrategias institucionales.
- Las directrices a considerar en la implementación de un proceso de gestión de los riesgos para apoyar el sistema de seguridad de la información y ciberseguridad.
- La determinación de los activos críticos de ciberseguridad, lógicos y físicos, que soportan el funcionamiento del negocio y las funciones de protección de los mismos frente a amenazas y vulnerabilidades, la respuesta a incidentes y la recuperación de la operación normal de las entidades.
- Las políticas y procedimientos para la identificación de los activos que componen la infraestructura crítica de la industria financiera.

Ir al Índice

Con esto se complementa lo indicado en distintas normativas de la CMF en que se menciona la seguridad de la información, como son el capítulo sobre la evaluación de gestión de riesgo operacional; el capítulo acerca de los riesgos en la externalización de servicios; el capítulo de información de incidentes operacionales; y el capítulo referido a la gestión de la continuidad del negocio.

El sector financiero, específicamente la banca, ha invertido en múltiples soluciones de ciberseguridad, adaptándose permanentemente a los desarrollos tecnológicos. (ABIF, 2019:2). Ejemplos de las medidas, a nivel del sector, se destacan los siguientes:

- **Pinpass:** Protección frente al riesgo de uso indebido de la tarjeta bancaria. Uso obligatorio de PIN para compras con tarjeta en terminales POS (excepto pagos "sin contacto" de bajo valor).
- **Perturbador magnético:** Protección frente al riesgo de clonación y extracción de datos de tarjetas. Se instalan en cajeros automáticos.
- **Mensajería a clientes:** Mejora monitoreo de transacciones por parte del cliente reduciendo el tiempo de reacción en caso de fraude. Ante cada transacción, los bancos envían mensajes de texto, push o correo electrónico al cliente.
- **Monitoreo y prevención de fraudes:** Incrementa la protección en uso de productos bancarios, estableciendo mecanismos de monitoreo para detección de.

Tres de los más importantes bancos que operan en Chile, han realizado inversiones en materia de seguridad de la información y ciberseguridad, permitiendo la implementación y desarrollo de departamentos especializados para la gestión de la seguridad en cada uno de ellos. A continuación, se presenta un cuadro basado en los informes anuales del Banco de Chile, el Banco Santander y en BCI, dividido en las dimensiones de gobierno y gestión, con la descripción de los avances en la materia de cada uno de ellas:

Gobierno		
Banco de Chile	**Santander**	**BCI**
Contempla a la Ciberseguridad como una división corporativa de Control, dependiente de la Gerencia General, como parte de su 1ª línea de defensa, junto a la Gestión Comercial y Gestión Operativa. Su estructura de gobierno incluye a Directorio, al Comité Superior de Riesgo Operacional y al Comité de Riesgo Operacional. También cuentan con la División Control Global de Riesgos, que es independiente de las unidades de negocio y soporte. Es ahí donde se ubica la Gerencia de Riesgo Tecnológico y la Gerencia de Riesgo Operacional, encargadas de supervisar la aplicación de políticas, normas y procedimientos, y la gestión de riesgo operacional y tecnológico de sus filiales.	Desde el año 2014 cuenta con una Gerencia de Ciberseguridad como parte de su División de Tecnología y Operaciones, así como en la División de Riesgos cuentan con una unidad dedicada exclusivamente a controlar y supervisar el riesgo cibernético. Santander cuenta con un Jefe de Ciberseguridad o CISO (Chief Information Security Officer), función que desempeña el Gerente de Riesgo Tecnológico y Operativo. A su vez existe un Gobierno basado en tres líneas de defensa, con instancias de supervisión que incluye al Comité de Ciberseguridad, entre otros. Toda esta arquitectura permite generar resultados orientados a la identificación y corrección de los riesgos cibernéticos; al desarrollo de una cultura y de la educación en ciberseguridad; a la inclusión de ciber-escenarios para la gestión anticipada, y al cumplimiento de las actualizaciones del marco normativo de la Superintendencia en la materia.	Existe una gerencia especializada en aspectos de ciberseguridad, administrando un sistema de gestión de seguridad, donde todos sus procesos están certificados bajo la norma ISO 27001. Como parte de gestión de riesgos cuentan con varios comités específicos: de riesgos operacionales, de seguridad de la información y riesgos tecnológicos, de continuidad de negocio, y de gestión de riesgo en servicios externalizados. Dichos comités sesionan periódicamente y su objetivo es velar por la ejecución del programa de identificación y evaluación de riesgos, así como la gestión de las causas raíces para mitigar dichos riesgos.

Ir al Índice

Gestión		
Banco de Chile	**Santander**	**BCI**
Durante el año 2019, los principales hitos de la gestión estuvieron enfocadas en campañas de: concientización, respuesta a incidentes de ciberseguridad, prevención de fuga de información, administración de cuentas privilegiadas, y la implementación de nuevos factores de autenticación para conseguir una disminución en el fraude electrónico, en todos los canales de operación. También realizaron modificaciones al Código de Ética, pasando a nombrarlo como Código de Conducta, agregando nuevas dimensiones, siendo Riesgo y Ciberseguridad una de ellas.	El año 2018 lanzaron una serie de campañas de ciberseguridad para los clientes, considerados como la primera barrera de seguridad. Además, realizaron una fuerte inversión destinada a modernizar la infraestructura y la innovación en modelos de atención presenciales. Entre sus principales hitos del año 2018, se encuentra lo relacionado a su programa de continuidad de negocio, redujeron las incidencias en un 45% respecto de 2017, y en un 65% respecto de 2016; según sus registros lograron reducir la obsolescencia tecnológica, invirtiendo aproximadamente MMUS$40 en infraestructura, para otorgar calidad y servicio para los clientes, y una inversión de MMUS$13 en infraestructura, con foco en los activos expuestos a internet, herramientas avanzadas de antimalware, segmentación de redes, control de accesos y antiphishing.	Con el Plan de Ética y Cultura de Riesgos, durante el 2018, realizaron Encuentros de Ciudadanía Digital, donde analizaron tendencias de ciberseguridad, como hacking ético, seguridad en la nube, transformación digital, ingeniería social y redes, en un segundo encuentro, seguridad en redes sociales e ingeniería social, como parte de sus planes de concientización. El banco mantiene un plan de trabajo permanente para robustecer su plan de continuidad del negocio y en la capacitación de los equipos de contingencia, así como de las tecnologías de la información y las comunicaciones, aumentando las capacidades para mantener la calidad del servicio a los clientes. Lo complementan con actividades de mantención y mejora del plan de continuidad del negocio y plan de recuperación ante desastres, incluyendo la ciberseguridad, con planes, pruebas y capacitación de personal.

Existe una tendencia a invertir en el fortalecimiento de la infraestructura, tecnológica y operativa, el cual está en constante actualización y adaptación a nuevas fuentes de ataques, y es en esta línea en la que también se considera fuerte la inversión, en mantener los planes de respuesta a incidentes y de continuidad del negocio. Es así como desarrollan el trabajo de comités específicos para la construcción de planes anuales de concientización de sus clientes, y la formación y capacitación de los colaboradores y proveedores. Sin un trabajo conjunto de todas estas áreas, no habría una reducción, que se demuestra estadísticamente en las auditorías, de la minimización de las vulnerabilidades y amenazas propias del negocio.

VI. Importancia de la *Ciber Resiliencia*

La norma ISO 27000, que rige la implementación de los SGSI en las empresas, indica la obligación de elaborar un levantamiento del *Plan de Continuidad del Negocio* y del *Plan de Recuperación frente a Desastres Tecnológicos*. Ambos planes conforman lo que actualmente se conoce como *"Ciber Resiliencia"*, la cual puede ser definida como la *capacidad de las organizaciones para recuperase de forma rápida frente a los ciberataques, centrándose en la ciberseguridad y no solamente en las estrategias de prevención*. Las ventajas de la Ciber Resiliencia están asociadas a:

Ir al Índice

Gestión de riesgos

Al evitar las brechas de seguridad en virtud de recuperarse lo antes posible de un virtual ataque, se revisa con mayor exhaustividad los riesgos, vulnerabilidades y eventos que puedan afectar a la organización.

Ventaja frente a la competencia

Un plan de recuperación efectivo será un factor en las relaciones comerciales, tanto con clientes como proveedores.

Reducción del impacto económico

Cuanto más rápida sea la respuesta de la organización ante una eventualidad, antes se recupera el funcionamiento operativo normal de la empresa y menos impacto tendrá sobre la organización.

Finalmente, para que una compañía sea considerada una organización *ciber resiliente* debe contemplar los siguientes aspectos:

Dimensión	Metodología
Evaluación: determinar fuentes de riesgo, información crítica a resguardar, así como definir y clasificar las brechas de seguridad según la magnitud de impacto dentro de la organización.	Análisis GAP, de brechas o de necesidades, para determinar la distancia entre el estado actual y a dónde queremos llegar, dependiendo la tolerancia de la organización.
Protección: implementar medidas que minimicen los riesgos.	Establecer, desarrollar e implementar un Sistema de Gestión de Riesgos. Contenido en ISO 27001.
Monitorización: revisar y comprobar las medidas implementadas, enfocadas en prevención y recuperación.	Establecer un plan de auditorías, internas y externas.
Solución: desarrollar un plan de resolución de problemas, identificando las acciones de los miembros del equipo de seguridad ante las amenazas.	Administrar un Plan de Respuesta a Incidentes. Contenido en ISO 27001.
Recuperación: diseñar e implementar un plan de continuidad del negocio.	Gestionar un Plan de Continuidad del Negocio. Contenido en ISO 27001.

Ir al Índice

Bibliografía

ABIF. (2019). *ABIF Informa N°139. Ciberseguridad en la banca*.
Disponible en: https://www.abif.cl/docs/default-source/abif-informa/informe-abif-n-139-(ciberseguridad).pdf

Banco de Chile. (2019). Memoria Anual 2019.
Disponible en: https://ww3.bancochile.cl/wps/wcm/connect/81b4cc804d5d5218b118f57c2d622285/Memoria_2019_web.pdf?MOD=AJPERES&CONVERTTO=url&CACHEID=81b4cc804d5d5218b118f57c2d622285

Santander. (2018). Informe Anual 2018.
Disponible en: https://www.santander.cl/nuestro_banco/pdf/memoria-financiera-banco-santander-2018.pdf

BCI. (2018). Memoria Integrada 2018.
Disponible en: https://www.bci.cl/investor-relations/memoria-anual/files/memoria-anual-2018-2

Castells, Manuel. (2008 [1996]). *La era de la información: economía, sociedad y cultura. Volumen 1: La sociedad red*.
Madrid: Alianza editorial.

CEPAL. (2017). *Estado de la banda ancha en América Latina y el Caribe*.
Disponible en: https://repositorio.cepal.org/handle/11362/43365

CEPAL. (2018). *Estado de la banda ancha en América Latina y el Caribe*.
Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/43365/1/S1800083_es.pdf

Cortina, Adela. (2005[1994]). Ética de la empresa· Claves para una nueva cultura empresarial. Madrid: Editorial Trotta.

Digital Banking Report. (2018). *2018 Retail Banking Trends and Predictions*.
Disponible en: https://www.digitalbankingreport.com/trends/2018-retail-banking-trends-and-predictions/

Ministerio de Hacienda. (2012). *Guía Metodológica 2012. Programa de mejoramiento de la gestión. Sistema de Seguridad de la Información*.
Disponible en: https://www.mop.cl/acercadelmop/PMGSSI/Guia_Metodologica2012.pdf

OCDE. (2002). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.
Disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf

Ciberseguridad Gobierno de Chile.
Disponible en: https://www.ciberseguridad.gob.cl/faq/

Ir al Índice

Av. Libertador Bernardo O’Higgins 949 Piso 14 Santiago Chile
+(56 2) 2829 1900
www.creasys.cl
info@creasys.cl