UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL

GUÍA DE IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ENTIDADES DE INTERMEDIACIÓN FINANCIERA

TESIS PARA OPTAR AL GRADO DE MAGISTER EN GESTIÓN Y DIRECCIÓN DE EMPRESAS

JUAN LUXEN GUMUCIO SUAREZ

PROFESOR GUÍA:
IVÁN MIGUEL BRAGA CALDERÓN

MIEMBROS DE LA COMISIÓN
CHRISTIAN ANDRE DIEZ FUENTES
EMILIO GIMÉNEZ

SANTIAGO DE CHILE
2021

RESUMEN

GUÍA DE IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DE RIESGOS DE CIBERSEGURIDAD EN ENTIDADES DE INTERMEDIACIÓN FINANCIERA

La transformación digital, ha puesto a la Ciberseguridad a la altura de los riesgos establecidos por el acuerdo de Basilea II Basilea. En Latinoamérica, se ha comenzado a legislar respecto a Ciberseguridad de forma muy general. Es por esta razón, que se definió y realizó el presente trabajo, que entrega una guía para los gerentes de riesgo de cara a implementar la gestión de Ciberseguridad en Entidades de Intermediación Financiera, utilizando como base el Marco de Trabajo NIST (National Institute of Standards and Technology), De esta forma se resuelve el problema de cómo encarar la incorporación de la gestión del riesgo de Ciberseguridad en Entidades de Intermediación Financiera.

Los métodos utilizados en la presente guía integran el proceso que parte desde la base del Marco de Trabajo NIST en su primer pilar que describe el “IDENTIFICAR”. Este va desde el entendimiento y estructura de la Organización, los cambios en el gobierno corporativo de riesgos, así como la propuesta de pasos a seguir para implementar la gestión y Cultura organizacional de cara a la Ciberseguridad, para finalmente cerrar el ciclo con una propuesta de gestión integral del riesgo de Ciberseguridad a partir de la metodología actualmente existente para la medición del riesgo operacional como punto base. Esta se fusiona luego con la propuesta de medición emitida por Common Vulnerability Scoring System CVSS, la cual integra en la forma de medición a la vulnerabilidad y la amenaza dentro el factor de probabilidad.

Como base práctica se utilizó la metodología aplicada actualmente en una Entidad de Intermediación Financiera Boliviana, como un caso de éxito y ejemplo en dicho país. Esta metodología le ha permitido no solo gestionar los riesgos no financieros de forma integral, sino también de agregar valor a la Organización permitiendo asegurar sus pilares digitales como punta de lanza de su estrategia de negocio. Lo que permite avanzar maximizando la rentabilidad del accionista al contar con productos y servicios seguros y eficiente y con un apetito de riesgo claramente definido, controlado y gestionado.

DEDICATORIA

Al finalizar este trabajo quiero agradecer primero a Dios por sus bendiciones, a mi familia, compañeros de trabajo, universidad y amigos por su apoyo en esta etapa del Magister, en especial a:

A mi esposa Lore, quien más directamente ha sufrido las consecuencias del MBA por todo su amor, comprensión, paciencia y apoyo incondicional siendo ese soporte que te impulsa a seguir adelante con una palabra, un gesto de cariño, aliento y compañía a lo largo de esto este camino que tuvo alegrías, pero también largas jornadas de estudio, noches en vela y el sacrificio del poco tiempo juntos ¡Mil Gracias por que este logro es de los dos, Te Amo!!

A mi mami Beby, por su amor, comprensión y apoyo incondicionalmente a lo largo de todo el camino de mi vida, quien además me ha enseñado con el ejemplo a encarar las adversidades sin perder nunca la fortaleza, en especial en aquellos momentos donde solo toca esperar y sacrificar el poco tiempo juntos ¡Mil gracias Te Amo!!

A mi Papa (Luxen) y mi hermana (Vanessa), por su amor, preocupación, comprensión y apoyo ¡Mil gracias Los Amo!

A dos personas que amo, aunque no estén ya presentes y quienes estoy seguro que desde el cielo me estuvieron dando fortaleza para seguir adelante Mami Nena y mi tío Coco

A mi pequeña “Morita” por ser esa dulce compañía y amor constante e incondicional. A toda esa música (en especial a KISS) que acompañaron el vacío de esos momentos donde solo queda remar a pesar de la hora y el cansancio.

También agradezco a…

Mis compañeros del MBA, por todo lo compartido en especial a mi amigo Nico Papic por ser ese socio constante.

Por su apoyo, lealtad y su tiempo cuando los necesite, Gracias Robert A., Raul Q., Edgar V., Alejandro G., Pablo H. y Carito P. y a todo mi equipo de Riesgo Operativo BCP.

A esas grandes personas y líderes Marcelo Trigo, Sara Huaman y Liliana Riveros por su apoyo en mi carrera en el Banco de Crédito sin cortarme las alas para llevar adelante todos mis objetivos.

¡Siempre estaré en deuda con cada uno de ustedes!!!

Luxen.

TABLA DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE CUADROS

INTRODUCCIÓN

El uso masivo de las Tecnologías de la Información y Comunicación (TIC) ha tenido efectos trascendentales en lo político, social y económico a nivel mundial. La globalización tecnológica ha ocasionado aspectos positivos como ser, la generalización del conocimiento, nuevos medios de producción en lo industrial, nuevos canales y formas de prestar servicios financieros. Sin embargo, los adelantos tecnológicos no solo han sido utilizados para el bien de la humanidad, sino que también para intereses ilícitos de algunos individuos, grupos o Estados.

Hoy en día la sociedad moderna depende de las computadoras y las redes informáticas, es así que estas herramientas se han convertido en vitales para funciones clave como la gestión y operación de Sistema financiero, centrales nucleares, represas, red de energía eléctrica, el sistema de control de tráfico aéreo y el gobierno.

La transformación digital si bien ha conseguido cambiar la forma de hacer negocio bancario y de interactuar con los clientes, en busca de ser más rentable, eficiente y no perder espacio versus empresas como Facebook que quieren ingresar al negocio bancario, ha puesto a la Ciberseguridad a la altura de los riesgos tradicionalmente monitoreados en la Banca. Todo esto deja ver claramente la dependencia del sistema financiero a los sistemas informáticos, con lo cual son más vulnerables ante las ciberamenazas y a pesar de los riesgos que corren, es una tendencia que no se va a detener, lo que nos indica que hay que actualizar la forma en la cual la banca en general debe gestionar el riesgo de Ciberseguridad.

En la actualidad se aprecia que los delitos cibernéticos se han vuelto mucho más sofisticados, se han complejizado las actividades de ciberespionaje militar, económico, industrial y político, y se han incrementado los ciberataques a estructuras críticas, tanto por parte de grupos organizados como por individuos. El ciberespacio es muy atractivo por ser un ambiente complejo, que permite mantener en el anonimato[1]casi total a los ciberatacantes.

Recientes estudios del Fondo Monetario Internacional, mediante modelaciones de riesgo financiero y una muestra de 7.947 Entidades Financieras en el mundo, establecen que pueden comprometerse del 9% al 62% de los ingresos netos de las entidades (USD$97.000 millones a USD$ 642.000 millones) por ataques cibernéticos. [2]

De acuerdo con el estudio presentado por Ernst and Young sobre Ciberseguridad, en el III Congreso de Riesgo Bancario, en República Dominicana[3], las causas que están impulsando el riesgo de Ciberseguridad son:

- Empleados descuidados o mal intencionados.

[1] *Los ciberataques se llevan a cabo de una forma anónima de modo que sea casi imposible detectar a su autor, y en caso de que se lo detecte este ya haya cumplido su cometido. Se busca actuar anónimamente en línea para realizar transacciones financieras fraudulentas o lanzar ataques con poco riesgo de ser localizados por las agencias policiales y con el objetivo evitar las consecuencias de un comportamiento criminal o socialmente inaceptable. (Weber & Heinrich, 2012, pág. 5).*

[2] **(Asociación Bancaria y de Entidades Financieras de Colombia, 2019)**.

[3] **(Rodriguez, 2018)**.

- Phishing.
- Falta de Controles de Sistema y Organización (SOC).
- Entidades no estén preparadas con un plan de respuesta ante incidentes.

El sistema financiero realiza funciones de servicio que son de carácter central para la actividad económica a nivel mundial, tales como captar ahorros, otorgar créditos, facilitar transacciones de pagos, transferir riesgos, proporcionar liquidez e incluso medir la asignación de precios en el mercado, es así que, el deterioro significativo de cualquiera de las actividades antes descritas puede causar inestabilidad financiera. Las crisis financieras suelen ser originadas generalmente por fallas de mercado o de política económica, mientras que los eventos de ciberataques son siempre realizados y programados de manera premeditada con el objetivo de deshabilitar, destruir, corromper, comprometer el funcionamiento del mercado.

El Foro Económico Mundial a través de su informe anual de Riesgos Globales, muestran la creciente importancia que han adquirido los ataques cibernéticos con la finalidad de fraude y robo de datos, motivo por el que concluye que existe una alta probabilidad de ocurrencia de este riesgo y con el nivel de impacto equivalente al de los desastres naturales y los ataques terroristas.

Por lo expuesto, el presente trabajo permite facilitar una guía de actividades, pasando desde la identificación de etapas, metodologías y legislación guía comparativa, para que las empresas y en especial los bancos construyan sus propias estrategias de implementación de cara a la gestión del riesgo de Ciberseguridad.

1. Situación actual de la Banca en América Latina en cuanto a la Ciberseguridad.

Utilizando como base el estudio realizado por la Organización de Estados Americanos (OEA) emitido en el año 2018, La información analizada en el estudio que se utiliza como base para este capítulo tuvo dos frentes. El primero orientado a las Entidades Financieras, analizándose datos de 191 entidades financieras de la región. El segundo frente estuvo enfocado en los clientes del sistema bancario, y se analizaron los aportes de 722 usuarios de la región.

El presente capítulo, realiza una descripción breve a fin de dar al lector una mirada general respecto a la situación actual del sistema financiero en América Latina y en qué etapa de madurez se encuentran respecto a la gestión de la Ciberseguridad, de cara a robustecer las capacidades y nivel de conciencia sobre las crecientes amenazas a la seguridad digital que aborda la nueva forma de prestar servicios financieros, no solo en la región, sino también a nivel mundial.

1.1. Antecedentes.

Respecto a la preparación y gobierno corporativo de la seguridad digital, en promedio 41% de las Entidades Financieras en América Latina, cuentan con dos niveles de jerarquía entre el CEO y el responsable de la seguridad digital. No obstante, en la última etapa y debido a que la Ciberseguridad ha escalado en el ranking de prioridades de las empresas y bancos a nivel mundial, el rol del CISO (Chief Information Security Officer) ha tomado mayor relevancia en la estructura de gobierno de las entidades financieras, llegando a estar incluso a un nivel de diferencia del CEO. Ejemplos claros de estos cambios que han marcado tendencia son el Grupo Santander, BBVA, Itaú y el grupo CREDICORP de la cual forman parte el Banco de Crédito del Perú y Banco de Crédito de Bolivia.

Hasta finales de 2017, en promedio en el 74% de las Entidades Financieras se tiene una única área responsable por la seguridad digital. Cabe señalar qué, el rol de la gestión del riesgo de seguridad digital (incluyendo seguridad de la información, Ciberseguridad y prevención del fraude vía canales digitales) debe originarse en la alta dirección de los bancos, por este motivo el 60% del total de las Entidades Financieras en la región han empezado a adoptar las siguientes medidas en busca de gestionar la Ciberseguridad:

- Adopción de buenas prácticas de seguridad.
- Impulsar la cultura a través de capacitación y sensibilización en educación de seguridad digital.
- Promover planes de seguridad digital.

En la actualidad, el 72% de las Entidades Financieras en América Latina presentan a sus juntas directivas y de accionistas reportes periódicos acerca de su adecuación al Marco de Ciberseguridad del NIST (National Institute of Standards and Technology), así como sus indicadores y gestión de riesgos de seguridad digital. Sin embargo, según el estudio de la OEA el 60% de los encuestados (incluido el autor) considera que convencer a la

alta dirección de la Organización de invertir en soluciones de seguridad digital es bastante complejo, debido a la relevancia que tienen las inversiones especialmente en materia de programas de monitoreo, herramientas prevención y desarrollo de capacidades y/o habilidades dentro de la Organización. Sin embargo, la clave para lograr el apoyo de la alta dirección es enfocarse en demostrar a través de la medición del riesgo, el impacto de una posible pérdida financiera.

Dentro de los estándares, mejores prácticas y marcos metodológicos más implementados en las Entidades Financieras de la región, se encuentran las normas Ciberseguridad del NIST (National Institute of Standards and Technology), ISO 270032, ISO 27001 y COBIT, es así que el 68% y 50% de las Entidades Financieras, están utilizando como marcos de referencia el NIST y las normas ISO.

1.2. Medidas que están siendo adoptadas.

De toda la información revisada, el 82% de Organizaciones en la región consideran que es necesario que el equipo a cargo de seguridad de información y de gestión de riesgo de Ciberseguridad, debe ser ampliado en el corto plazo, así mismo. Este crecimiento implica que dentro las unidades de riesgos, debe reconvertirse el equipo a fin de que los analistas de riesgos puedan realizar un control a la gestión propia de la seguridad de información tecnológica y Ciberseguridad, facilitando políticas y lineamientos que permitan una gestión completa, preventiva y estratégica más allá de lo operativo.

Adicionalmente a lo mencionado, la necesidad de probar la efectividad de los controles de seguridad de información y Ciberseguridad en las entidades financieras, llevan en muchos casos a requerir procesos de tercerización, dentro las cuales la actividad contratada con mayor frecuencia son las pruebas de seguridad Ethical Hacking (65% del total).

Respecto a capacidades de detección y análisis de eventos de seguridad digital, las entidades de la región han implementado:

a) El 90% cortafuegos y actualizaciones automatizadas de virus y sistemas.

b) El 85% implementaron Sistemas de Detección / Prevención de intrusiones (IDS e IPS), como Procesos de Monitoreo de Amenazas y Vulnerabilidades.

Debido a los altos costos de las herramientas de defensa y monitoreo, las cuales resultan vitales a la hora de prevenir ciberataques o determinar patrones sospechosos asociados a fraude entre otras capacidades de detección, como ser, el SOC (Centro de Operaciones de Seguridad), Antimalware, Antispam, Virtual Patching, Segmentación de Redes, Machine Learning, Big Data, etc. Para adquirir dichas tecnologías, las entidades financieras necesitan esforzarse de manera significativa y planificada en cuanto a su presupuesto,

En América Latina y El Caribe, el 49% de las entidades aún no han implementado herramientas y controles de cara a la gestión de seguridad de información y Ciberseguridad, situación que lleva a concluir que el sistema latinoamericano regional convive con una alta probabilidad de ser víctima de ciberataques a nivel sistémico.

1.3. Riesgos principales en América Latina y El Caribe.

Los principales riesgos de seguridad digital que merecen mayor atención de parte de las Entidades Financieras en el continente son:

I. El robo de base de datos crítica;

II. El compromiso de credenciales de usuarios privilegiados;

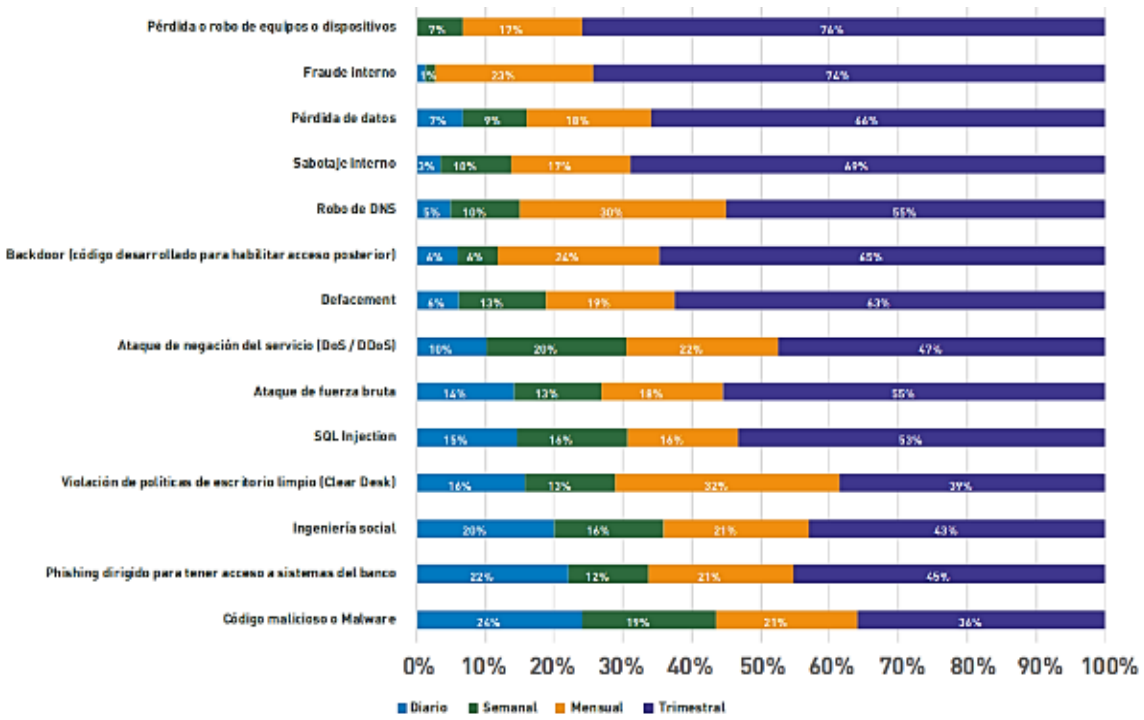
III. La pérdida de datos.

Del estudio realizado por la Organización de Estados Americanos (OEA), se concluyó que el 92% de las Entidades Financieras aceptaron haber sufrido ciberataques (ataques exitosos y ataques no exitosos). Adicionalmente, el estudio de la OEA utilizado como base para el presente capítulo, establece como los eventos principales ataque en Entidades Financieras:

- Malware-código malicioso en el 80%;
- Violación de Políticas Clear Desk en el 63%;
- Phishing en el 57%.

A continuación, el Gráfico 1 detalla los eventos de seguridad digital contra Entidades Financieras durante 2018 y el primer trimestre de 2019.

Gráfico 1. Eventos de seguridad digital contra Entidades Financieras durante 2018 y el primer trimestre de 2019.



Fuente: **(Organización de los Estados Americanos, 2018).**

De acuerdo al estudio de la OEA el rango de afectación en dólares Americanos señalado por los usuarios bancarios está entre 101 y 500 dólares Americanos y solo en un 0,67% de las veces los clientes han llegado a perder más de 10 mil dólares Americanos[4], los motivos para que esta pérdida sea tan sectorizada monetariamente, se debe a que los usuarios en su generalidad confían por ahora más en la presencia física que en la digital.

Por lo expuesto, se decide profundizar en los ataques por phishing y Malware que son los más comunes en la región latinoamericana, de acuerdo a los antecedentes, la estadística brindada por Karspersky Lab entre enero y junio de 2018, América Latina recibió 510.671 ataques, con un promedio por día de 2.837.

Como puede verse en el cuadro 1 Brasil es el país que más ataques recibió 22.12%, siendo el número 1 no solo a nivel región, sino también a nivel mundial, como puede verse, Chile (14.13%) y Bolivia (13.84%), se encuentran en los puestos 19 y 22 del ranking mundial respectivamente y todos los países de la región se encuentran en el top 30 del ranking, situación que lleva a concluir que de no hacer algo pronto la probabilidad de ataques y pérdidas económicas en el continente es altísima.

Cuadro 1. Ranking de países atacados por phishing, enero-junio de 2018.

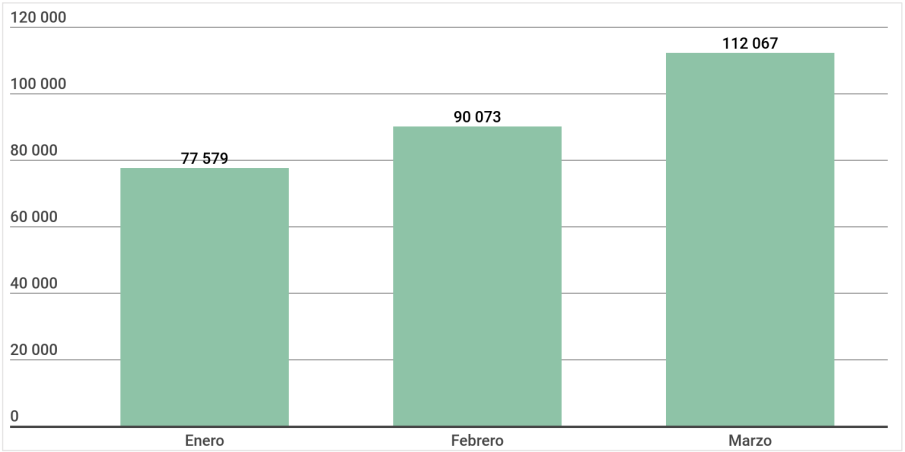
LatAm	Worldwide	País	% de usuarios infectados
1	1	Brasil	22.12%
2	5	Venezuela	16.26%
3	7	Argentina	15.5%
4	15	Peru	14.42%
5	**19**	**Chile**	**14.13%**
6	**22**	**Bolivia**	**13.84%**
7	28	Panamá	13.19%
8	29	Colombia	13.11%
9	30	Ecuador	13.09%
10	35	Nicaragua	12.42%

Fuente: **(Kaspersky Lab, 2019).**

Por lo expuesto a continuación en el cuadro 2, conforme a lo señalado en el Boletín de Seguridad de Kaspersky Lab, durante el primer trimestre de 2019 se identificaron intentos de ejecutar programas maliciosos para robar dinero de cuentas bancarias en los equipos de 279,719 personas afiliadas a los servicios que presta esta empresa a nivel mundial.

[4] *Fuente:* **(Organización de los Estados Americanos, 2018)**.

Cuadro 2. Ataques registrados por Kaspersky a sus usuarios, enero-marzo de 2019.

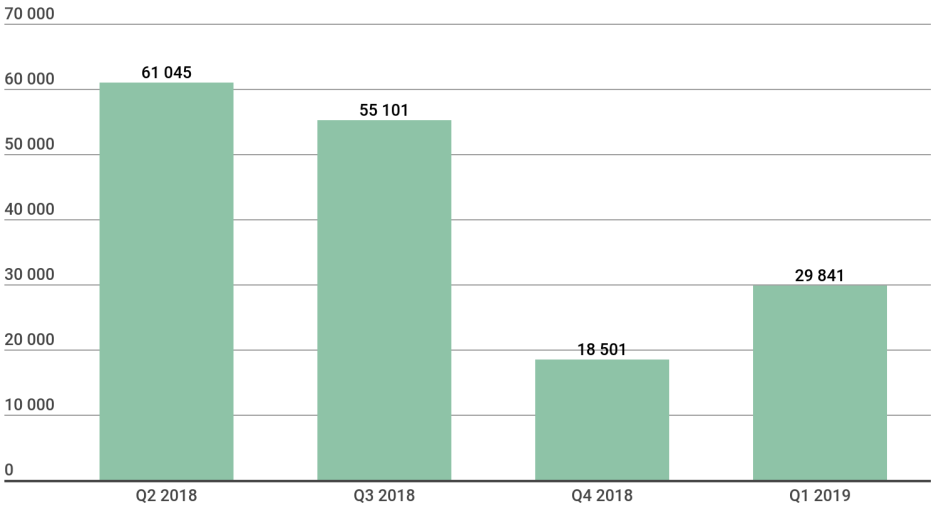


Fuente: **(Kaspersky Lab, 2019).**

Siguiendo con el relevamiento, en el cuadro 3, se exponen el número de paquetes de instalación de troyanos bancarios móviles, el cual muestra que a partir del segundo trimestre de 2018 y hasta el primer trimestre de 2019 tiene una tendencia descendente, arrojando a la fecha de corte 30 mil instalaciones de troyanos entre Bancos, Empresas de Sistemas de Pago, Retail, siendo el foco de los ataques Cajeros Automáticos e infraestructura financiera.

Si bien es posible inferir que el primer cuatrimestre de 2019 los ataques han disminuido versus el 2018, debe señalarse que habría que realizar el monitoreo específico que permita confirmar si la caída se debe a que las entidades del sector evaluado han implementado medidas más robustas de cara a la protección de sus sistemas, o si se trata de un factor de comportamiento cíclico en función a la demanda y uso de aplicaciones bancarios de las personas.

Cuadro 3. Troyanos bancarios móviles registrados a nivel mundial por Kaspersky a sus usuarios (2018-2019).



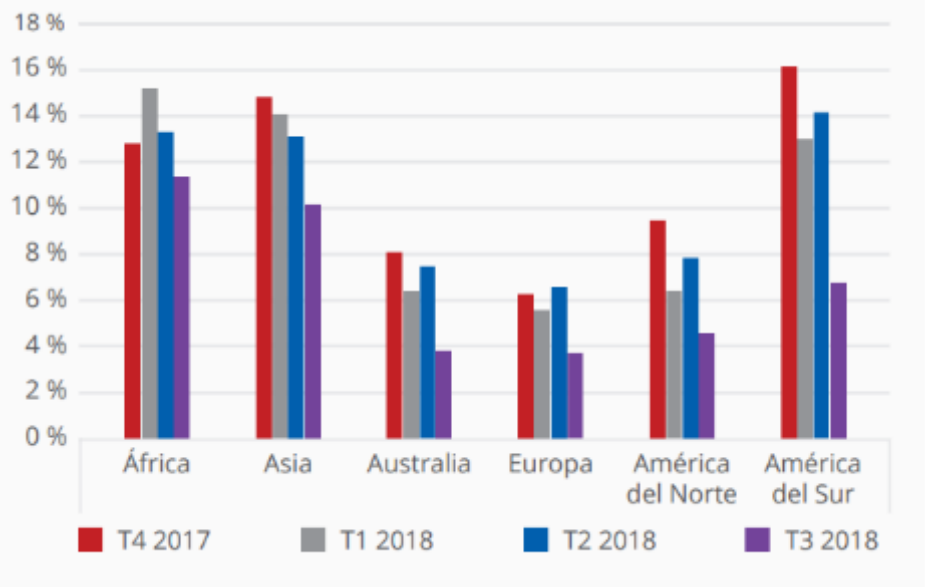
Fuente: **(Kaspersky Lab, 2019).**

A continuación, el cuadro 4 publicado en 2018 por McAfee Labs, permite observar la tasa comparativa por región a nivel mundial de infección, debido a los tipos de ataques vía Malware en móviles, de este gráfico se puede inferir que:

A nivel de América del Sur, si bien los ataques han disminuido respecto a 2017, siguen siendo más elevados que en Europa, América del Norte y Australia, esto debido a que al ser América Latina una región culturalmente menos digital respecto a las demás regiones, esta menos preparado de cara a la gestión del riesgo de fraude digital, incrementando así la probabilidad de ataques.

Por lo expuesto, las entidades que comparten el ecosistema financiero en América Latina, se ven en la necesidad de implementar la gestión del riesgo de Ciberseguridad, a fin de mitigar pérdidas económicas para ellos y sus clientes y además ver este tema como una oportunidad de diferenciación de servicio desde el punto de vista de la seguridad digital.

Cuadro 4. Tasas de infección por malware en móviles por región 2018.



Fuente: **(Labs, McAfee, 2018).**

Por otra parte, es necesario precisar que de acuerdo al estudio de la Organización de Estados Americanos (OEA) "*Estado de la Ciberseguridad en el Sector Bancario en América Latina y El Caribe",* publicado en 2018 y utilizado como guía de este apartado, nueve de cada diez bancos admitieron recibir ataques cibernéticos.

De la encuesta realizada a 191 Entidades Financieras en la región, se puede ver que crecen cada vez más los grupos de delincuentes cibernéticos que apuntan al sistema financiero. Es así que, el 37% de Entidades Financieras manifestaron que sí fueron víctimas de incidentes (ataques exitosos) y la principal motivación de dichos ataques durante el año 2017 fueron Motivos Económicos (79% de las Entidades Financieras víctimas).

Si bien los informes públicos sobre ataques cibernéticos sofisticados en Bancos de América Latina y el Caribe son menos frecuentes que en América del Norte, Europa y

Asia, hay evidencia reciente que muestra que la relativa tranquilidad de la región está llegando a su fin.

A mediados de 2018, los Bancos en México fueron blanco de grupos con las características de Amenaza Persistente Avanzada (APT, por sus siglas en inglés), asimismo, durante el mismo año, el Banco de Chile fue atacado llegando a sufrir una pérdida de aproximadamente 10 Millones de Dólares Americanos y de 1.800 Millones de Dólares Americanos en gastos en asesorías y servicios tecnológicos.

La Organización de los Estados Americanos (OEA) en su reporte Estados de la Ciberseguridad en el Sistema Financiero Mexicano de 2019, indicó que, de 240 entidades financieras mexicanas, 43% sufrieron incidentes cibernéticos en 2018, de las cuales 56% no reportó el ataque ante las autoridades, por lo que la cifra de usuarios víctima del cibercriminal alcanzó los 14.3 millones de personas, lo que representa al 31% del total de clientes. Esto sin contar que el costo monetario de dichos ciberataques llegó aproximadamente a los 107 millones de dólares. Precisar que, los principales ataques en la región provienen de ataques vía Phishing, ransomwere (Wanna Cry, Blue Keep).

Otro ataque de magnitud reportado en 2019 en la región fue el ocurrido al Banco Capital One en Estados Unidos quien fue víctima de uno de los ataques más grandes que jamás haya ocurrido a una Entidad Financiera, mediante la filtración de datos de 100 millones de solicitudes de tarjetas de crédito en Estados Unidos, entre la que se encuentra información personal como fechas de nacimiento, domicilios, datos de contactos.

1.4. La Ciberseguridad y sus efectos para la sociedad.

Los cambios tecnológicos y los riesgos a los cuales se enfrenta la Banca, son una consecuencia de las necesidades de la evolución y transformación tecnológica en la sociedad moderna, en este entendido de cara a las personas individuales, si bien la tecnología y el vivir interconectado ha mejorado en general su calidad de vida, a su vez, han generado nuevas amenazas con las que deben aprender a convivir y gestionar. Algunas de estas nuevas amenazas son el robo, secuestro y el uso sin consentimiento de datos personales, el robo de dinero a través del hackeo de cuentas, además del poder de las grandes empresas tecnológicas como Facebook, WhatsApp, Google, incluso las Entidades Financiera respecto al manejo y mercadeo de información (que las personas autorizan sin saber ni leer los términos y condiciones).

1.4.1. Datos personales e información confidencial.

Las redes sociales con las que todos los ciudadanos interactúan como Facebook, WhatsApp, Instagram, los buscadores como Google, las empresas de telecomunicaciones, Entidades Financieras y servicios digitales como Apple, Amazon e incluso los Estados, se han dado cuenta de los siguientes puntos que al ser utilizados de mala manera pueden llevar a generar daños irreparables en la sociedad:

- El valor que representan los datos de las personas de cara a la generación de negocio.

- Cómo pueden motivar cambios en la conducta de las personas de forma inconsciente a través de la entrega de información a medida de cada usuario.

- Carencia o vacío legal de una figura jurídica de aplicación global de protección de datos y privacidad, que lleva a generar un “mercado de venta de datos”, sin consentimiento consiente del dueño de la información, debido a que está obligado a aceptar los términos y condiciones si quiere formar parte del ecosistema.

Es así que los ciber delincuentes más allá de realizar ataques a los individuos uno a uno se han dado cuenta que las empresas que tienen los datos masivos de las personas tampoco se encuentran protegidas de ataques al 100% por lo que en los últimos 5 años se han volcado a realizar ataques directos a estas Entidades para así conseguir datos de sus clientes, propietarios y funcionarios y venderlos en la Deep Web a cambio de miles de dólares.[5]

a) El riesgo de la falta de regulación de la relación jurídica Usuario – empresas de servicio.

Al no existir límites jurídicos uniformes a nivel mundial que permitan regular la contratación de servicios en línea y uso de datos personales de parte del prestador del servicio, el vacío legal permite que los usuarios sin su conocimiento sean vulnerados en su información personal, y así potenciar el negocio de la Organización y segmentar sus campañas de productos, sin embargo a su vez, las empresas a través de sus contratos de adhesión de servicio se eximen de responsabilidad en caso de robo o vulneración de sus bases de datos en las cuales mantienen el resguardo de la información de sus clientes.

Analizando el contrato de términos y condiciones de WhatsApp, podemos ver los siguientes riesgos para el usuario y los abusos de la empresa:

Confidencialidad: WhatsApp al estar en la nube, no garantiza la confidencialidad y seguridad de la información que el usuario comparte, (mensajes de texto, audio, fotos y contactos). Lo cual le permite, por un lado, transferir su responsabilidad al mismo usuario así sean ellos quienes tienen el control de los servidores y redes que son vulneradas y por otro les da el pie para poder ceder los datos de los usuarios a terceros.

Asimismo, WhatsApp no se hace responsable de controlar la información que sea compartida que le pueda causar algún tipo de daño a un tercero, lo cual demuestra la baja diligencia en cuanto a controles que la aplicación debería tener para proteger a sus usuarios de robo o extravío.

Solo para mayores de "edad": Según las condiciones de WhatsApp solo es para personas mayores de 16 años, pero no cuenta con controles para validar que quien autoriza los términos y condiciones sea un mayor de edad y tampoco prevé las condiciones en caso de uso inadecuado de menores de edad. Este riesgo es muy alto,

[5] *Estudio* **(Asociación de Bancos de Bolivia , 2019)**.

debido a que los niños suelen no tener el deber de cuidado necesario por lo que son blanco fácil de vulneración de privacidad ante ciberataques.

Cambio de reglas cuando quiera: WhatsApp puede cambiar sus condiciones de uso cuando desee y en cualquier momento, no importa que sean cambios que les afecte negativamente a los usuarios, en caso de que no estés de acuerdo simplemente debes dejar de usar sus servicios. En este sentido, al no tener un regulador que cuide las espaldas del consumidor controle a la empresa, existe un abuso de poder y los usuarios lo aceptan al no tener otra alternativa.

Borrar Datos transmitidos: Los datos transmitidos por medio de WhatsApp nunca son eliminados de sus servidores, aunque señalen lo contrario, siempre mantienen una copia de esa información, lo único que haces es eliminarla del dispositivo. Al administrarse WhatsApp en la nube, esta información puede ser adquirida en caso de ataque a WhatsApp.

En caso de robo o extravío al usuario: WhatsApp no se hace responsable del mal uso que le den terceros a la aplicación y tampoco genera canales para aviso y bloqueo de cuenta que permitan al usuario estar seguro.

Derechos de Autor: WhatsApp no se hace responsable de información protegida por derechos de autor que sea almacenada en la aplicación, toda responsabilidad y consecuencias recaen sobre el usuario que usa la aplicación.

Recopilación de datos: Esta es una de las más graves, debido a que uno autoriza a WhatsApp para que recopile:

- Información de los números de teléfono de los contactos guardados, y acceso a cualquier información de éstos (nombres, direcciones físicas, correos electrónicos, etc.). En este caso, sí el usuario A no tiene WhatsApp, pero B que lo tiene como contacto si tiene WhatsApp, la empresa podrá acceder a la información de A.

- Información personal del usuario y del dispositivo utilizado.

Restringe liberta de expresión: El usuario acepta (sin darse cuenta o más remedio en caso de necesitar la aplicación) no perjudicar el nombre de WhatsApp en ningún tipo de problema que pueda suceder por medio del cual haya participado el uso de la aplicación.

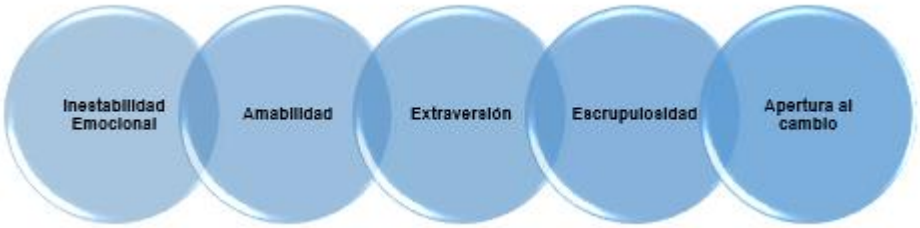
En conclusión, validando un solo documento el cual sirve para afiliarse a un servicio estratégico y que además es parte de Facebook, podemos ver los riesgos respecto a la administración de datos personales a los que se exponen el usuario desprotegido jurídicamente.

b) Caso Cambridge Analytica.

Como es de conocimiento público, el caso de la empresa Cambridge Analytica muestra como ésta se dedicó a promocionar servicios de influencia en redes sociales para incidir en el comportamiento de las personas de cara a que emitan sus votos electorales con cierta tendencia o realizar compras de ciertos productos y servicios en el ciberespacio.

De lo que pudo rescatarse del caso, aparentemente realizaban estas acciones mediante un algoritmo que recolectó las interacciones que los usuarios habían creado en Facebook para interactuar con sus amigos y páginas de su interés, lo cual permitió a esta empresa detectar cinco aspectos básicos para segmentar a cada usuario.

Gráfico 2. Aspectos de segmentación de usuario.



***Fuente: Elaboración propia en base a* (Club Seguridad, 2018).**

Después de un análisis cualitativo y cuantitativo de estos aspectos, realizaron la clasificación de los usuarios por medio de la tipología de su personalidad.

Cuando este tema estalló a nivel internacional, los líderes políticos a nivel mundial quedaron sorprendidos, debido principalmente por las campañas políticas electorales en las que incidieron, logrando al parecer, elegir a un presidente en los Estados Unidos. Se hicieron citaciones al Presidente de Facebook para que compareciera ante el Senado en los Estados Unidos de América debido a la seriedad de las acusaciones que se realizaron en contra de su empresa, toda vez que, se le señaló de vender los datos de sus usuarios para realizar las perfilaciones.

Si nos detenemos en Facebook según CNN Mundo (22 marzo, 2018). *"Qué es Cambridge Analítica. Guía para entender el polémico caso del que todo mundo habla"*[6]*…* puede verse como realizaron la recolección de información de los usuarios que descargaban su aplicación, que ofrecía un test de personalidad y le daba al científico Aleksandr Kogan acceso a sus datos personales y al de sus contactos, según señalan las investigaciones, Kogan traspasó esos datos al grupo SCL y Cambridge Analytica que estaba trabajando para desarrollar técnicas que pudieran ser usadas para influir en los votantes. Facebook dijo que la transferencia de información de Kogan a Cambridge Analytica violó sus reglas. Cambridge Analytica mantiene que borró todos los datos en 2015 cuando supo que las normas de Facebook habían sido violadas.

Por otra parte, para el año 2025 más del 60% de los clientes bancarios a nivel mundial tendrá menos de 35 años y sumado a la encuesta realizada por la empresa Accenture que muestra la tendencia del nuevo cliente, se pueden identificar los pilares principales y las expectativas que las Entidades Financieras deben atender.

[6] *Fuente:* **(Wiener-Bronner, 18)**.

Gráfico 3. Pilares objetivo a ser atendidos por el sector Bancario.

PILAR	DESCRIPCIÓN ENCUESTA
Auto servicio	**61%** de las personas quieren herramientas de transacción sin necesidad de entrar en contacto con nadie.
	50% Quiere herramientas que den acceso directo a monedas digitales.
Expectativas de servicio	**78%** Contrataría servicios bancarios de empresa no financieros – GAFA (Google, Apple, Facebook, Amazon)
	43% Está dispuesto a co-crear productos actuales y futuros de sus bancos por medio de aportaciones on line.
Innovación	**41%** Está muy dispuesto a recibir orientación totalmente generada por computadora para los servicios bancarios.
	45% Usaría los medios sociales para comunicarse con los bancos si fuese más rápido/eficaz.
Personalización	**59%** Quiere herramientas que ayuden a controlar su presupuesto mensual, con ajustes en tiempo real basados en sus gastos.
	54% Quiere ofertas en tiempo real específicas a partir de su ubicación (ejemplo, ofertas basadas en localización y actividades de tarjetas de crédito)

Fuente: Elaboración propia en base a **(Accenture, 2020).**

Finalmente, como se ha podido evidenciar y de acuerdo a lo señalado en el informe de la empresa auditora KPMG respecto a la visión 2020, el riesgo que más ha aumentado en cuanto a ocurrencia es el de Ciberseguridad. Según Akamai Technologies, los ataques cibernéticos y la violación de datos personales se han incrementado un 75% desde 2013, y ese mismo año supusieron un gasto para las empresas solo en España de 12.000 millones de euros.

Frente a estos ataques las empresas deben abandonar las herramientas decimonónicas como los cortafuegos o software antivirus y utilizar medios más avanzados que van desde disfrazar digitalmente los datos más valiosos hasta desviar a los atacantes hasta callejones sin salida.

Añadir que España es el tercer país más castigado por estos ciberataques y que, en la actualidad, han sufrido un déficit en expertos en la materia y las organizaciones requieren cada vez más a personas especializadas en Ciberseguridad. Cabe señalar que no todas las empresas disponen de los recursos propios necesarios para poder contar con un experto en la materia dentro de su plantilla.

Finalmente, es importante que las Entidades Financieras como prestadoras de servicio público básico, asuman de forma consiente su responsabilidad como custodios de información, buscando no solo asegurarse ellos mismos, sino también asegurar los datos de sus clientes, y ser quienes (al igual que el Estado) impulsen campañas de educación y concientización para que tanto los funcionarios que trabajan en la Entidad Financiera como los clientes puedan saber a qué se enfrentan y tomar las precauciones que hoy por hoy son necesarias en el mundo digital a fin de evitar ser víctimas de la ciberdelincuencia.

Las Entidades Financieras deben utilizar sus herramientas y canales digitales de forma segura, transparente y responsable, protegiendo por sobre todas las cosas la información y los datos de sus clientes, debido a que una mala gestión de la seguridad de la información puede ocasionar a la Entidad Financiera pérdidas económicas al ser víctimas de la ciberdelincuencia, teniendo además que asumir la responsabilidad civil y penal que corresponda producto de procesos judiciales de parte de los clientes afectados y/o el Estado mismo, así como de multas y sanciones de parte de los reguladores y por último la pérdida de reputación de la Organización ocasionando así su pérdida de negocio.

De cara a los clientes, deben comprender, el efecto que les ocasionaría la pérdida de sus datos personales, como ser pérdida de dinero, ser víctimas de fraude, suplantación de identidad, extorción.

De cara a los Estados, estos deben sentar las bases de derecho que permitan precautelar los datos e información de sus habitantes, debido a que la información mal administrada y en manos equivocadas puede llegar a ser utilizada inclusive para diseñar campañas (políticas, publicitarias, raciales, sociales etc.) que conduzcan a las personas a tomar ciertas decisiones que impacten en la economía, en la política de un determinado Estado.

2. Marco Teórico: La Ciberseguridad desde el punto doctrinal.

2.1. Conceptos Fundamentales.

2.1.1. Definición de Riesgo:

Su origen etimológico tiende a confundirlo con la palabra peligro (RISK en inglés), por este motivo se dan las siguientes definiciones encontradas que servirán para entender su significado.

Se entiende por Riesgo a:

- "La posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. Y establece que se mide en términos de impacto y probabilidad".

- "La combinación de probabilidad de un evento y su consecuencia".

De ambas definiciones se concluye que, *"el Riesgo es la condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos y el giro de un determinado negocio"*.

Sin embargo, en el mundo financiero, y conforme lo estipulado en el acuerdo de Basilea, se define al riesgo como *"La potencialidad de que eventos, anticipados o no, puedan tener un impacto adverso contra el ingreso y el Patrimonio de una Entidad Financiera"*. [7]

Dentro de la ISO 27000, existen diferentes definiciones que para el presente análisis son muy importantes y estas son:

- **Riesgo residual:** Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.

- **Evaluación de riesgos:** Proceso general de identificación, análisis y evaluación de riesgos.

- **Estimación de riesgos:** Proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una Organización con respecto al riesgo.

- **Tratamiento del riesgo:** Proceso para modificar el riesgo.

[7] **(Comité de Basilea en Supervisión Bancaria, Banco Internacional de Pagos, 2004)**.

2.1.2. Definición de Riesgo Operativo:

El Acuerdo de Basilea II lo entiende… *"como la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el Riesgo Legal, pero excluye el Riesgo Estratégico y el de Reputación"*.

2.1.3. Definición de Ciberespacio:

ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información), y la norma ISO 27032, cláusula 4.21 y 4.22, define el Ciberespacio como*…" el entorno complejo, resultante de la interacción entre las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física"* ...

Debido a que los servicios de aplicaciones en el ciberespacio han adquirido un rol y lugar muy importante en la vida cotidiana, esto se están expandiendo más allá del vínculo empresa-consumidor y de consumidor a consumidor, por lo que está provocando un incremento de amenazas y vulnerabilidades que son el objetivo de los ciberdelincuentes, es así que, hoy por hoy la definición del ciberespacio cuenta con cinco entidades que también deben ser analizadas e identificadas:

a) **Personas:** La Real Academia Española (RAE) inicialmente, la define como…*" Individuo de la especie humana"*, sin embargo, en la actualidad ese concepto se ha extendido e incluso la misma RAE distingue a la persona física (antes definida) y a la persona jurídica como*…" Organización de personas o de personas y de bienes a la que el derecho reconoce capacidad unitaria para ser sujeto de derechos y obligaciones, como las corporaciones, asociaciones, sociedades y fundaciones"*.

b) **Internet:** La RAE lo define como…" *Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación".*

Dentro de esta definición general, se debe señalar la referente al Internet of Things o Internet del Todo (IoT), el cual consiste en que *"tanto personas como objetos puedan conectarse a Internet en cualquier momento y lugar"*[8]*.*

[8] *Fuente:* **(Fundación de la Innovación Bankinter, 2011)**.

Gráfico 4. Internet de las Cosas (IoT).

Fuente: **(Evans & IBSG, 2011).**

c) Software: La RAE lo define como…*" Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora"*.

d) Conexión de dispositivos: Se la define como *"…enlace entre dispositivos con la finalidad de transferir datos, usualmente en ambos sentidos"*[9]*.*

e) Conexión de Redes: Si bien no se trata de un concepto académico de algún autor en específico, de forma empírica, se puede determinar que se trata de una *"Red de comunicación que permite enlazar un gran número de usuarios y compartir los diferentes recursos tecnológicos y de sistema"*.

2.1.4. Definición de Ciberdelincuencia:

De acuerdo a la ISO 27032, cláusula 4.18, se entiende por Ciberdelincuencia a "*la actividad criminal donde los servicios o aplicaciones en el ciberespacio se utilizan o son el blanco de un crimen, o donde el ciberespacio es la fuente, herramienta, destino o el lugar de un crimen".*

Los ataques pueden provenir de diferentes actores. Los diferentes tipos de ataque tienen características como ser:

- Tipo de Blanco u objetivo
- Método de ataque
- Escala de impacto

En la actualidad, las empresas dependen de la tecnología y de proveedores externos para la gestión de su información clave, con más frecuencia, como por ejemplo para almacenar datos confidenciales de sus clientes. Dicha dependencia lleva a las empresas a ser un objetivo vulnerable para los hackers, tanto externos como internos, quienes además pueden tener diferentes motivaciones para querer realizar un cibercrimen, es así

[9] **(ALEGSA, 2019)**.

que a continuación se definirá a un hacker y a los tipos de ciberdelincuentes de acuerdo a lo definido en el diccionario de Ciber Riesgo del Bróker de Seguros Willis Tower Watson:

a) Hacker: *"Persona con extraordinarios conocimientos informáticos, independientemente de si sus fines son legales o ilegales"*. Se dividen en dos tipos:

- Hackers White Hat: encuentran vulnerabilidades en los sistemas y los corrigen.
- Hackers Black Hat: Roba información con fines ilícitos, como la ciber extorsión.

b) Cibercriminales con motivaciones financieras: *"La fuerza motriz detrás de este tipo de atacantes es clara: robar y monetizar información. O lo que es lo mismo: convertir la información en rehén para extorsionar a las empresas a cambio de pagos por su rescate".*

c) Hacktivistas: "*Son ciberdelincuentes que cometen ataques cibernéticos en apoyo a una ideología"*. Su motivación principal es la de sacar a la luz una determinada información política que permanecía oculta para la opinión pública.

Este tipo de ataque, si bien son una forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las organizaciones o sistemas gubernamentales.

A este colectivo se les han atribuido ataques a webs oficiales del gobierno chino, a la web de Justicia británica y al Instituto Tecnológico de Massachusetts, o el robo de un gran número de perfiles de usuario del portal SonyPictures.com en 2011. Pero quizás por el hecho que más se le conoce a nivel mundial es por declarar de forma abierta su "guerra" al Estado Islámico tras los atentados de Charlie Hebdo y Paris en noviembre de 2015. Por ejemplo, publicaron en una web el listado de unos 9.200 tuiteros, supuestamente afines y vinculados a ISIS, así como una guía para 'hackear' el Estado Islámico, además de difundir un vídeo en el que advierten que dirigirán "numerosos ciberataques" a los yihadistas.

A parte de Anonymous no podemos dejar de nombrar a WikiLeaks con su fundador Julian Assange que han hecho públicos informes y documentos con contenido sensible en materia de interés público, o a Snowden que filtró documentos de la CIA.

En conclusión, este tipo de atacantes son sumamente peligrosos para la soberanía y paz en los Estados debido que suelen exponer información confidencialidad que luego puede desatar en guerras a nivel interno (guerra civil), revoluciones e incluso guerras a nivel mundial afectando la vida de millones de personas.

d) Empleados deshonestos: Se trata de empleados a menudo descontentos con su empresa, pueden ser reclutados por la competencia para conseguir información confidencial de la compañía para la que trabajan. Según datos de Willis Towers Watson, los empleados deshonestos son la cuarta causa que más pérdida de

información provoca a las organizaciones, solo por detrás de los hackeos, las brechas de seguridad en los proveedores y la pérdida de ordenadores o móviles.

2.1.5. Definición de Controles:

Gráfico 5. Clasificación de controles según la norma ISO/IEC 27001.

***Fuente: Elaboración Propia en base a* (International Organization for Standardization ISO/IEC 27001 , 2013).**

2.1.6. Definición de Ciberseguridad:

ISACA define la Ciberseguridad como, la *"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados"*.

Para entender el concepto, es necesario definir que debe entenderse cuando se hace referencia a Activos de Información y los Sistemas de información, es así que, de acuerdo a la ISO 27001:

a) Los Activos de información se definen, como "conocimientos o datos que tienen valor para una Organización".

- **Activos físicos:** se definen por la ISO 27032, cláusula 4,39 como *"Activos que tienen una existencia material o tangible"*.
- **Activos Virtuales:** se definen por la ISO 27032, cláusula 4,49 como "*Representación de un activo en el ciberespacio".*
- **Activo Crítico:** se define por la ISO 55000, cláusula 3.2.7 como *"Activo que posee un impacto potencial a significativo en el logro de los objetivos de la Organización".*

b) Los Sistemas de Información se definen como "los que comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma".

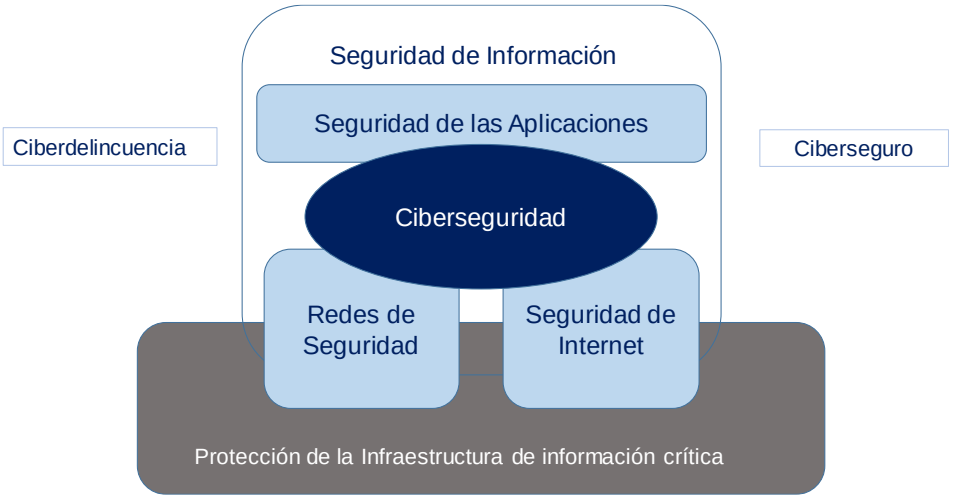
La ISO 27003 en su cláusula 4.20, la define como…" Preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio".

Como se vio en la definición, la Ciberseguridad, incluye la protección de los activos de las amenazas mayormente relacionadas con actividades humanas maliciosas entre otras. Es por este motivo que las unidades a cargo de gestionar la Ciberseguridad, a su vez son responsables de gestionar todos los posibles riesgos que puedan materializarse tomando en cuenta las diferentes amenazas existentes y las propias vulnerabilidades de la Organización. Una vez las unidades a cargo logran identificar los posibles riesgos, deben definir y seleccionar la necesidad y el tipo de controles a implementar, con la finalidad de minimizar la probabilidad de ocurrencia y/o el impacto a un nivel de criticidad lo más bajo que se pueda conforme el apetito de riesgo de la Organización.

Por otro lado, la UIT-T X.1205, Directrices Básicas para la Ciberseguridad, va un poco más allá y señala que La Ciberseguridad es un conjunto de acciones, directrices, políticas, conceptos de seguridad, salvaguardas de seguridad, enfoques de gestión de riesgos, capacitaciones, mejores prácticas, garantías, herramientas y tecnologías que pueden utilizarse para proteger el medio ambiente, las organizaciones cibernéticas y los activos del usuario.

Básicamente para que exista Ciberseguridad, la gestión debe asegurar y realizar mantenimiento de las propiedades de seguridad de la Organización y los activos de los usuarios contra los riesgos significativos identificados en el entorno cibernético.

Cuadro 5. Esquema de dependencia de la Ciberseguridad.



Fuente: **(International Organization for Standardization ISO/IEC 27032, 2012).**

2.1.7. Definición de Seguridad de Información:

Para la ISO 27001, la Seguridad de Información se encarga de…"la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada".

Asimismo, cuenta con distintos componentes para clasificar los activos de información, estos son: Confidencialidad; Integridad, la cual puede incluir la autenticidad y el no

repudio; y Disponibilidad de esta información, sin importar el formato de dichos activos (Digitales, Físicos, audios o videos).

a) Confidencialidad: De acuerdo a la ISO 27000, cláusula 2,12, es "*la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados"*.

b) Integridad: La cláusula 2,40 de la ISO 27000, la define como "*la propiedad de proteger la exactitud e integridad de los activos".*

c) Disponibilidad: La ISO 27000, cláusula 2,9 la define como *"la posibilidad de que el activo sea accesible y utilizable por una entidad o persona autorizada"*.

La cláusula de la ISO 27002, señala que el alcance de la seguridad de información llega a ser optimo cuando se han implementado un conjunto de controles adecuados, que incluyen políticas, procesos, procedimientos, estructuras organizacionales, funciones software y hardware. Dichos controles, deben ser establecidos, implementados, supervisados, revisados y mejorados, en función a la necesidad y evolución de la Organización que lo está gestionando, con el objetivo de garantizar que cumplan los objetivos de negocio y de seguridad.

2.1.7.1. Diferencias entre Seguridad de Información y Ciberseguridad.

Los términos Ciberseguridad y Seguridad de Información en la actualidad son utilizados de forma indistinta, es así que, algunas personas, empresas e incluso expertos en Sistemas utilizan el término "Ciberseguridad" como sinónimo de Seguridad de Información, Seguridad de TI y la gestión de riesgos de la información, de hecho, suelen creer que están implementando la gestión de Ciberseguridad al implementar algunos de mecanismos de seguridad anterior.

A nivel de gobiernos, especialmente los del primer mundo, han adoptado definiciones más técnicas relacionadas a la defensa nacional, incluida la guerra cibernética y la protección de la infraestructura crítica de sus sistemas de defensa y gestión.

Las principales diferencias son:

a) De acuerdo a lo descrito por COBIT 5 para la Seguridad de Información: *"La Ciberseguridad como disciplina al formar parte de la seguridad de Información, está sujeta a su jerarquía a la gestión de Seguridad de la información".*

b) La seguridad de la Información es la entidad madre bajo la cual uno de los factores.

c) Un propósito dos contextos:

- **Seguridad de Información:** Trata con la información, independientemente de su formato, ya sea física o digital.

- **Ciberseguridad:** Se refiere a protección de los activos digitales. Información procesada, almacenada o transportada.

d) Descripción del perfil del encargado de Seguridad de Información versus el de Ciberseguridad.

Cuadro 6. Perfil en Seguridad de Información.

TAREA	CARACTERÍSTICA
Mandato	Responsabilidad total de la gestión de seguridad de información.
Principios operacionales	Reportes e informes al CISO, CEO y unidades de negocios.
Ámbito de control	Aplicaciones e infraestructura de seguridad de información, gestión de accesos, amenazas, riesgos, programas de concientización, métricas.
Toma de decisiones	Facultado para la toma de decisiones respecto a todo el dominio de seguridad de información.
Ciberseguridad	Rendición de cuentas; responsabilidad en pequeña y mediana empresa, delegación a expertos en grandes empresas y entidades financieras.

Fuente: Elaboración propia.

Cuadro 7. Perfil en Ciberseguridad.

TAREA	CARACTERÍSTICA
Mandato	Gestión de Ciberseguridad con responsabilidad global
Principios operacionales	Informes a la gestión de Seguridad de Información.
Ámbito de control	Monitoreo y gestión de Ciberseguridad.
Toma de decisiones	Recomienda e implementa políticas, controles y procesos para la gestión y monitoreo de los riesgos de Ciberseguridad.
Ciberseguridad	Responsabilidad de gestión del riesgo.

Fuente: elaboración propia.

2.1.7.2. Interfaces de Ciberseguridad hacia otras áreas o unidades de la entidad.

Dependiendo el escenario de gobierno de la Organización seleccionados, los gerentes o encargados de seguridad, también deben decidir sobre la responsabilidad y confiabilidad en lo que respecta a la ciberdelincuencia y guerra cibernética.

Cuadro 8. Matriz de cooperación.

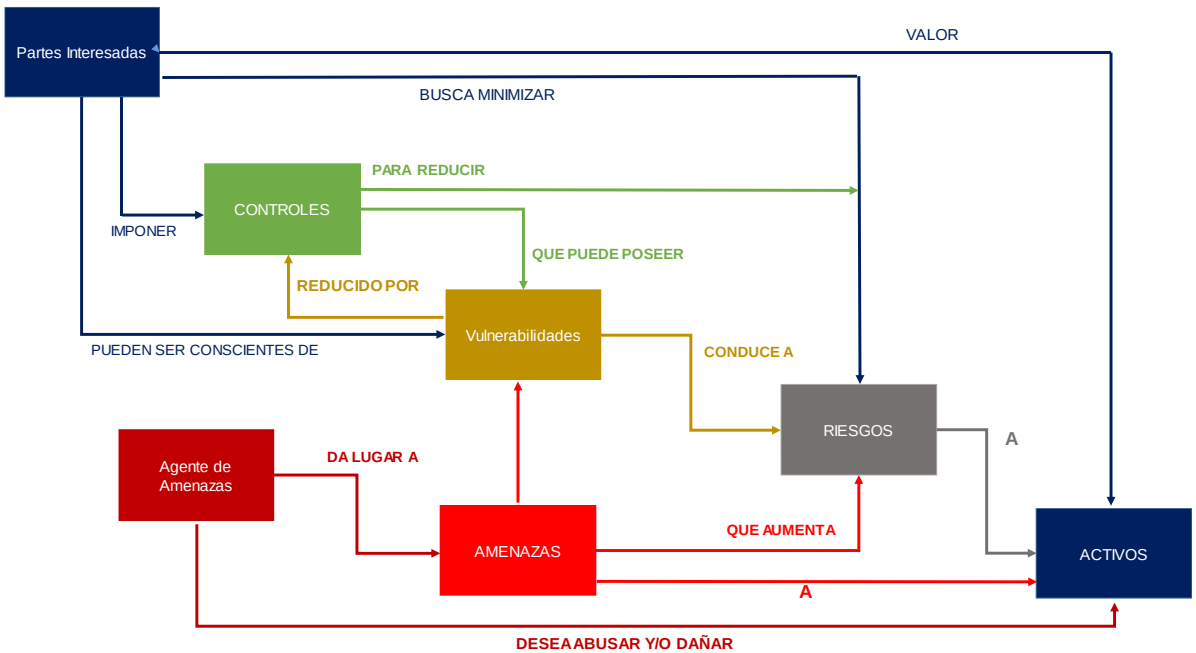
Interfaz de departamento	Áreas de Cooperación
Seguridad Corporativa	Investigación, análisis forense (inicial), aspectos sociales y relacionados con el personal, aplicación de la ley.
Tecnología de la información	Aspectos de arquitectura TI, soluciones de seguridad, controles técnicos (pre-aplicados), gestión de sistemas, gestión de configuración.
Gestión de riesgos	Riesgos vinculados a ciberseguridad, escenarios de amenazas y ataques, relacionados con los riesgos del negocio.
Auditoría Interna	Investigación y Análisis Forense.
Adquisición	Gestión de proveedores y contratación.
Legal	Requisitos externos en ciberseguridad, leyes y regulación local
Usuario Final	Reglas de comportamiento, informes, sugerencias y expectativas del usuario, innovación

Fuente: Elaboración propia.

2.1.7.3. Contexto de Seguridad a nivel general.

Conforme lo señalado en la ISO 27032, cláusula 6.4.2, la seguridad se refiere a la protección de los diferentes activos de amenazas, las cuales se definen como el *"potencial abuso sobre los activos protegidos"*, Si bien todas las categorías de amenazas deben ser consideradas en el dominio de la seguridad, debe prestarse mayor atención a las que se relacionan con la actividad humana y/o maliciosa. En el cuadro 7 puede verse de forma esquemática, cuales son los actores definidos por la ISO 27032 y como interrelacionan en la gestión del riesgo y los controles para buscar su mitigación.

Gráfico 6. Interrelación de los actores de la Ciberseguridad.



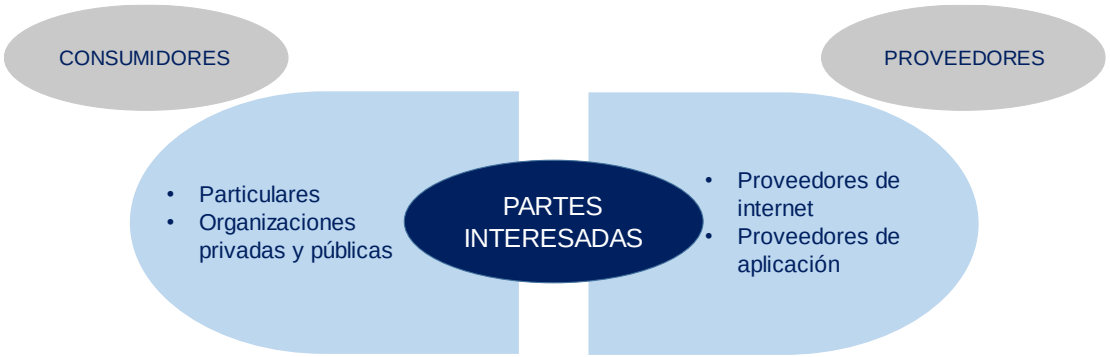
Fuente: **(International Organization for Standardization ISO/IEC 27032, 2012).**

2.1.8. Partes Interesadas:

De acuerdo a la ISO 27032, la cláusula 4.44 establece que. *"son las personas u organizaciones que pueden afectar, ser afectadas, o percibir que está afectada por una decisión o actividad"*, así mismo, la cláusula 4.45, señala que…" *es el individuo u organización que posee un derecho, participación, reclamo o interés en un sistema o en su posesión de características que satisfacen sus necesidades y expectativas"*.

- Las partes interesadas son los responsables de establecer y mantener la seguridad en el ciberespacio, su estructura y entorno, su principal responsabilidad es:
- Definir el valor de los activos de la entidad;
- Percibir las amenazas potenciales;
- Evaluar el riesgo y mitigarlo;
- Seleccionar los controles adecuados para reducir la probabilidad de ser vulnerado y/o su impacto.

Gráfico 7. Diagrama de Stakeholders.



Fuente: **(International Organization for Standardization ISO/IEC 27032, 2012).**

2.1.8.1. Consumidores.

La ISO 27032, cláusula 7,2 los define como…*" usuarios individuales, organizaciones privadas y organizaciones públicas que tienen acceso al ciberespacio".*

La misma norma citada en el punto anterior, pero en su cláusula 4.37, define a la Organización como…*" Grupo de personase infraestructuras con una estructura de responsabilidades, autoridades y relaciones".*

2.1.8.2. Proveedores.

La cláusula 7,3 de la norma ISO 27032, señala que los proveedores pueden ser de servicio de aplicaciones o de servicios de internet, y los define de la siguiente manera:

a) Proveedores de servicio de aplicación: Cláusula 4,3, ISO 27032, los define como, *"Operador que ofrece una solución de software alojada externamente que*

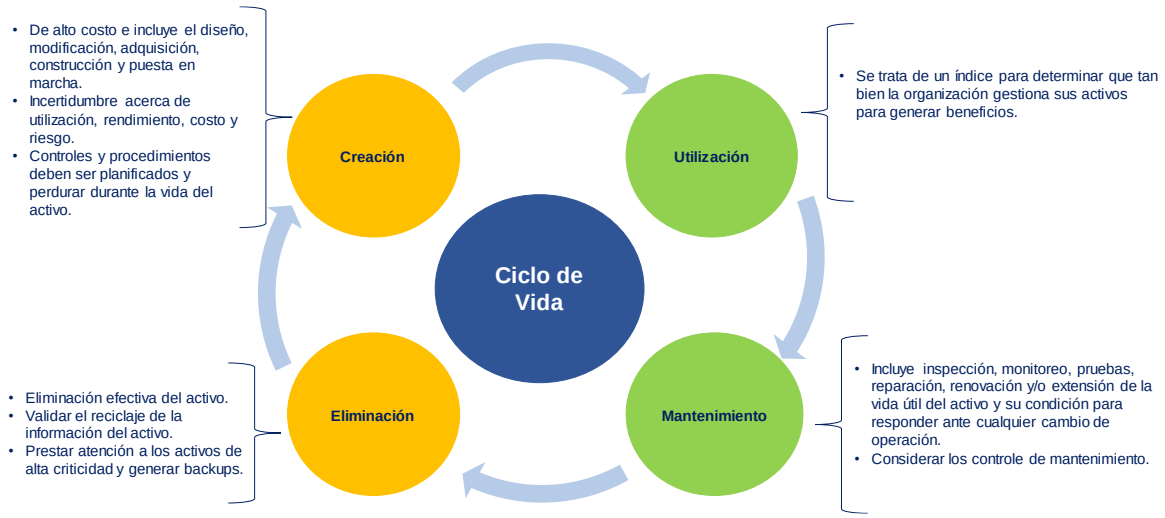
provee servicios de aplicación y que incluyen modelos basados en la web o cliente-servidor".

b) Proveedor de servicio de internet: Cláusula 4,34, ISO 27032, los define como, *"Organización que proporciona servicios de internet a un usuario y le permite a sus clientes acceder a internet".*

2.1.9. Ciclo de vida del Activos:

Al haber definido lo que es Activo de información líneas arriba, se procederá a describir el ciclo de vida por cual tiene que atravesar todo activo desde su creación hasta la eliminación, analizar este ciclo es necesario a fin de buscar incrementar la productividad de una determinada Organización.

Gráfico 8. Ciclo de vida del activo



Fuente: Elaboración propia en base a: **(International Organization for Standardization ISO/IEC 27000, 2014) (International Organization for Standardization ISO/IEC 27032, 2012).**

2.1.10. Vulnerabilidad:

De acuerdo a la norma ISO 27032, cláusula 4,52 y a la ISO 27000, cláusula 2,89, se define como "*La debilidad de un activo o de un control que puede ser explotada por una amenaza".*

La evaluación de las vulnerabilidades debe ser una tarea recurrente y asignada a un área específica que no esté necesariamente vinculada a la unidad que realiza la actividad principal ni al área que ejecuta el control a la anterior, esto con la finalidad de tener una óptica externa y objetiva.

Las vulnerabilidades pueden ser intrínsecas o extrínsecas, las primeras se relacionan a las características propias del activo y las extrínsecas a características de las circunstancias específicas del activo, como ser la probabilidad de inundación del espacio físico donde está ubicado un servidor.

Cuadro 9. Tipología para clasificar las vulnerabilidades (sin ser limitativas).

TIPOS	Ejemplo
HARDWARE	Mantenimiento Insuficiente.
SOFTWARE	Falta de registros de inscripción.
RED	Falta de encriptación para las transferencias.
PERSONAL	Formación insuficiente/Falta de supervisión.
SITIO /UBICACIÓN	Ubicación en zona susceptible a terremoto/Inundación/Incendios.
Estructura de la organización	Falta de segregación de funciones/Falta de descripción de un puesto.

***Fuente: Elaboración propia, basado en anexo D* (International Organization for Standardization ISO/IEC 27005 , 2001).**

2.1.11. Amenazas y Tipos de amenazas:

Por definición una amenaza tiene el potencial de hacer daño a los diferentes tipos de activos, ya sea en información, procesos y sistemas, ocasionando perjuicios a la Organización ya sea en lo económico, reputacional y/o legal.

La ISO 27032, en su cláusula 4,46 la define como *"La causa potencial de un incidente no deseado, que puede resultar en daño a un sistema, individuo u Organización"*.

Las amenazas en el ciberespacio pueden dividirse en dos clases:

a) Amenazas a los activos personales: Robo o enmascaramiento de identidad en línea, acceso no autorizado a información financiera y/o robo de dinero a una persona.

b) Amenazas a los activos organizacionales: En este caso el atacante busca:

- Desfigurar o modificar páginas web;
- Robo de URL;
- Información confidencial revelada, ya sea de empleados, clientes, socios o proveedores;
- Información y datos financieros confidenciales interceptados;
- Acceso no autorizado a información importantes y clasificada de los gobiernos.

El anexo C de las normas ISO 270005, proporciona la tipología expuesta en el cuadro a continuación.

Cuadro 10. Tipología para clasificar las amenazas (sin ser limitativas).

TIPOS	Ejemplo
Daño físico	Fuego/daño por agua
Desastre natural	Terremoto/Inundación
Pérdida de servicios esenciales	Falta de aire acondicionado/Corte de suministro eléctrico
Trastornos causados por radiación	Radiación electromagnética
Información comprometida	Escucha telefónica/ Robo de información, documentos, datos
Fallas técnicas	Falla de equipo/sobrecarga de red.
Acción no autorizada	Acceso no autorizado/Uso de software pirata

Fuente: Elaboración propia, basado en anexo D **(International Organization for Standardization ISO/IEC 27005 , 2001).**

Según el reporte de la firma auditora Ernst & Young realizado en el III Congreso de Gestión de Riesgo Bancario y Gestión de Riesgos Cibernéticos organizado por la Superintendencia de Bancos (SIB) de la Republica Dominicana en 2018, el 77% de las organizaciones, señalan que el punto más obvio de vulnerabilidad provendrá de un empleado descuidado o de un empleado con intenciones maliciosas, el 64%de las organizaciones ven el phishing como la mayor amenaza, y cada vez preocupa más la poca conciencia y comportamiento del usuario.

A continuación, se presenta la evolución de los riesgos y amenazas globales definidos en la norma ISO 270005 y como según el foro económico mundial han ido evolucionando, y por lo tanto el enfoque de gestión de los gobiernos y las organizaciones en general debe también adaptarse a esta nueva realidad.

Cuadro 11. Evolución de los riesgos y amenazas globales.

Fuente: **(Asociación Bancaria y de Entidades Financieras de Colombia, 2019).**

De acuerdo a lo expuesto hasta ahora, las amenazas por Ciberseguridad han ido incrementándose a nivel mundial, tanto en phishing, como en ataques vía programas maliciosos que buscan obtener los datos de personas naturales o jurídicas que conforman la sociedad, ya sea con la intención de robarles dinero, sistemas o vender sus datos a terceros interesados sin su consentimiento.

Las Entidades Financieras y en general las empresas suelen no estar al mismo ritmo de evolución que los atacantes, por lo que es cada vez más importante el contar con una guía referencial que permita a los principales ejecutivos de las entidades financieras y de las empresas en general poder aplicar un plan de gestión de Ciberseguridad, no solo por ayudarlos a gestionar su propia seguridad sino también la de sus clientes, quienes si bien buscan experiencia y agilidad, cada vez crece más la búsqueda y exigencia de seguridad respecto al manejo de la información, por lo que en el corto plazo los clientes también utilizaran como un factor de decisión la capacidad de la compañía de brindar seguridad, respeto y protección a sus datos.

3. Metodologías de Trabajo e Investigación.

Es necesario identificar las normas y guías que serán más útiles para aplicar las mejores prácticas para implementar un programa eficaz de Ciberseguridad, Las normas que existen hoy por respecto a Ciberseguridad pueden aplicarse de forma general a todas las organizaciones, independientemente del tipo de industria, sector o tamaño, es por este motivo qué, en el siguiente capítulo analizaremos los diferentes marcos que serán utilizados para el trabajo de investigación, con la precisión de que si bien está enfocado el trabajo en su aplicación para instituciones bancarias, no es limitativo de cara a otros sectores.

3.1. Marco de Trabajo de Ciberseguridad del NIST (National Institute of Standards and Technology).

El marco del NIST para mejorar la seguridad cibernética de la infraestructura crítica (Marco de seguridad cibernética de NIST o CSF) se publicó originalmente en febrero del 2014, en respuesta a la Orden Ejecutiva Presidencial 13636 para la mejora de la Ciberseguridad de infraestructuras críticas, "Improving Critical Infrastructure Cybersecurity".

El NIST consultó con varios socios del gobierno, la industria y el mundo académico durante más de un año para crear unas directrices y prácticas sólidas y basadas en el consenso. La Ley de mejora de la seguridad cibernética del 2014 reforzó la legitimidad y la autoridad del CSF al codificarlo y convertirse voluntariamente en ley y hasta que la Orden Ejecutiva Presidencial sobre el fortalecimiento de la seguridad cibernética de las redes federales y la infraestructura crítica, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, firmada el 11 de mayo del 2017, obligó a todos los organismos federales de los EE.UU. a utilizar el CSF.

El marco de Ciberseguridad NIST, denominado como “Mejoramiento en la Infraestructura crítica de Ciberseguridad” emitido por el Departamento de Comercio del Instituto Nacional de Estándares y Tecnología, más que introducir nuevas normas o conceptos, busca aprovechar e integrar las prácticas ya desarrolladas de Ciberseguridad por la Organización Internacional de Estandarización (ISO) y la misma NIST.

El marco de referencia es un enfoque basado en el “riesgo” para la gestión del riesgo de Ciberseguridad y puede ser utilizado:

- Parte clave del proceso de gestión de riesgo de Ciberseguridad a fin de prevenir y estar preparados para responder a estos nuevos riesgos cibernéticos.
- Base de un programa de Ciberseguridad nuevo o como mecanismo de mejora para el existente.
- Identificar brechas en las prácticas de Ciberseguridad dentro de la Organización.

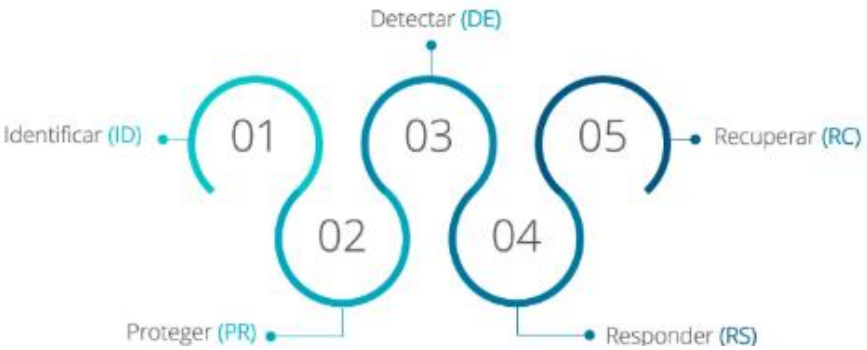
3.1.1. Descripción del marco de referencia.

El marco de referencia del NIST, está compuesto de las siguientes tres partes:

a) Núcleo central del marco de referencia (core).

- Conjunto de actividades de Ciberseguridad, resultados deseados y referencias aplicables, comunes a todos los sectores de infraestructura crítica.
- Presenta los estándares de la industria, guías y prácticas de forma que permite la comunicación desde el nivel ejecutivo hasta el nivel de implementación u operaciones.
- Consta de 5 funciones simultaneas y continuas: Identificación, Protección, Detección respuesta y recuperación.

Gráfico 9. Núcleo central del marco de referencia (core).



Fuente: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

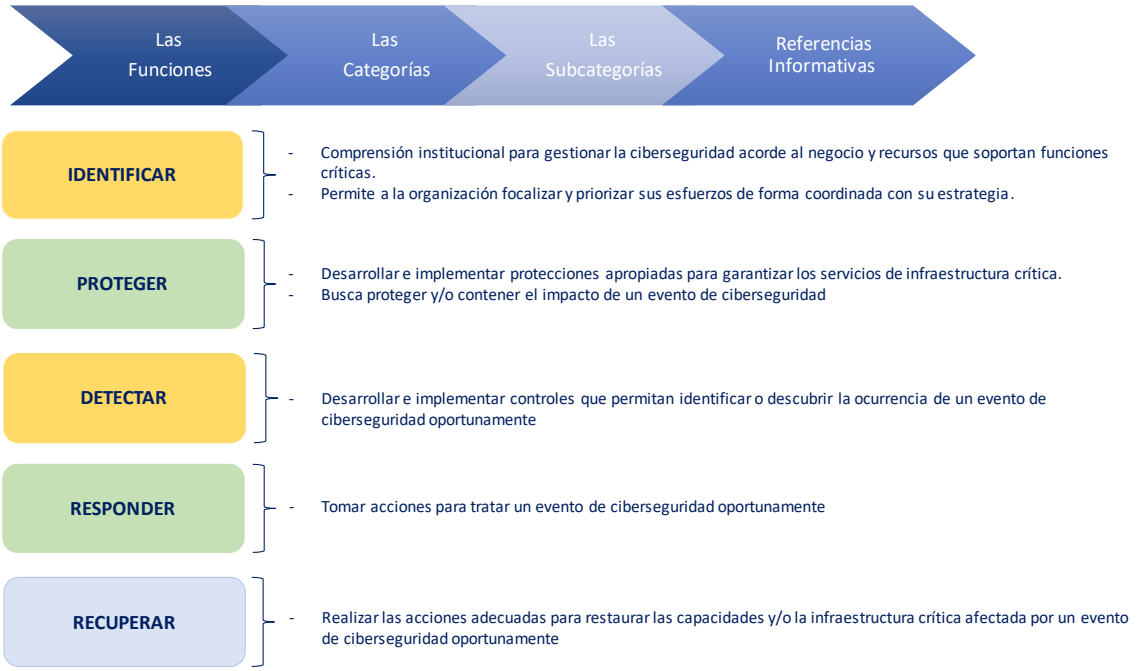
El núcleo permite exponer los resultados clave de Ciberseguridad identificados por la industria como útiles para gestionar el riesgo cibernético, está compuesto de cuatro elementos: funciones, categorías, subcategorías y referencias informativas.

Gráfico 10. Elementos del Núcleo.

Fuente: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

- Las Funciones básicas del nucleo del Marco de referencia y que se definen a continuación, estan destinadas a formar un proceso serial y pueden realizarse simultaneamente para formar una cultura operacional que trate el riesgo de Ciberseguridad:

Gráfico 11. Funciones básicas del nucleo.



Fuente: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

b) Niveles de Implementación del marco de referencia.

Los tiers proporcionan un contexto sobre cómo una institución ve el riesgo de la Ciberseguridad y los procesos implementados para tratarlo. Las escalas describen el grado en que las prácticas de gestión de riesgos cibernéticos de una empresa exhiben las características definidas en el marco. Por ejemplo: riesgo y amenaza, repetible y adaptable.

Los niveles de implementación definen las prácticas de una compañía en un rango que va de parcial hasta adaptativo. Estos “niveles” reflejan una progresión desde respuestas informales y reactivas hasta enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de un tier, la empresa debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio/misión y restricciones de organización.

Cuadro 12. Niveles de control de Implementación.

NIVEL	TIPO	Proceso de gestión de riesgos	Programa de gestión integral de riesgos	Participación externa
1	PARCIAL	No se formalizan prácticas organizativas de gestión de riesgo de ciberseguridad y se gestiona el riesgo ad hoc y de forma reactiva	Se conoce muy poco del riesgo de ciberseguridad en la organización y no se tiene un enfoque de gestión riesgo organizacional	Puede no tener procesos establecidos para participar en la coordinación colaboración con otras entidades
2	RIESGO INFORMADO	Las prácticas de gestión de riesgo son aprobadas por la administración pero no pueden establecerse como políticas en la organización	Se conoce el riesgo de ciberseguridad a nivel de la organización pero no se tiene un enfoque de gestión de riesgo en la organización	La organización conoce su papel en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente
3	REPETIBLE	Las prácticas de gestión de riesgo son formalmente aprobadas y expresadas como políticas de la organización	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad	La organización entiende sus dependencias y socios y recibe información que permite la colaboración y las decisiones de gestión basadas en riesgo
4	ADAPTATIVO	La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos	Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos	La organización gestiona el riesgo y comparte activamente la información con los socios para garantizar que se distribuye información precisa para mejorar la ciberseguridad antes de que se produzca un evento

Fuente: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

c) Perfil de Marco de Referencia.

Representa los resultados basados en las necesidades del negocio que la Organización ha seleccionado desde las categorías y subcategorías del Marco de Referencia. Asimismo, el perfil puede ser caracterizado como el alineamiento de las normas, guías y prácticas respecto al Núcleo Central del Marco de Referencia para un escenario de implementación en particular. Los perfiles pueden utilizarse a su vez para identificar las oportunidades de mejora de cara a la “postura objetivo” versus el “estado actual real” de la Organización.

Finalmente, para desarrollar un perfil de riesgo, la Organización puede examinar todas las categorías y subcategorías en función a los impulsores del negocio y a la evaluación del riesgo, determinando así, la criticidad e importancia.

3.1.2. Pasos para robustecer la Ciberseguridad en función al NIST.

A continuación, se detallan los pasos mediante los cuales una Organización debe trabajar como punto de partida guía de cara a mejorar y robustecer su estructura de gestión del riesgo de Ciberseguridad.

Paso 1: Priorizar y alcance: La Organización una vez identificados sus objetivos de negocio y sus prioridades estratégicas, debe adoptar las decisiones referentes a la implementación de Ciberseguridad y determinar el alcance de los sistemas y activos de información que dan soporte tanto al proceso como a la línea de negocio. De esta forma el marco de Referencia podrá ser adaptado para brindar el soporte correspondiente a las diferentes líneas de negocio y procesos que servirán de apoyo para el cumplimiento de los objetivos de la Organización. Del mismo modo permitirá identificar un apetito de riesgo de la Organización versus el negocio que quiere potenciarse.

Paso 2: Orientar: Una vez que el alcance del programa de Ciberseguridad ha sido determinado por la línea de negocio o proceso, la Organización identifica los sistemas

y activos relacionados, requisitos regulatorios y el enfoque integral del riesgo, para luego identificar las amenazas y vulnerabilidades de los mencionados sistemas y activos, con la finalidad de robustecerlos o cambiarlos.

Paso 3: Crear un perfil actual: La Organización debe desarrollar un perfil actual indicando los resultados de categorías y subcategorías del Núcleo Central del Marco de Referencia (Core) que actualmente se encuentra alcanzado.

Paso 4: Realizar una evaluación de riesgos: Esta evaluación puede ser guiada mediante el proceso de gestión integral de riesgo de cada Organización o bien mediante actividades de evaluación de riesgo previas. La Organización debe analizar el entorno operacional a fin de discernir la probabilidad de ocurrencia de un evento de Ciberseguridad y el impacto que este tendría en el estado de ganancias y pérdidas. En este sentido, es importante que toda Organización busque incorporar los datos de riesgos, amenazas y vulnerabilidades emergentes para facilitar una sólida comprensión de la probabilidad e impacto de materializarse un riesgo de Ciberseguridad.

Paso 5: Crear un perfil objetivo: La Organización crea un perfil objetivo centrado en la evaluación de las categorías y subcategorías del Marco de Referencia y describiendo los resultados de Ciberseguridad deseados por la Organización. Cabe señalar que el Marco de Referencia no es limitativo en cuanto a categorías y subcategorías, por lo que cada Organización puede adaptarlas a su negocio y crear nuevas con la finalidad de considerar riesgos propios de su giro. Así también, puede cada Organización considerar la influencia y requisitos de las partes interesadas externas, como ser clientes, reguladores, socios de negocio y proveedores a momento de crear su perfil objetivo.

Cuadro 13. Categorías de función e identificadores únicos del Marco de Referencia.

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

Paso 6: Determinar, analizar y priorizar las brechas: Toda Organización en este paso, debe comparar su “perfil actual” y el “perfil objetivo” a fin de determinar las brechas, para luego, crear un plan de acción priorizado en función a un análisis costo/beneficio, con la finalidad de identificar los recursos necesarios para tratar cada brecha en función de las actividades de Ciberseguridad, soporte de gestión de riesgo, equipo humano y herramientas de control, estas últimas suelen tener un costo de inversión elevado.

Paso 7: Implementar un plan de acción: La Organización determina que acciones debe tomar para reducir las brechas, definiendo un cronograma con responsables y plazos de entrega de cara a cumplir el perfil objetivo.

3.1.3. Consideraciones.

Como puede verse hasta ahora el Marco de Referencia NIST es un documento madre con principios y marcos generales que permitan a cada Organización adecuarse y robustecer su nivel de control a la Ciberseguridad, sin embargo el autor considera que debe exponerse una segunda herramienta que como Marco de Referencia es más específica de cara a las Entidades Financieras y a entidades que suelen por su naturaleza (Ministerios, ONG´S, Cooperación Internacional) estar más expuestas a los ciberataques dado la cantidad valiosa no solo de recursos económicos sino también de datos e información confidencial de personas e incluso de Estados Nacionales.

3.2. Herramienta de Evaluación de Seguridad Cibernética (FFIEC).

Como bien se mencionó en capítulos anteriores, debido al aumento del volumen y la complejidad de las amenazas informáticas, las instituciones financieras que conforman el Consejo Federal de Examen (FFIEC) desarrolló una Herramienta de Evaluación de la Seguridad Cibernética, para colaborar a las instituciones a identificar sus riesgos y determinar su preparación para la seguridad cibernética. Dicha evaluación proporciona un proceso repetible y medible para las instituciones, con la finalidad de que pueda monitorearse su evolución en la seguridad cibernética.

La evaluación incorpora los principios relacionados con la seguridad cibernética de la FFIEC Tecnología de la Información (IT) Manual de Examen y la orientación normativa y conceptos de otras normas de la industria, como el Instituto Nacional de Estándares y Tecnología (NIST) en su Marco de seguridad, expuesto en el punto anterior.

3.2.1. Beneficios para la Institución.

Las entidades que utilicen este marco de referencia, serán capaces de:

- Identificar factores que contribuyen a determinar el riesgo global y cibernético de la institución.

- Evaluación de la preparación para la seguridad cibernética de la institución y si está alineada con los riesgos de acuerdo a la madurez de su negocio.

- Determinar tanto las prácticas de gestión de riesgos, como los controles necesarios a mejorar o implementar.

3.2.1.1. Proceso de evaluación.

La evaluación consta de dos factores: Perfil de riesgo inherente y Madurez Ciberseguridad. Al término de las dos partes, la dirección puede evaluar si el riesgo inherente y la preparación de la institución están alineados.

a) Perfil de riesgo inherente.

La primera parte de la Evaluación identifica riesgo inherente de la institución. El perfil de riesgo inherente identifica las actividades, servicios y productos organizados en las siguientes categorías:

Tecnologías y tipos de conexión: Determinados tipos de conexiones y tecnologías suponen un riesgo inherente mayor de acuerdo a la complejidad, conexiones, y la naturaleza de productos o servicios tecnológicos. Esta categoría incluye adicionalmente a proveedores de servicios de Internet (ISP) y conexiones de terceros, a los sistemas internos o externos, conexiones no seguras, uso del acceso inalámbrico, dispositivos de red, extensión de servicios en la nube, y el uso de dispositivos personales.

Canales de entrega: Los canales de distribución de productos y servicios suponen también un riesgo inherente mayor, dependiendo de la naturaleza del producto o servicio específico, toda vez el riesgo incrementa en la medida de la variedad y número de canales de distribución disponibles en línea, móviles y en el caso de Entidades Financieras de operaciones en cajeros automáticos (ATM).

Línea / Productos y Servicios Móviles Tecnología: Los diferentes productos y servicios tecnológicos ofrecidos por las instituciones financieras pueden suponer un riesgo inherente mayor en función a la naturaleza del producto o servicio, como ser servicios de pago, como tarjetas de débito y tarjetas de crédito, pagos entre personas naturales o jurídicas, cámaras de compensación automatizada (ACH), transferencias bancarias minoristas y mayoristas, captación de depósitos y remesas, servicios de tesorería, servicios fiduciarios. Esta categoría también incluye la consideración de si la institución ofrece servicios de tecnología a otras organizaciones.

Características de la Organización: En esta categoría se considera las características organizativas, tales como fusiones y adquisiciones, el número de empleados directos y contratistas de seguridad cibernética, los cambios en la dotación de personal de seguridad, el número de usuarios con acceso privilegiado, cambios en la tecnología de la información (TI), la ubicación de la presencia de negocios, y la ubicación de operaciones y datos centros.

Las amenazas externas: El volumen y el tipo de ataques (o intento de éxito) afectan a la exposición al riesgo inherente de una institución. En esta categoría se considera el volumen y la sofisticación de los ataques dirigidos a la institución.

El riesgo inherente incorpora el tipo, volumen y complejidad de las operaciones y las amenazas para la Organización, sin incluir los controles que se tienen para su mitigación. Por otra parte, el perfil de riesgo inherente incluye la descripción de las

actividades que abarca cada categoría. El perfil tiene por objetivo coadyuvar a la dirección a determinar la exposición al riesgo del negocio de la Organización.

Gráfico 12. Evolutivo del perfil riesgo inherente.

Fuente: **(Federal Financial Institutions Examination Council's (FFIEC), 2015).**

Least Inherent Risk: Una institución con un perfil de riesgo inherente "Least" en general tiene un uso muy limitado de la tecnología. Tiene pocas computadoras, aplicaciones, sistemas y conexiones. Su variedad de productos y servicios son limitados.

Minimal Inherent Risk: La institución con un perfil de riesgo inherente "Mínimal" utiliza una complejidad limitada en cuanto a la tecnología. Ofrece una variedad limitada de productos y servicios con un riesgo menor. Los sistemas críticos de la institución se han externalizado y mantiene algunos tipos de conexiones a clientes y terceros con una complejidad limitada.

Moderate Inherent Risk: La institución que tiene un perfil de riesgo inherente "moderate" utiliza tecnología de mayor complejidad en términos de volumen y sofisticación. La institución puede externalizar los sistemas y aplicaciones críticos y también puede soportarlos internamente. Cuenta con mayor variedad de productos y servicios ofrecidos en diferentes canales, expuestos a un riesgo medio.

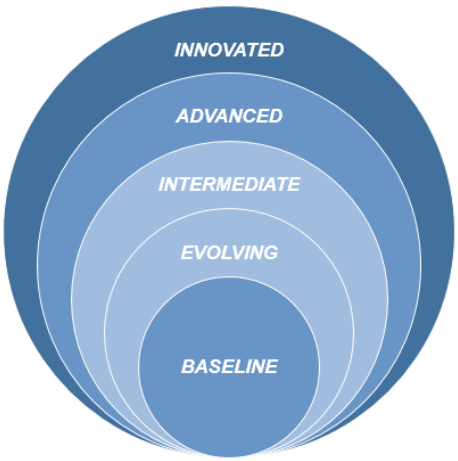
Significant Inherent Risk: Una institución con un perfil de riesgo inherente "significant" utiliza tecnología de mayor complejidad en términos de alcance y sofisticación. La institución ofrece productos de alto riesgo y servicios que pueden incluir tecnologías emergentes. La institución puede albergar un número significativo de aplicaciones internamente. La institución permite interactuar con un gran número de dispositivos personales o una gran variedad de tipos de dispositivos y además mantiene un importante número de conexiones a clientes y terceros. Una gran variedad de servicios de pago se ofrece directamente, en lugar de a través de terceros y puede reflejar un nivel significativo del volumen de transacciones.

Most Inherent Risk: Una institución con un perfil de riesgo Inherente "MOST" utiliza de forma extrema tecnologías complejas en sus productos y servicios. Muchos de los productos y servicios están en el más alto del nivel de riesgo. Utiliza tecnologías nuevas y emergentes a través de múltiples canales de distribución. La institución puede externalizar algunos sistemas o aplicaciones críticos, pero muchos están alojados internamente. La institución mantiene un gran número de tipos de conexión para la transferencia de datos con clientes y terceros.

b) Madurez Ciberseguridad.

Es el segundo factor para la Evaluación de Madurez es la seguridad cibernética, tiene el objetivo de medir la gestión de nivel de riesgo y los controles correspondientes de la institución, cuenta con 5 niveles que empiezan en el Baseline hasta innovador.

Gráfico 13. Evolutivo del nivel de madurez.



Fuente: **(Federal Financial Institutions Examination Council's (FFIEC), 2015).**

Cuadro 14. Definiciones nivel de madurez.

Definición de Niveles de madurez	
Baseline	La madurez de línea de base se caracteriza por expectativas mínimas requeridas por ley, las regulaciones o recomendaciones de la guía de supervisión. Este nivel incluye objetivos a cumplir. La gerencia ha revisado y evaluado la orientación.
Evolving	La madurez en evolución se caracteriza por una formalidad adicional de los procedimientos y políticas documentados que aún no se requieren. Se establecen objetivos basados en el riesgo. La responsabilidad por la ciberseguridad se asigna formalmente y se amplía más allá de la protección de la información del cliente para incorporar activos y sistemas de información.
Intermediate	La madurez intermedia se caracteriza por procesos detallados y formales. Los controles son validados y consistentes. Las prácticas y el análisis de gestión de riesgos están integrados en las estrategias comerciales.
Advanced	La madurez avanzada se caracteriza por prácticas y análisis de ciberseguridad integrados en todas las líneas de negocio. La mayoría de los procesos de gestión de riesgos están automatizados e incluyen la mejora continua del proceso. La responsabilidad de las decisiones de riesgo se asigna formalmente a la primera línea.
Innovative	La madurez innovadora se caracteriza por impulsar la innovación en personas, procesos y tecnología para que la institución y la industria administren los riesgos cibernéticos. Esto puede implicar el desarrollo de nuevos controles, nuevas herramientas o la creación de nuevos grupos de intercambio de información. Los análisis predictivos en tiempo real están vinculados a respuestas automatizadas

Fuente: **(Federal Financial Institutions Examination Council's (FFIEC), 2015).**

La Madurez de la seguridad cibernética incluye los siguientes cinco dominios:

- Gestión de Riesgos y Supervisión de la tecnología;
- Amenaza de Inteligencia y Colaboración;
- Controles de Ciberseguridad;

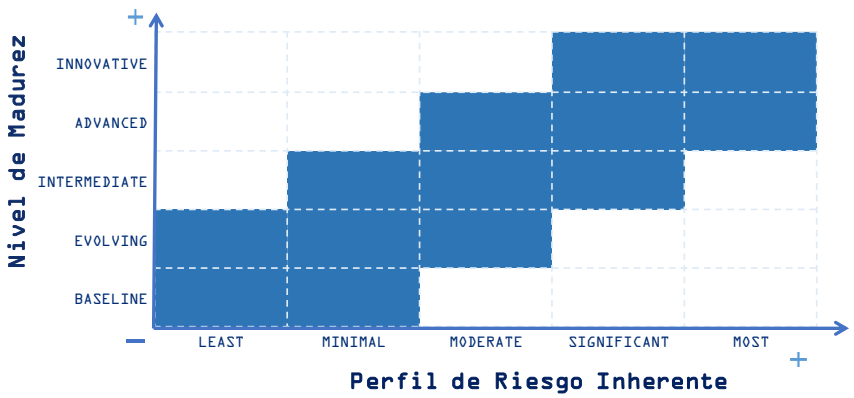
- Gestión de la dependencia externa;
- Gestión de incidentes cibernéticos y resiliencia.

Los diferentes dominios serán desarrollados a profundidad en el siguiente punto, incluyen factores de evaluación y componentes que se complementan y contribuyen a la madurez.

Relación riesgo inherente y Nivel de Madurez:

En la tabla descrita a continuación, se puede observar la relación entre el perfil de riesgo inherente de la Organización y su nivel de madurez de dominio, debido a que no existe un solo nivel de madurez para una institución, toda vez que a medida que el riesgo inherente aumenta, los niveles de madurez deben incrementar. Es así que, las entidades deben evaluar su perfil de riesgo inherente y la madurez de la Ciberseguridad de forma periódica, a fin de identificar si los cambios previstos y requeridos por el negocio y la estrategia pueden afectar a su perfil de riesgo inherente (por ejemplo, el lanzamiento de nuevos productos o servicios, nuevas conexiones).

Gráfico 14. Matriz de medición del nivel de riesgo y madurez.



Fuente: **(Federal Financial Institutions Examination Council's (FFIEC), 2015).**

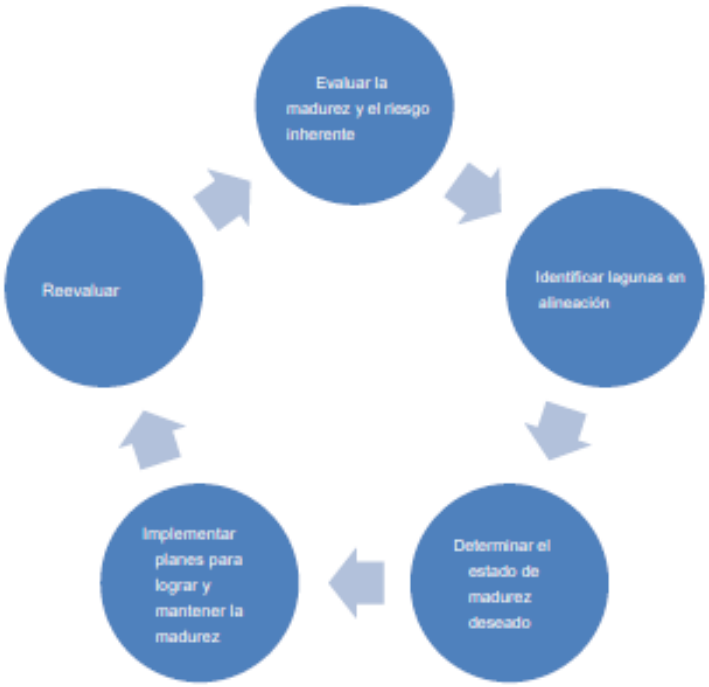
En función a lo expuesto, la Organización podrá identificar si los niveles de madurez que tiene son o no apropiados en relación con su perfil de riesgo inherente y de no ser apropiados los niveles, debe considerar la reducción del riesgo inherente o el desarrollo de planes de acción. Dicho proceso incluye:

- La determinación de los niveles de madurez de destino;
- La realización de un análisis de brecha;
- La priorización y planificación de acciones;
- La implementación de cambios;
- Reevaluación a lo largo del tiempo;
- Comunicación de los resultados.

De esta forma cada Organización podrá establecer los niveles de madurez objetivo para cada dominio o en aquellos dominios que se consideren estratégicos para los objetivos del negocio y/o para su apetito de riesgo.

Finalmente, la Entidad Financiera o cualquier otro tipo Organización que desee utilizar este marco de referencia, deberá realizar un análisis de la brecha entre las corrientes y tendencias del mercado con la finalidad de orientar sus niveles de madurez y así poder realizar planes de acción enfocados en la mejora de sus controles en busca de hacer más eficiente su gestión ya sea para atender un riesgo específico o preparación general para la seguridad cibernética de la Organización.

Gráfico 15. Circuito de gestión de riesgo de Ciberseguridad.



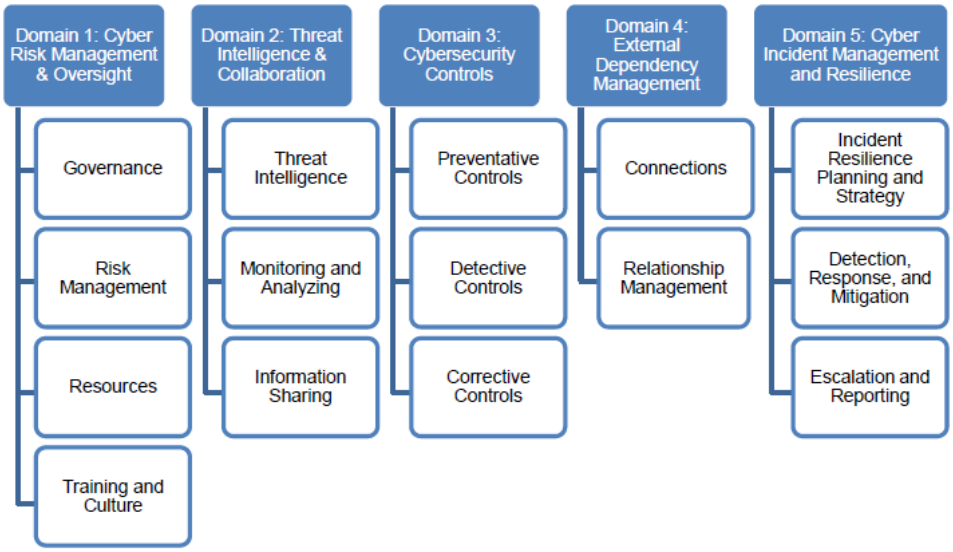
Fuente: **(Federal Financial Institutions Examination Council's (FFIEC), 2015).**

3.2.1.2. Definición de los 5 dominios de la gestión Ciberseguridad.

Como ya se adelantó, una vez se realiza el análisis del perfil de riesgo inherente, la institución debe determinar su nivel de madurez de Ciberseguridad, para cada uno de los dominios mencionados en el punto anterior, es así que, en este apartado, se explicará el significado y el trabajo para cada dominio.

Dentro de cada dominio hay factores de evaluación y componentes contribuyentes. Debajo de cada componente, hay declaraciones que describen una actividad que respalda el factor de evaluación en ese nivel de madurez.

Gráfico 16. Dominios de gestión de Ciberseguridad.



Fuente: **(Federal Financial Institutions Examination Council's (FFIEC), 2015).**

a) Dominio 1: Gestión y supervisión del riesgo cibernético:

La gestión y supervisión del riesgo cibernético aborda el desarrollo y la implementación de un programa eficaz de seguridad cibernética, liderado por el Directorio y a nivel de toda la Organización, definiendo políticas y procedimientos integrales para establecer una responsabilidad y supervisión apropiadas.

Factores de evaluación:

- *Gobierno:* incluye supervisión, estrategias, políticas y gestión de activos de TI para implementar un gobierno efectivo del programa de Ciberseguridad.
- *Gestión de riesgos*: Incluye un programa de gestión del riesgo de Ciberseguridad, que conste de la evaluación de riesgos y una función de auditoría para gestionar eficazmente los riesgos y evaluar la efectividad de los controles clave.
- *Recursos:* Incluyen el presupuesto de personal, herramientas y procesos, con la finalidad de garantizar que el personal de la institución o los recursos externos tengan conocimiento y experiencia acorde con el perfil de riesgo de la institución.
- *Capacitación y cultura*: Incluye la capacitación de los empleados y los programas de concientización del cliente que contribuyen a una cultura organizacional que enfatiza la mitigación de las amenazas de Ciberseguridad.

b) Dominio 2: Inteligencia de amenazas y colaboración:

La inteligencia de amenazas y la colaboración incluyen procesos para descubrir, analizar y comprender de manera efectiva las amenazas cibernéticas, con la capacidad de compartir información internamente y con terceros de forma apropiada.

Factores de evaluación:

- *Inteligencia de amenazas*: Se refiere a la adquisición y análisis de información para identificar, rastrear y predecir capacidades, intenciones y actividades cibernéticas, proponiendo planes de acción para mejorar la toma de decisiones.

- *Monitoreo y análisis:* Se refiere a cómo una institución monitorea las fuentes de amenazas y qué análisis puede realizar para identificarlas.

- *Intercambio de información*: Abarca el establecimiento de relaciones con pares y con foros de intercambio de información, así como el proceso de comunicación sobre amenazas entre estos grupos de forma efectiva y oportuna, así como a los stakeholders de la Organización.

c) Dominio 3: Controles de Ciberseguridad:

Los controles de Ciberseguridad, son en esencia prácticas, y procesos utilizados para proteger los activos, la infraestructura y la información de la Organización. Buscan robustecer la postura defensiva de la institución a través de una protección y un monitoreo continuo y automatizado.

Factores de evaluación:

- *Controles preventivos*: Disuaden y previenen los ataques cibernéticos. Incluyen la gestión de la infraestructura, gestión de acceso, seguridad de dispositivos y puntos finales y la codificación segura.

- *Controles detectivos:* Buscan detectar amenazas y vulnerabilidades, detección de actividad anómala y detección de eventos. Alertan a la institución sobre las irregularidades de la red y del sistema que indican que ha ocurrido o puede ocurrir un incidente.

- *Controles correctivos:* Se utilizan para resolver las vulnerabilidades del sistema y el software a través de la gestión de parches y la solución de problemas identificados durante los escaneos de vulnerabilidades, pruebas de penetración o posterior a un ciberataque real en el peor escenario.

d) Dominio 4: Gestión de dependencia externa:

La gestión de la dependencia externa, implica establecer y mantener un programa integral para supervisar y gestionar las conexiones externas y las relaciones con terceros que tengan accesos a los activos y la información de tecnología de la institución.

Factores de evaluación:

- *Conexiones:* Incorporan la identificación, monitoreo y administración de conexiones externas y flujos de datos a terceros.

- *Gestión de relaciones:* Incluye la debida diligencia, los contratos y el monitoreo continuo para ayudar a garantizar que los controles complementen el programa de seguridad cibernética de la institución.

e) Dominio 5: Gestión de incidentes cibernéticos y resiliencia:

La gestión de incidentes cibernéticos incluye el establecimiento, identificación y análisis de un evento, en busca de priorizar la contención o mitigación de este y escalar la información necesaria a las partes interesadas que correspondan. La resistencia cibernética abarca tanto la planificación como las pruebas para mantener y recuperar las operaciones en curso durante y después de un incidente cibernético.

Factores de evaluación:

- *Planificación y estrategia de resiliencia ante incidentes*: Incorpora la planificación y las pruebas de resiliencia en los planes existentes de continuidad del negocio y recuperación ante desastres para minimizar las interrupciones del servicio y la destrucción o corrupción de datos.

- *Detección, respuesta y mitigación:* Se refiere a los pasos que toma la administración para identificar, priorizar, responder y mitigar los efectos de las amenazas y vulnerabilidades internas y externas.

- *Puesta en conocimiento y reporte: El escalar* y generar informes aseguran que las partes interesadas clave estén informadas de forma oportuna sobre el impacto de los incidentes cibernéticos, y que se notifique de la misma forma a los clientes, Entes reguladores, Policía, seguros y demás entes que sean necesario.

3.3. Análisis Comparativo de los Marcos de Referencia expuestos.

Gráfico 17.Comparativo de Marcos de referencia.

Marco de Trabajo de Ciberseguridad del NIST

- Flexible y adaptable a cualquier tipo de entidad financiera o no.
- Recopila las principales recomendaciones ISO.
- Enfocada en la gestión del riesgo cibernético.
-
- Estructura con tres elementos: Núcleo, Niveles y Perfiles.
  - Núcleo: Conjunto de prácticas de seguridad cibernética, resultados y controles
  - Funciones de gestión de riesgos: Define los pasos de gestión del riesgo: Identificar, Proteger, Detectar, Responder y Recuperar.
  - Perfiles: Sirven para transmitir la seguridad cibernética actual y futura de la empresa.
- Facilita la identificación, priorización y gestión de riesgos de seguridad cibernética.

Herramienta de Evaluación de Seguridad Cibernética (FFIEC)

- Herramienta con enfoque en Entidades Financieras
- Recopila recomendaciones del Marco NIST e ISO
- Herramienta base para la gestión de auditoría y controles de ciberseguridad.
- Estructura con dos factores:
  - El perfil de riesgo inherente identifica las actividades, servicios y productos.
  - Evaluación de Madurez en seguridad cibernética, se distribuye en niveles: Baseline, Evolving, Intermediate, Advanced e Innovated.
- Facilita la identificación de controles y la gestión auditable del proceso integral de ciberseguridad.

***Fuente: Elaboración propia en base a* (National Institute of Standards and Techonology U.S. Department of Commerce, 2019) (Federal Financial Institutions Examination Council's (FFIEC), 2015).**

En conclusión, puede verse como existen diferentes herramientas y marcos de referencia como el NIST que se puede aplicar a todo nivel y no solo el financiero, y el FFIEC que se enfoca más en el sector financiero. En este sentido, se utilizará para el presente estudio el marco de referencia del NIST debido a que este marco está enfocado en la gestión del riesgo de Ciberseguridad y su tratamiento a nivel Entidades Financieras, mientas que el FFIEC será una buena elección en trabajos que se enfoquen en la implementación de guías de incorporación de controles de Ciberseguridad que son necesarios para el proceso integral de Ciberseguridad.

4. Regulación y Avances de la Ciberseguridad.

El presente capítulo tiene por objetivo, mostrar en tres países diferentes de América Latina, la evolución de la Ciberseguridad desde el punto de vista de la regulación y finalmente comparar su situación con la de países del primer mundo como España, dicho análisis será llevado adelante en función a los siguientes factores:

- Existencia de normas básicas de seguridad de información;
- Directrices mínimas que deben cumplirse en el campo financiero para contar con una gestión del riesgo de Ciberseguridad;
- Identificar si los diferentes gobiernos han puesto interés o no en este tema de forma integral, emitiendo normativas que vayan en busca de la protección de datos de todos sus habitantes (Naturales y Jurídicos) y de las diferentes carteras de gobierno.

Los países seleccionados para el análisis son a nivel América Latina Colombia, Chile y Bolivia. La selección de estos países se hace debido a sus características similares, en cuanto a la regulación, evolución y desarrollo tecnológico del país y en especial en el sector financiero, además del idioma y cultura.

4.1. Colombia.

4.1.1. Gobierno:

El Gobierno Colombiano en los últimos años, ha avanzado en el establecimiento de una política pública de Ciberseguridad y en el fortalecimiento institucional. Sin embargo, debido a los enormes impactos que podría tener un incidente cibernético en términos monetarios, pérdida de información y amenaza sobre la reputación, las instituciones públicas y privadas se encuentran trabajando de forma coordinada en el fortalecimiento de sus capacidades para anticiparse a las ciberamenazas.

El Gobierno ha trabajado en el diseño e implementación de estrategias de Ciberseguridad nacional integral, en 2011 se aprobó el CONPES 3701, el cual definió la política pública orientada a fortalecer las capacidades del Estado en Ciberseguridad y establecer espacios y mecanismos de articulación de las diferentes instituciones estatales y privadas en este sentido. En dicha política se establecieron tres objetivos:

- Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regularlos incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la Ciberseguridad y ciber defensa nacional.

- Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciber defensa y ciber seguridad nacional.

- Fortalecer la legislación en materia de Ciberseguridad y ciber defensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática como ser el Convenio de Cibercrimen de Budapest, del cual Colombia participa como invitado.

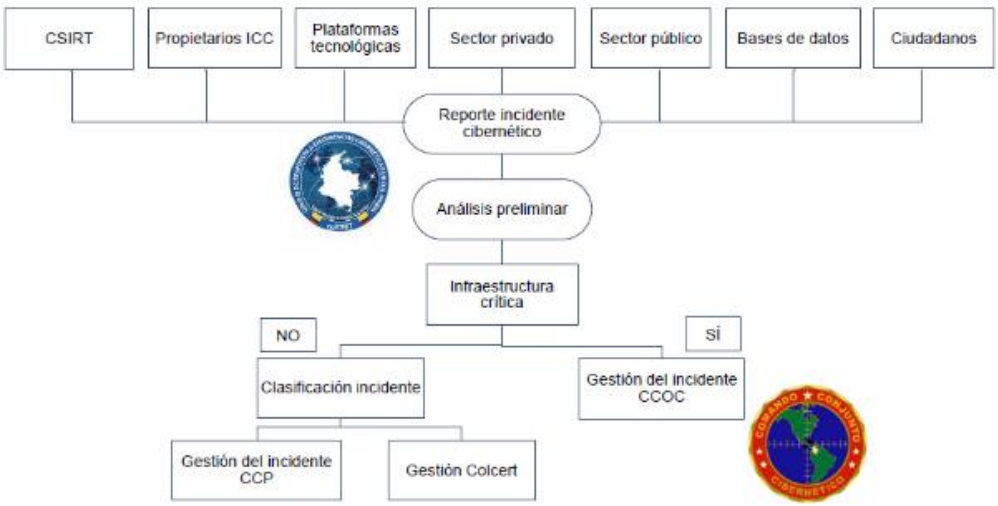
En el año 2016 el Gobierno actualizó la política de Ciberseguridad CONPES emitiendo un nuevo documento, el “CONPES 3854” vigente hasta la fecha, el cual buscó diseñar estrategias de colaboración, donde se comparten responsabilidades para reorientar la política nacional en torno a 5 dimensiones estratégicas:

- Gobernanza de la seguridad digital;
- Marco legal y regulatorio de la seguridad digital;
- Fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital;
- Cultura ciudadana;
- Gestión de riesgos de seguridad digital.

Esta última dimensión es quizás el mayor avance entre los dos documentos de política pública. Cambiar el enfoque hacia uno de gestión de riesgos como uno de los elementos más importantes para abordar la seguridad digital, siendo parte principal de su estrategia el fortalecer las capacidades de las múltiples partes interesadas, para Identificar, Gestionar, Tratar, Mitigar los riesgos de seguridad digital.

El Ministerio de Tecnología y las Comunicaciones ha trabajado en la implementación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés), denominado Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT, el cual tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Gráfico 18. Estructura del modelo de Gestión de Incidentes de Colombia:



Fuente: **(Asociación Bancaria y de Entidades Financieras de Colombia, 2018).**

4.1.2. Marco Legal Nacional:

4.1.2.1. Ley 527: Comercio Electrónico:

En agosto de 1999 nace la Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.

Dentro de los contenidos y los asuntos que regula la presente norma, se encuentran los requisitos jurídicos de los mensajes de datos, comunicación de los mensajes de datos, comercio electrónico en materia de transporte de mercancías, firmas digitales, certificados digitales, entidades de certificación, suscriptores de firmas digitales y funciones de la Superintendencia de Industria y Comercio.

La presente Ley, tiene como principal objetivo otorgar seguridad jurídica a las transacciones electrónicas, a través del reconocimiento jurídico de los mensajes de datos, determinando que no se negarán efectos legales, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos, y en consecuencia admitir los mensajes de datos como medios de prueba, con la misma fuerza probatoria que tienen los documentos previstos en el Código de Procedimiento Civil.

Finalmente, la ley presume: 1) Cuando se hace uso de una firma digital en un mensaje de datos, el suscriptor tiene la intención de acreditar ese mensaje de datos como suyo y de ser vinculado con el contenido del mismo; 2) La firma digital tendrá la misma fuerza y efectos que una firma manuscrita, siempre que cumpla con los requisitos previstos en el parágrafo del artículo 28 de la ley 527 de 1999; 3) Señala de forma clara que cuando una norma exija que la información conste por escrito, este requisito queda satisfecho con un mensaje de datos, siempre que la información sea accesible para posterior consulta.

En cuanto a las entidades de certificación, se crean como aquellas personas facultadas conforme a la ley, para emitir certificados en relación con las firmas digitales, así como ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, entre otros posibles servicios que permita la tecnología.

4.1.2.2. Ley 1581 de 2012 Protección de Datos Personales:

La ley de protección de datos personales 1581 del año 2012, complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

En este sentido define dato personal como “cualquier *información vinculada o que pueda asociarse a una o varias personas naturales que, dependiendo de su grado de utilización y acercamiento con la intimidad de las personas podrá ser pública, semiprivada o privada”*.

La presente Ley, determina que la entidad administrativa encargada de velar por el cumplimiento de las normas sobre protección de datos personales es la Superintendencia de Industria y Comercio (SIC), a través de la Delegatura para la Protección de Datos Personales.

El registro nacional de bases de datos es el directorio público administrado por la SIC en donde reposarán todas las bases de datos y archivos, con sus correspondientes Políticas de Tratamiento, sujetas a la aplicación de las normas sobre protección de datos personales.

4.1.3. Sector Financiero.

En cuanto al sector financiero y de acuerdo a diferentes declaraciones de realizadas por la Asociación de Bancos de Colombia (ASOBANCARIA) este sector es uno de los que más invierte en materia de protección de los datos y sistemas de información, además de haber incorporado, prácticas para la gestión de la Ciberseguridad y seguridad de la información.

Independientemente a las normas de Seguridad de Información que emite la Superintendencia, en 2018, se publicó la CIRCULAR EXTERNA 007 que busca *"impartir instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de Ciberseguridad"*, dicha normativa señala:

- Conceptos básicos de Ciberseguridad;
- Incluye el enfoque de riesgos frente a los temas de Ciberseguridad y seguridad de la información;
- Ascenso de las responsabilidades de aprobar y monitorear las acciones por parte de los mayores órganos de dirección;
- Lineamientos mínimos necesarios para la gestión del riesgo de Ciberseguridad en entidades financieras, desde el gobierno corporativo, gestión y cultura en la Organización;
- Define las siguientes etapas de la gestión en línea con las recomendaciones otorgadas por el Marco NIST y por la FFIEC expuestos en capítulos anteriores: Prevención, Protección y detección, Respuesta y comunicación, Recuperación y aprendizaje.

La mencionada Circular Externa 007, se expidió tomando en cuenta el auge de la digitalización de los servicios financieros, la mayor interconectividad de los agentes y la masificación en el uso de canales electrónicos y busca complementar las normas existentes respecto a los riesgos operativos y la seguridad de la información. En detalle, la circular establece:

- Obligatoriedad de informar a los consumidores financieros sobre los incidentes cibernéticos que se hayan presentado y en los que se vieran afectadas la confidencialidad o integridad de su información y las medidas adoptadas para solucionar la situación.

- La conformación de una unidad que gestione los riesgos de seguridad de la información y la Ciberseguridad. En este aspecto, es importante la actualización constante sobre nuevas modalidades de ciberataques, por lo que deben realizarse capacitaciones periódicas a los funcionarios en Ciberseguridad.

- Las entidades deben contar con una estrategia de comunicación e información para el envío de reportes a las autoridades.

- Incluir en el plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de un ataque cibernético.

Finalmente, señalar que bajo el paraguas de la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, a partir de 2019, se ha puesto en marcha el equipo de respuesta a incidentes sectorial denominado CSIRT Financiero, el cual beneficia a todas las entidades fortaleciendo su capacidad de anticipar, contener y mitigar los riesgos de Ciberseguridad.

4.2. Chile.

4.2.1 Gobierno:

El programa elaborado por el Gobierno de Chile 2018-2022, considera el desarrollo de una estrategia de seguridad digital, denominada “Política Nacional de Ciberseguridad”, la cual tiene la misión de proteger a los usuarios privados y públicos, y a la privacidad de su información y datos. La política describe los siguientes ejes de trabajo:

Eje infraestructura de la información:

Definición de un enfoque de gestión de riesgo, identificación de las infraestructuras críticas de la información, creación de mecanismos de reportes de incidentes, definición de requisitos y estándares de seguridad, la definición de medidas para enfrentar un incidente y el diseño de planes de contingencia en Ciberseguridad.

Eje prevención, persecución y sanción del cibercrimen:

- Definición de capacidades de levantamiento, estandarización e integración de datos e información relacionados con los ciberdelitos.

- Determinación de los desafíos en los ámbitos de prevención, detección y sanción de delitos.

- Incrementar la capacidad de investigación y generación de evidencia en el cibercrimen.

- Diseñar mecanismos de resguardo de derechos fundamentales en la prevención, persecución y sanción de la ciberdelincuencia.

Eje sensibilización, formación y difusión en Ciberseguridad:

- Promoción de una cultura de Ciberseguridad a nivel escolar, universitario y en todos los sectores sociales privados y públicos de la sociedad.

- Fomentar la investigación y desarrollo para la seguridad en el ciberespacio orientada a generar capacidad tecnológica propia, de acuerdo a las necesidades nacionales.

- Generar y promocionar programas de capacitación, educación y formación profesional a nivel de pre y posgrado en materia de Ciberseguridad.

Eje cooperación y relaciones internacionales:

Promover la postura de Chile a nivel internacional e impulsar la cooperación con otros países.

Eje desarrollo industrial y productivo en Ciberseguridad:

Busca identificar los desafíos para la industria nacional e impulsar los mecanismos que permitan incentivar el crecimiento de la industria nacional de Ciberseguridad.

Eje institucionalidad de la Ciberseguridad:

- Revisión del sistema nacional vinculado a la Ciberseguridad, definir roles, atribuciones y competencias de los actores identificados, impulsar el mecanismo de intercambio de información.

- Creación de una alianza público-privada para la seguridad.

- Aumentar la capacidad nacional de respuesta a incidentes y potenciar los equipos de Respuesta ante Emergencias Informáticas (CSIRTs, en inglés).

En función al documento antes descrito, a través del Decreto Supremo 533 de abril de 2015, se creó el Comité Interministerial sobre Ciberseguridad (CICS) de Chile, el cual tiene la misión principal de *"proponer una Política Nacional de Ciberseguridad"*, dicho Comité, está integrado por representantes permanentes e invitados de las siguientes instituciones del gobierno central de Chile:

- Subsecretaría del Interior;

- Subsecretaría de Defensa;

- Subsecretaría de Relaciones Exteriores;

- Subsecretaría General de la Presidencia;

- Subsecretaría de Justicia;

- Subsecretaría de Economía;

- Subsecretaría de Telecomunicaciones;

- Agencia Nacional de Inteligencia;
- Subsecretaría de Hacienda, en calidad de invitado.

El CICS está presidido por un representante de la Subsecretaría del Interior, a su vez, el Comité cuenta con una secretaría ejecutiva, a cargo de un profesional designado por la Subsecretaría de Defensa.

El Comité trabajó en torno a seis ejes temáticos, que sirvieron de base para la definición de objetivos estratégicos en la política: 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. La discusión sobre estos ejes, además, permitieron fundamentar y orientar las medidas específicas contempladas en la Política Nacional de Ciberseguridad.

Un hito fundamental, es la formalización a través de la Resolución Exenta 5.006 del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), como un Departamento dentro de la estructura del gobierno, específicamente en la Subsecretaría del Interior y Seguridad Pública.

El CSIRT, busca fortalecer y promover buenas prácticas, políticas, leyes, reglamentos, protocolos y estándares de Ciberseguridad en los órganos de la Administración del Estado, las Infraestructuras Críticas del país en su conjunto, esta entidad está constituida por los Ministerios, las Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley.

Para el caso del sector privado, se integra a la cobertura en la medida que pertenezca a sectores estratégicos o se haya establecido un convenio de colaboración público-privado.

4.2.2 Marco Legal Nacional:

La reforma a la Ley 19.628 sobre *Protección de la vida privada* busca actualizar la normativa en materia de control de datos. Actualmente, esta reforma se encuentra en primer trámite constitucional, habiéndose aprobado en general en el Senado de la República. Sin embargo, a la fecha aún están en discusión y aprobación algunos artículos en el Senado.

Desde el punto de vista de reglamentación normativa vigente para la protección de datos en Chile, existen 2 áreas del sistema jurídico que son particularmente relevantes, por lo que es necesario exponerlas y explicar cómo interactúan entre sí:

1) La legislación Procesal Penal: En Chile (al igual que en el resto de legislaciones, con base en el Código Napoleónico Francés) la ley contempla la posibilidad de obtener información personal en la investigación de ciertos delitos, mediante mecanismos que incluyen la interceptación y registro de comunicaciones privadas. Estas disposiciones se encuentran en el Código Procesal Penal chileno y en

algunas leyes especiales que rigen por materia sectorial, por ejemplo, la Tributaria, investigación del tráfico de sustancias ilícitas y de acciones terroristas. Esta información debe ser autorizada previamente por orden jurisdiccional a solicitud del Ministerio Público, órgano a cargo de la investigación y persecución criminal.

2) Ley 19.628. Protección de datos de carácter personal de 1999: Ha sido un blanco de críticas desde el comienzo, por contar con una regulación poco proteccionista con las personas naturales que entregan sus datos, debido a que no provee una reglamentación que permita dar cuerpo a un marco adecuado de fiscalización, reclamación, sanción y compensación.

   La simpleza de la normativa deja un vacío legal respecto al tratamiento de datos para la transferencia comercial por sobre los derechos de los individuos, debido a que no contempla una autoridad de control que vele por la protección de datos (local y transfronterizo) personales.

4.2.2.1 Proyecto de Reforma Ley 19.628. Protección de datos de carácter personal:

Busca reforzar la idea de que los datos personales deben estar bajo la esfera de control de su titular, buscando su protección y asegurando estándares de transparencia y seguridad, basándose en los principios de la proporcionalidad, finalidad, seguridad, responsabilidad e información. Asimismo, las principales novedades del Proyecto consisten en la regulación del consentimiento, las responsabilidades de los responsables de datos, las categorías especiales de datos personales y la creación de la agencia de protección de datos personales.

Finalmente, de cara al marco legal chileno, actualmente se encuentran atravesando el proceso correspondiente de aprobación los siguientes cuerpos normativos de acuerdo a lo señalado por el Asesor Presidencial de Ciberseguridad.

Cuadro 15. Proyectos de Ley en curso.

Nombre iniciativa	Estado de Avance
Proyecto de Ley sobre Delitos Informáticos (adecuación al Convenio de Budapest, sobre Ciberdelincuencia)	Se encuentra en primer trámite constitucional (Comisión de Seguridad Pública, Senado).
Proyecto de Ley Marco de Ciberseguridad	Se encuentra en proceso de validación interna (Ejecutivo).
Proyecto de Infraestructuras Críticas	Se incorpora la materia en el Proyecto de Ley Marco de Ciberseguridad.

Fuente: Elaboración Propia en base a: **(Comité Interministerial sobre Ciberseguridad Política Nacional de Ciberseguridad, 2018).**

Cuadro 16. Proyectos de Reglamento en curso.

Nombre iniciativa	Estado de Avance
Decreto Nº 533, 2015, Ministerio del Interior y Seguridad Pública (Crea el Comité Interministerial de Ciberseguridad)	Se encuentra en revisión de la División Jurídica Segpres, dentro de las próximas semanas se presentará ante Contraloría General de la República
Decreto Nº 83, 2004, Ministerio Secretaria General de la Presidencia (Seguridad de la Información)	Se realizará una actualización para que esté acorde a la Norma ISO 27.001 (activos de la información). Se encuentra en proceso de validación interno
Decreto Nº 1, 2015, Ministerio Secretaria General de la Presidencia (Norma Técnica sobre Sistemas y Sitios web de los órganos de la Administración del Estado)	Se encuentra en revisión las modificaciones. Se espera presentar dentro de las próximas semanas las modificaciones ante la Contraloría General de la República.
Decreto Nº 93, 2006, Ministerio Secretaria General de la Presidencia (Norma técnica para la adopción de medidas destinadas para minimizar los efectivos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios).	Se encuentra en revisión las modificaciones. Se espera presentar dentro de las próximas semanas las modificaciones ante la Contraloría General de la República

Fuente: Elaboración Propia en base a: **(Comité Interministerial sobre Ciberseguridad Política Nacional de Ciberseguridad, 2018).**

4.2.3 Sector Financiero:

Independientemente de las normas relacionadas a la Seguridad de Información, la Superintendencia de Bancos y Entidades Financieras de Chile (SBIF) a través de su circular 2.633. de enero de 2018 emitió los lineamientos mínimos que deben ser considerados por las instituciones a fin de gestionar la seguridad de sus activos de información sujetos a riesgos en el ciberespacio. Las exigencias son de manera general:

- Las instituciones financieras deben definir, identificar y gestionar los principales activos de información y de la infraestructura física que soporta y resguarda su seguridad y realizar pruebas para detectar amenazas y vulnerabilidades sobre sus sistemas.

- Gestionar la seguridad de los activos de información expuestos a riesgos en el ciberespacio, y contar con un inventario de activos claramente identificados.

- Establece la necesidad de contar con políticas y procedimientos y con un programa de cultura a nivel de toda la Organización.

- Información y comunicación de incidentes operacionales relevantes y base de datos de incidentes de Ciberseguridad.

Posteriormente, a través de la circular 3.640 de agosto de 2018, se realizaron las siguientes adecuaciones:

- Precisiones a los conceptos de incidentes operacionales, su plazo (30 minutos de conocido el hecho para remitir antecedentes iniciales) y forma de reporte al regulador.

- Establece la obligación de designar un encargado de nivel ejecutivo para establecer comunicación con la SBIF y la asignación de un número único, con la finalidad de hacerle seguimiento hasta su conclusión.

- Define el tipo de información a ser proporcionada a clientes y al sistema financiero.

- De cara al Sistema financiero, establece la obligación de mantener un sistema de alerta de incidentes de Ciberseguridad, con la finalidad de compartir información entre bancos, para que se tomen los resguardos pertinentes para la detección, respuesta y recuperación de sus servicios.

- Establece las obligaciones de las Entidades Financieras de contar con una base de incidentes y de comunicar al directorio los mismos, se hayan o no materializado. Además de ser esta base la que alimenta el criterio de pruebas anuales de los sistemas.

4.3. Bolivia.

4.3.1 Gobierno y Marco Legal:

El Gobierno Boliviano, lamentablemente a la fecha no ha puesto su interés real en generar una política gubernamental de cara a la gestión integral de la Ciberseguridad. Es así que, se ha protegido de manera ineficiente este derecho, hasta su inclusión en la reforma constitucional en su artículo 21.2 y 130, del cual el primero refiere a los derechos civiles, especificando la privacidad, intimidad, honra, honor, propia imagen y dignidad, y el segundo, crea la Acción de Protección de la Privacidad.

Posteriormente, con la sanción de la Ley No. 164 de Telecomunicaciones, Tecnologías de Información y comunicación se empieza a crear un marco legal que describe los derechos y obligaciones de los proveedores de tecnología, y entre ellos el manejo de la información y la inviolabilidad de la privacidad de la información personal, el correo electrónico, la firma digital, entre otros. Durante los años previos a la reforma constitucional, dos eventos marcaron cierto avance en este tema: la sentencia constitucional 0965/2004-R de junio de 2004 donde se menciona a los datos sensibles y a las personas jurídicas y la ley del 2005 sobre acceso a la información.

Por otra parte, la modificación al artículo 79 de la Ley del Órgano Electoral que permite interactuar el Servicio de Registro Cívico (SERECI) con el Servicio General de Identificación (SEGIP) contiene disposiciones sobre la seguridad de los datos personales y permite a los ciudadanos poder consultar los datos personales almacenados para autenticar y validar la información. Finalmente, la reciente Ley de ciudadanía digital en su Artículo 12 dispone el tratamiento de los datos personales se debe limitar a la finalidad que establece la ley, limitando así estos derechos y obligaciones a interacción de las personas con las entidades públicas y privadas que presten servicios públicos delegados por el Estado.

Este conjunto de normas permite crear un marco regulatorio que **no es suficiente**, al no existir una visión integral y tampoco mecanismos de seguridad, por lo que la labor del Gobierno Boliviano en esta materia, es no solo alcanzar el desarrollo de sus pares en la región, sino también brindar la seguridad jurídica y operativa necesaria a sus ciudadanos que cada vez se encuentran más expuestos y vulnerables a ser víctimas de ataques cibernéticos.

Cabe señalar que el Gobierno de forma muy individualista, ha dado una primera señal en busca de gestionar la Ciberseguridad a través de la creación de la Agencia de Gobierno

Electrónico y Tecnologías de Información y Comunicación, mediante Decreto Supremo 2514, el cual también crea Centro de Gestión de Incidentes Informáticos (CGII).

El Centro de Gestión de Incidentes Informáticos (CGII), tiene la misión de establecer lineamientos para la protección de activos de información críticos del Estado y promover la conciencia en seguridad, para prevenir y responder a incidentes de seguridad, si bien su comunidad objetivo alcanza a todo el país, por ahora tratará primero de coordinar con responsables de seguridad de la información (RSI) y equipos de seguridad tecnológicas y los equipos de respuesta a incidentes de seguridad informática (CSIRT) de las instituciones públicas.

En conclusión, cada vez se hace más necesario gestionar la Ciberseguridad desde el Gobierno Boliviano a través de una *Política Nacional De Ciberseguridad* donde que defina una estrategia de desarrollo con plazos específicos para implementar aspectos, como ser:

- La protección del estado hacia la identidad digital de las personas naturales y jurídicas contra ataques informativos de diferente naturaleza.
- El reforzamiento de una unidad de prevención, apoyo y mitigación contra ataques informáticos. Digo reforzamiento por cuanto la idea del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) debe ser fortalecida.
- El establecimiento y definición de estándares de seguridad para entidades públicas y privadas que tienen responsabilidad sobre los datos e información sensible a nivel país.
- La creación de una unidad para el desarrollo de programas de concientización en seguridad a nivel de colegios, universidades y empresas publicas donde se genera, procesa almacena y transmite información sensible para el país.
- Apoyo para que las universidades generen proyectos de Ciberseguridad a nivel de Sistemas Operativos, criptografía, controladores, drivers y otros elementos tecnológicos.
- Establecimiento de legislación y regulación sectorial orientada a establecer adecuados niveles de seguridad y cumplimiento.

4.3.2 Sector Financiero:

Si bien en el ámbito nacional en general existe un vació regulatorio que brinde los lineamientos y directrices básicas para la gestión de la Ciberseguridad, la Autoridad de Supervisión del Sistema Financiera (ASFI) si ha emitido normas de Seguridad de Información que permiten al menos de forma básica poder brindar lineamientos a las Entidades Financieras en busca de poder mitigar riesgos tecnológicos, estos son:

1) Reglamento para la gestión de seguridad de la información (ASFI/193/2013):

   Establece requisitos mínimos que las entidades deben cumplir para la gestión de seguridad de la información, de acuerdo con la complejidad de los procesos y

operaciones que realizan. Por otra parte, define criterios que deben tomarse en cuenta de cara a cumplir con niveles de seguridad adecuados en cuanto al manejo de su información, como ser: Autenticación, Confiabilidad, Confidencialidad, Cumplimiento, Disponibilidad, Integridad y No repudio.

Este mismo documento establece que las entidades deben contar con políticas, estructura, organización, segregación y recursos tecnológicos, exige contar con procedimientos para la identificación y gestión de activos de información y control de accesos, gestión de seguridad en redes y comunicaciones, gestión de incidentes y exigencia de contar con un plan de continuidad de negocios de cara a asegurar la continuidad de los servicios. Para el caso de contratos con terceros exige un análisis de riesgo y si se trata de administración de data de clientes en la nube es necesario pedir la no objeción y que el proveedor cumplas las mismas exigencias de seguridad (antes mencionadas) que requieren las Entidades Financieras.

2) Reglamento para el Envío de Información:

El mencionado documento, establece los criterios de seguridad mínimos que se requiere cumplir para realizar cualquier tipo de transferencias de información dentro la entidad financiera, de éste con sus clientes, con otras instituciones e incluso con la ASFI y otros entes reguladores, así también prevé el monitoreo regulatorio de las operaciones y transacciones que realizan las entidades financieras. Los criterios están divididos según el destinatario en Contenidos, Tipos, Formatos, Sistemas, Nomenclatura y establecen plazos (cuando se trata de información que debe ser reportada a la ASFI).

Cabe señalar que de manera independiente la Asociación de Bancos de Bolivia (ASOBAN) ha tomado la iniciativa de crear un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), por ahora dicho proyecto está siendo liderado por la comisión de Seguridad de Información de ASOBAN y se espera que el proyecto sea aprobado en el primer semestre de 2020. Sin embargo, debe señalarse que a nivel financiero ya existe una red de comunicación entre todos los oficiales de seguridad de información y de riesgo tecnológico de las Entidades Financieras, permitiendo así tener fluida comunicación y la capacidad de reacción ante incidentes de forma coordinada.

4.4. España.

4.4.1 Gobierno:

El Consejo de Seguridad Nacional de España, ha incluido la Ciberseguridad como una prioridad de la Estrategia de Seguridad Nacional desarrollada por el Ministerio de Asuntos Exteriores y de Cooperación. Es así que la Política de Ciberseguridad Nacional se desarrolla a través de dos ejes: 1) Estrategia de Ciberseguridad Nacional, cuyo fin es articular una adecuada capacidad de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas; 2) El Plan Nacional de Ciberseguridad, que recoge las líneas de acción para desarrollar el primer documento.

Es así que, el Consejo Nacional de Ciberseguridad ha elaborado una nueva Estrategia de Ciberseguridad Nacional actualizando la de 2013. En su diseño, solo han intervenido representantes gubernamentales del mencionado Consejo, la actualización ha sido publicada en abril de 2019.

La Estrategia se limita a emitir directrices generales y técnicas a las que tendrán que seguir decisiones políticas concretas para ejecutar las líneas de actuación recogidas en ella. Corresponde al Gobierno respaldar o no al Consejo Nacional de Ciberseguridad.

La estrategia señala los 4 principios por las que se rige, siendo estos:

1. *Unidad de acción:* La eficacia y rapidez de respuesta frente a los ciberincidentes que involucren a diferentes agentes estatales se lograrán con coordinación de la Unidad de Acción del Estado.

2. *Anticipación:* Las acciones estatales para reducir los alcances de las amenazas críticas, demandan mecanismos preventivos ideados por organismos especializados. El sector privado también debe participar con su conocimiento.

3. *Eficiencia:* La estrategia nacional de Ciberseguridad requiere sistemas multipropósito, como ser: tácticas tecnológicas, económicas y socialmente responsables que optimicen los recursos y encaucen la acción del Estado.

4. *Resiliencia:* El Estado debe disponer de elementos que mejoren la capacidad de reacción contra las ciberamenazas.

Por otro lado, la estrategia de Ciberseguridad Nacional 2019 obedece al objetivo general de *"garantizar el uso fiable y seguro del ciberespacio, protegiendo los derechos y libertades de los ciudadanos, y promoviendo el progreso económico"* y a otros de carácter específico:

1. El sector público y sus servicios principales, deben ser un ejemplo en cuanto a buenas prácticas en Ciberseguridad.

2. Cooperación policial, ciudadana y judicial (nacional e internacional) para enfrentar el uso ilícito del ciberespacio.

3. Establece el intercambio de información entre privados y estatales, velando por la constante actualización y puesta en práctica de las medidas de ciberdefensa.

4. Busca impulsar la cultura de Ciberseguridad, en busca de recursos humanos y técnicos que garanticen la autonomía tecnológica del país.

5. Participación activa en la Ciberseguridad internacional.

Para conseguir los objetivos descritos define líneas de acción a seguir:

- *Líneas de acción 1 y 2:* Fortalecer capacidades ante ciberamenazas y garantizar la resiliencia de los activos estratégicos del país (enfoque en el objetivo 1).

- *Línea de acción 3:* Profundizar la investigación y persecución del cibercrimen (responde al objetivo 2).

- *Línea de acción 4:* impulsar la Ciberseguridad ciudadana y empresarial (responde al objetivo 3).

- *Línea de acción 6:* Trabajar en la Ciberseguridad internacional (objetivo 5).

- *Líneas de acción 5 y 7:* Reforzar la autonomía digital mediante el talento y la industria de Ciberseguridad nacional, y desarrollar la cultura de Ciberseguridad (objetivo 4).

Finalmente, define la estructura de la Ciberseguridad en el Sistema de Seguridad Nacional, de acuerdo al siguiente detalle:

- El Consejo de Seguridad Nacional;

- El Comité de Situación (que actuará en situaciones críticas);

- El Consejo Nacional de Ciberseguridad;

- La Comisión Permanente de Ciberseguridad;

- El foro Nacional de Ciberseguridad;

- Las Autoridades públicas competentes y los CSIRT (Computer Security Incident Response Team, o Equipo de Respuesta ante Incidencias de Seguridad Informáticas) de referencia nacionales.

En España el **Foro CSIRT.es** es una plataforma independiente de coordinación y colaboración de confianza entre los CSIRTs de ámbito nacional que permita optimizar la cooperación entre los mismos para actuar frente a problemas de seguridad informática en las redes españolas. A su vez, fomenta la divulgación de información de interés y la mejora de la visibilidad de los CSIRTs miembros del Foro en la comunidad española e internacional.

A la fecha el Foro CSIRT cuenta con más de 40 CSIRT afilados, desde empresas como Telefónica hasta Bancos como CAIXA.

4.4.2 Marco Legal Nacional:

4.4.2.1 Unión Europea:

La Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión. Esta Directiva define temas sobre la seguridad de las redes y sistemas de información para los operadores de servicios esenciales y para los proveedores de servicios digitales.

De este modo, se establece en el artículo 14 que *“Los Estados miembros velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización*

adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado".

Es decir, los Estados miembros velarán para que se cumpla con las medidas proporcionadas o adecuadas al riesgo planteado. Y también para que se adopten medidas a efectos de minimizar, reducir o prevenir incidentes que afecten a la seguridad.

Así mismo, también se deberá notificar sin dilación indebida a la autoridad competente o al CSIRT (siglas de término en inglés Computer Security Incident Response Teams) los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que se presten para que se puedan tomar medidas con carácter institucional o nacional al respecto, en su caso.

El artículo 16 establece "el deber del Estado para que los proveedores de servicios digitales determinen y adopten medidas de seguridad técnicas, organizativas y proporcionadas para gestionar los riesgos existentes a la seguridad de las redes y sistemas de información que se utilizan". Por ello, deben adoptar medidas con relación a la seguridad de sistemas e instalaciones, gestión de incidentes, gestión de la continuidad de las actividades, supervisión, auditorías y pruebas y cumplimiento de normas internacionales.

4.4.2.2 España:

En España se cuenta con el Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio y el velar por la mencionada Ciberseguridad.

Normativas de seguridad nacional:

- Ley 36 de 28 de septiembre de 2015, de Seguridad Nacional, regula los principios y organismos clave, así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.

- Orden TIN/3016/2011, de 28 de octubre de 2011, crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

Normativas de seguridad:

- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

- Ley 5/2014, de 4 de abril, de Seguridad Privada.

- Con relación a incidentes de seguridad, existe todo un entramado relacionado con las Fuerzas Armadas, pero también se dispone de una inclusión parcial en la Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.

Relacionadas con las telecomunicaciones, existen las siguientes normas:

- Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico (antes citada).

- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.

- Ley 50/2003, de 19 de diciembre, de firma electrónica.

- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- Relacionado con la ciberdelincuencia, encontramos inclusiones parciales en el Código Penal, la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores; o en el Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.

- También es de aplicación lo dispuesto en la normativa de protección de datos, desarrollada por la Ley Orgánica 15/1999, de 13 de diciembre y su Reglamento, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Otras leyes que regulan la Ciberseguridad a nivel técnico y organizativo.

Con relación a la Ciberseguridad a nivel técnico y organizativo, hay que tener en cuenta también lo establecido por el nuevo Reglamento Europeo de Protección de Datos 2016/679, así como la existencia de otro tipo de protocolos o reglas internacionales, en especial las relacionadas con las transferencias internacionales de datos, como el Privacy Shield.

4.4.3 Sector Financiero:

4.4.3.1 PSD2 (Payment Services Directive 2).

Nace en 2007, con la primera **"Directiva de Servicios de Pago (PSD)"**, por sus siglas en inglés (Payment Service Providers), con el objetivo de contribuir al desarrollo de un mercado único de pagos en la Unión Europea, y fomentar así la innovación, la competencia y la eficiencia en territorio comunitario.

En 2013, la Comisión Europea propuso una revisión (de ahí el '2' de la PSD2), que pretendía ahondar en estos objetivos. Busca mejorar la protección del consumidor, impulsar la competencia e innovación del sector, y reforzar la seguridad en el mercado de pagos, lo que se espera que favorezca el surgimiento de nuevos métodos de pago y el comercio electrónico.

La PSD2 regula y armoniza 2 clases de servicios que ya existían cuando se adoptó la primera PSD en 2007 pero que se estaban popularizando en los últimos años: por un

lado, los servicios de iniciación de pagos (PIS) y por otro los servicios de información de cuenta (AIS).

El servicio de información de cuenta (AIS) consiste en recoger y almacenar la información de las distintas cuentas bancarias de un cliente en un solo lugar, permitiendo a los clientes tener una visión global de su situación financiera y analizar fácilmente sus gastos y sus necesidades financieras.

Por su parte, en el servicio de iniciación de pagos (PIS), terceros proveedores facilitan el uso de la banca 'online' para realizar pagos por internet. Estos servicios ayudan a iniciar un pago desde la cuenta del consumidor a la cuenta del comercio mediante la creación de una interfaz "puente" entre ambas cuentas, rellenando la información necesaria para la transferencia (cuantía de la transacción, número de cuenta, mensaje) e informando al comercio del inicio de la transacción. Asimismo, la PSD2 también posibilita al cliente la realización de pagos a terceros desde la aplicación de un banco utilizando cualquiera de sus cuentas (pertenezcan o no a esa Organización).

El segundo punto de la PSD2 es la introducción de nuevos requisitos de seguridad, lo que se conoce como Autenticación Reforzada de Clientes (Strong Customer Authentication o SCA en inglés). Esto implica el uso del doble factor de autenticación en operaciones bancarias que antes no lo requerían, incluyendo pagos y acceso a cuentas online o a través de apps, así como una definición más estricta de lo que puede servir como factor de autenticación.

Esta normativa se materializa en el ámbito de la seguridad para las Entidades Financieras, las cuales han tenido que actualizar los elementos de autenticación que facilitan a sus clientes, sustituyendo tarjetas de coordenadas o 'tokens' con mensajes al móvil o tokens más avanzados.

Además, han tenido que desarrollar sistemas y procesos que permitan al banco hacer uso de las exenciones que permite la normativa a la autenticación reforzada en aquellas transacciones en que el nivel de riesgo se considera bajo.

La PSD2 ha entrado en vigor progresivamente desde enero de 2018, no obstante, el principal hito regulatorio ha sido la entrada en vigor de las obligaciones de autenticación y acceso de terceros el pasado 14 de septiembre de 2019.

Dicho esto, no todos estos requisitos técnicos han entrado en vigor ya, ante el posible impacto negativo que podía tener la entrada en vigor de la PSD2 en el comercio electrónico, las Entidades Financieras van a contar con un período transitorio adicional cuya duración máxima ha sido establecida por la Asociación de Bancos de España (ABE) en el 31 de diciembre de 2020.

4.4.3.2 Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679).

Marco legal de la Unión Europea que reemplaza a la Directiva de Protección de Datos. La diferencia más importante entre ambas es la diferencia entre una "regulación" y una "directiva".

Mientras que las directivas son recomendaciones a tener en cuenta y no son legalmente vinculantes, las regulaciones sí son leyes y responsabilizan legalmente a las compañías. Esto significa que el RGPD es una ley que debe ser cumplida por todos los estados europeos miembros, mientras que la anterior Directiva de Protección de Datos no lo era.

Su objetivo es proteger los datos personales y la forma en la que las organizaciones los procesan, almacenan y, finalmente, destruyen, cuando esos datos ya no son requeridos. La ley provee control individual acerca de cómo las compañías pueden usar la información que está directa y personalmente relacionada con los individuos, y otorga ocho derechos específicos.

Además, establece normas muy estrictas, que rigen lo que sucede si se viola el acceso a datos personales y las consecuencias (penalidades) que las organizaciones pueden sufrir en tal caso.

El RGPD incluye una definición muy amplia respecto a lo que debe entenderse como filtración de datos: *"una filtración en la Seguridad que lleva a la destrucción, pérdida, alteración, divulgación no autorizada, o acceso -accidental o ilegal-, a datos personales transmitidos, almacenados, o procesados de alguna forma"*. Entiende como *"datos personales" a "cualquier información relacionada a una persona identificable o no identificable"*, no se trata solo de datos que puedan ser usados para fraude o robo de identidad.

Esas definiciones son importantes porque significa que muchos eventos o actividades diferentes pueden calificar como violaciones según el RGPD.

El RGPD aplica a:

- Organizaciones con presencia física en al menos algún país miembro de la Unión Europea.

- Organizaciones que procesan o almacenan datos sobre individuos que residen en la Unión Europea.

- Organizaciones que utilizan servicios de terceros que procesan o almacenan información sobre individuos que residen en la Unión Europea.

Los 8 derechos que establece el RGPD:

- *Derecho a estar informado:* Proporciona transparencia sobre cómo son utilizados sus datos personales.

- *Derecho al acceso:* Provee acceso a sus datos, a cómo son utilizados, y a cualquier información suplementaria que pueda ser utilizada juntos con sus datos.

- *Derecho a la rectificación:* Otorga el derecho a que sus datos personales sean rectificados en caso de ser incorrectos o incompletos.

- *Derecho a ser borrado (o derecho a ser olvidado):* Es el derecho a que sus datos personales sean removidos de cualquier lugar si no existe una razón convincente para que estén almacenados.

- *Derecho a restringir el procesamiento:* Permite que sus datos sean almacenados, pero no procesados. Por ejemplo, puede recurrir a este derecho si siente que datos erróneos acerca de usted son almacenados a la espera de ser rectificados.

- *Derecho a la portabilidad de datos:* Puede solicitar copias de la información almacenada sobre usted, para utilizar en cualquier otro lugar. Tal es el caso de si aplicara para productos financieros entre distintas entidades.

- *Derecho a objetar:* Otorga el derecho a objetar acerca del procesamiento de sus datos. Un ejemplo podría ser la objeción de que sus datos sean utilizados por organizaciones de marketing directo.

- *Derecho sobre la toma de decisiones y creación de perfiles automáticos:* Permite objetar sobre la toma de decisiones automáticas que se hagan sobre sus datos personales. "Automáticas" se refiere a sin intervención humana. Por ejemplo, la definición de determinados hábitos de compra online, en función a comportamientos previos.

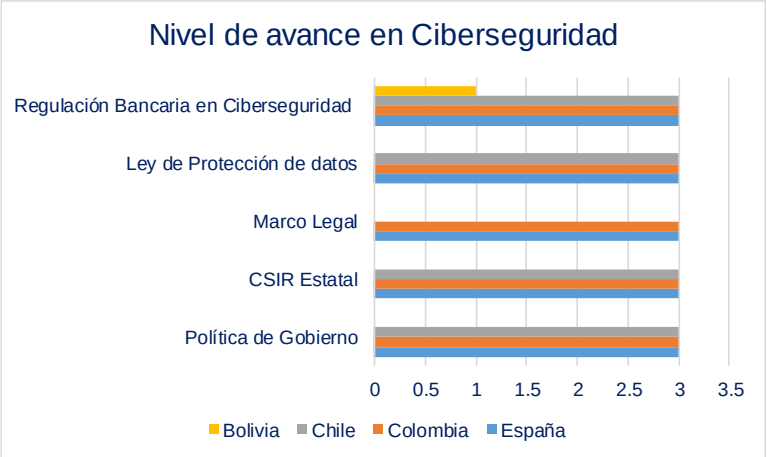
4.5. Análisis Comparativo.

Cuadro 17. Tabla Comparativa Normativa.

PAÍS	DESCRIPCIÓN COMPARATIVA
ESPAÑA	**Gobierno:** • Política nacional de Ciberseguridad (2013, actualizado en 2019); • Creación de un Consejo Nacional de Ciberseguridad; • Cuenta con un Grupo de Respuesta a Emergencias Cibernéticas "FORO CSIRT.es. **Marco Legal Nacional:** • Unión Europea, Directiva 2016/1148: Garantizar nivel común de seguridad en redes y sistemas de información; • Unión Europea, Reglamento Europeo de Protección de Datos 2016/679; • España Código de Ciberseguridad; • Cuenta con una estructura de12 normas de seguridad nacional y telecomunicaciones. **Sector Financiero:** • Directiva de Servicios de pago, (Dos normativas). • Unión Europea, Reglamento Europeo de Protección de Datos 2016/679.
COLOMBIA	**Gobierno:** • Estrategias de Ciberseguridad nacional: CONPES 3701 y CONPES 3854; • Grupo de Respuesta a Emergencias Cibernéticas de Colombia a nivel nacional. **Marco Legal Nacional:** • Ley 527: Comercio Electrónico: Reglamenta acceso y uso de los mensajes, comercio electrónico y firmas digitales; • Ley 1581 de 2012 Protección de Datos Personales. **Sector Financiero:** • Circular Externa 007 de la Superintendencia Financiera: Imparte requerimientos mínimos de gestión de ciberseguridad. • Equipo de Respuesta a Incidentes de Seguridad Informática "CSIRT Financiero".
CHILE	**Gobierno:** • Política nacional de Ciberseguridad 2018 – 2022: Describe la misión de proteger a usuarios privados y públicos; • Comité Interministerial sobre Ciberseguridad (CICS) de Chile; • Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT). **Marco Legal Nacional:** • Ley 19.628 sobre Protección de la vida privada, regula la protección de datos; • Proyecto de Ley: Reforma Ley 19.628; Ley Marco de Ciberseguridad y Proyecto de Infraestructura Crítica **Sector Financiero:** • Circular 2.633 de la Superintendencia Financiera: Lineamientos de seguridad de activos de información. • Circular 3.640 de la Superintendencia Financiera: Lineamientos de reporte al regulador respecto a eventos cibernéticos.
BOLIVIA	**Gobierno y Marco Legal:** • No cuenta con una política nacional de Ciberseguridad; • No cuenta con un Comité sobre Ciberseguridad y tampoco con un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT). **Sector Financiero:** • Reglamento para la gestión de seguridad de la información (ASFI/193/2013) de la Superintendencia Financiera. • Reglamento para envío de información a la Superintendencia Financiera. • La Asociación de Bancos esta realizando un proyecto para implementar un CSIRT Financiero.

Fuente: Elaboración propia.

Gráfico 19. Nivel de desarrollo en Ciberseguridad por país evaluado.



Nota: 0 = Inexistente; 1 = Nivel Bajo; 2 = Nivel Medio; 3 = Implementación completa

Fuente: Elaboración propia.

Como puede verse en América Latina existe una evolución importante en cuanto a la Ciberseguridad, debido al involucramiento de los Gobiernos dado el interés que existe en proteger a su sociedad de amenazas. Sin embargo, el desarrollo no ha llegado a todos los países ni en lo normativo, ni en lo tecnológico, por lo que existen grandes diferencias de un país a otro en cuanto al desarrollo de la Ciberseguridad.

Sin embargo, si comparamos la legislación española, podemos ver que incluso Colombia queda muy lejos en cuanto a los adelantos regulatorios en Ciberseguridad, debido a la importancia que los países desarrollados le han venido dando al tema, generando inclusive un Código de Ciberseguridad, incluyendo a los delitos en esta materia de manera transversal en su legislación con el afán de prevenirlos y poder juzgarlos, además por otra parte han y a través de la Unión Europea, han definido derechos propios respecto al uso almacenamiento y destrucción de los datos.

Algo que aprender de la Unión Europea es que en esta materia se han generado leyes de aplicación obligatoria todos los países miembros en temas puntuales, asegurándose así los gobiernos a que todos los países deban por un lado robustecer sus sistemas cibernéticos, compartir información de manera confidencial, generar una cultura a nivel continente respecto a la Ciberseguridad y por otro a uniformar y hacer respetar los derechos de los usuarios que es finalmente aquello que las entidades (financieras o no) deben proteger, debido a que hoy por hoy es el objetivo de los ciberatacantes.

Por tanto, es imperativo que la Organización de los Estados Americanos (OEA), las Naciones Unidades (ONU), la Comunidad Andina de Naciones (CAN), la Federación de Latinoamericana de Bancos (FELABAN) y demás entes que conforman la comunidad internacional, comprendan que en cuanto a temas digitales todos los estados y entidades están conectados de una u otra forma, por lo que el desarrollo debe trabajarse de forma conjunta y no individual, por tanto, se hace necesario crear un acuerdo que deba ser de carácter obligatorio con lineamientos base para que todos los países de la región puedan desarrollar medidas de control y gestión del riesgo de Ciberseguridad a nivel estatal, financiero, industrial, etc., toda vez que como ya se mencionó la diferencia con otros tipos

de riesgos o amenazas, está en que el mundo digital y el internet permiten la interconexión a nivel mundial, por lo que de existir un país con una alta probabilidad de vulnerabilidad, se puede generar un efecto domino que afecte a toda una región en cualquiera de los sectores de la economía y de la comunidad en general.

5. Marco de trabajo para implementar la Gestión de Riesgo de Ciberseguridad.

5.1. Alcance del trabajo.

El presente documento se enfocará en la primera etapa del Marco NIST la cual es “IDENTIFICAR “con el objetivo de que todas las Entidades Financieras, sin importar su nivel de madurez, ni su tamaño como Organización, puedan contar con una guía base de cómo empezar a implementar un marco de gestión de Ciberseguridad.

5.2. Inicio de la Implementación.

Para comenzar con la implementación, es necesario que de forma inicial los encargados de llevar adelante el programa de Ciberseguridad elaboren un listado de las actividades que deben realizar, a continuación, se sugieren los siguientes pasos o actividades de manera general:

1. Definir el enfoque bajo el cual se llevará a cabo la implementación;

2. Definir el marco metodológico para llevar adelante la implementación de la gestión de Ciberseguridad;

3. Alinearse a las mejores prácticas en función a la realidad de la Entidad Financiera.

5.2.1 Definición del enfoque de la implementación.

Es necesario que la Entidad Financiera tenga claridad respecto al objetivo a cumplir, por tal motivo deberá trabajar en función a la velocidad y eficacia de la implementación, el ámbito de aplicación, definiendo expectativas y el alcance del programa y por último trabajara bajo clara consciencia del nivel de madurez de los procesos internos y sus controles.

Los enfoques que se proponen para trabajar son al menos 5, y están prácticamente estructurados de forma previa a la puesta en marcha del plan de Ciberseguridad el cual es básicamente un proyecto específico dentro de un todo que es la Entidad Financiera, estos son:

a) Negocio: Busca identificar e integrar el contexto de la Ciberseguridad en las diferentes actividades comerciales de la Entidad Financiera y como a partir de ésta puede incrementar la oferta de valor en los diferentes productos y servicios que el banco presta, así como el poder gestionar los diferentes riesgos cibernéticos a los que se enfrenta la entidad al ofertar y prestar un determinado servicio o negocio (ejemplo, las transferencias interbancarios nacionales o vía Swift, las plataformas electrónicas, la firma electrónica o digital, el reconocimiento facial.

b) Sistemas: Es la implementación general del proceso a los diferentes sistemas, aplicaciones tecnológicas, los procesos y ecosistemas que soportan el funcionamiento integral de la Entidad Financiera.

c) Sistemático: Este enfoque, es de suma importancia debido a que el líder del equipo de Ciberseguridad que dirija su implementación en la Entidad Financiera, debe

poder utilizar y aplicar las mejores prácticas que tengan a disposición de cara a la implementación del riesgo cibernético, pero sin perder de vista la real factibilidad y utilidad de su implementación y aplicabilidad dentro la Entidad Financiera.

d) Integrado: Es necesario que el líder a cargo tenga influencia dentro de la Organización a fin de cuente con el apoyo de la alta gerencia y que además cuente con la capacidad para conseguir que el programa de Ciberseguridad armonice con los demás pilares y necesidades de la Organización.

e) Iterativo: El líder debe lograr una implementación ágil y rápida del programa de Ciberseguridad, por tanto, es importante que pueda generar un mínimo viable de evolución continua en el tiempo, a través de un cronograma de adecuación acorde a la realidad y las necesidades de la Entidad Financiera.

En función a lo expuesto, se realizan algunas sugerencias estratégicas de cara al inicio del proceso de implementación de la gestión de Ciberseguridad:

- El equipo Líder a cargo del programa de Ciberseguridad en el área de Riesgos, al ser responsables del gobierno de esta nueva gestión de riesgos, debe definir de forma previa y coordinada con el área de Sistemas y tecnología, las funciones y responsabilidades de todas las partes involucradas en la implementación de la gestión de la Ciberseguridad.

- Debe buscarse la integración de la Ciberseguridad a los procesos existentes, evitando la creación de nuevos procesos que después no puedan ser cumplidos debido a la situación real de la entidad u Organización.

- Buscar siempre la mejora continua e involucrar a todas las partes interesadas en el proyecto. Definir metas y objetivos alcanzables, con planes de acción a largo plazo en busca de la mejora continua de los procesos.

- Por otra parte, es importante entender que en el mundo de las Entidades Financieras existen roles de cara a la defensa de la Organización y en cuanto a la gestión de Ciberseguridad, estos se describen de la siguiente manera:

    - Primera línea de defensa: Suele ser el equipo de sistemas y de seguridad de información de la Organización, de forma general, suele ser la que está en el front de la operación misma, es decir, se encarga de ejecutar las diferentes tareas del día a día, brindar soporte en esquemas de seguridad a la Organización, define e implementa pautas y normas de Seguridad de Información, manteniendo actualizados los métodos y técnicas de evaluación, prevención y control de riesgos y finalmente, suelen encargarse de asesorar a las Unidades de Negocios (usuarios responsables de recursos de información) y de Sistemas coordinando la atención de sus necesidades.

    - Segunda Línea de defensa: Suele ser el equipo que se encarga de gestionar riesgos dentro de la Organización. Su gestión es básicamente la de analizar y desarrollar estrategias mediante la adopción y adaptación de las sugerencias dadas por el NIST, FFIEC, la ISO referentes a Ciberseguridad y Seguridad

informática, así como a las definidas por el regulador local o un referente internacional, con el objetivo de prevenir cualquier traspaso o violación cibernética, a fin de evitar y/o reducir la exposición frente a riesgo tecnológico.

- Tercera Línea de defensa: Esta línea se encuentra compuesta por el área de auditoría de la Entidad Financiera, quien debe validar que efectivamente las dos líneas previas cumplan a cabalidad con las responsabilidades acordadas y definidas en la estrategia de la Organización.

- Obtener el apoyo de la dirección, asegurando de forma inicial que la alta dirección de la Organización comprenda y apoye la implementación de la gestión de la Ciberseguridad, de conseguirse el apoyo, se contará con la fuerza para realizar cambios en la organización, gestionar recursos para llevar adelante el proyecto.

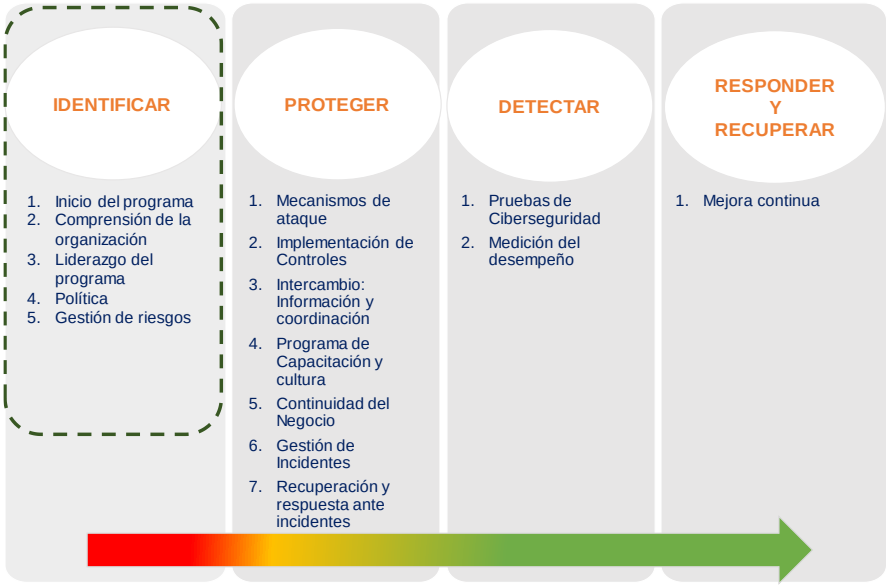
Una vez considerados estos puntos, el plan del proyecto para la gestión de la Ciberseguridad, debe ser puesto en conocimiento y aprobado por la alta dirección, pero consensuado con todas las partes interesadas para que todos se sientan comprometidos con el proyecto.

Por lo expuesto, las sugerencias realizadas se consideran esenciales de cara a que el líder del programa pueda tener claridad a la hora de conseguir el respaldo de la alta dirección no solo desde el punto de vista de riesgo, sino también el de negocio, segundo poder identificar e involucrar a sus stakeholders desde un inicio eliminado así la posibilidad de rechazo, reprocesos o reacciones contrarias que demoren o trunquen el proceso de implementación. Finalmente, es importante señalar en estos puntos, que el líder debe ser alguien de la unidad de riesgos, debido a que, al ser ajeno al equipo de tecnología o sistemas, puede tener la independencia de monitoreo y control de la gestión tecnológica de la institución generando así un equilibrio de poderes y roles a la interna de la Entidad Financiera.

5.2.2 Marco de trabajo para implementar la Ciberseguridad.

El marco de trabajo propuesto, se basa en la hoja de ruta inicial trazada desde la experiencia en una Entidad Financiera de Bolivia, la cual se ha basado en el marco de trabajo de Ciberseguridad del NIST y la ISO 27032, a continuación, se resume dicho marco en el siguiente esquema de etapas:

Gráfico 20. Etapas del Marco de Trabajo NIST.



Fuente: Elaboración propia en base a: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019) (International Organization for Standardization ISO/IEC 27032, 2012).**

Como puede verse en el cuadro anterior el esquema de etapas que sugiere el NIST abarcan un trabajo sumamente extenso, es así que el presente trabajo de grado se enfocará en la primera etapa “IDENTIFICAR “, la cual deben trabajar las Entidades Financieras, toda vez que, lo que el objetivo que tiene es brindar una guía base de cómo empezar a implementar un marco de gestión de Ciberseguridad.

5.3.2.1 Identificar.

<u>Comprensión de la Organización.</u>

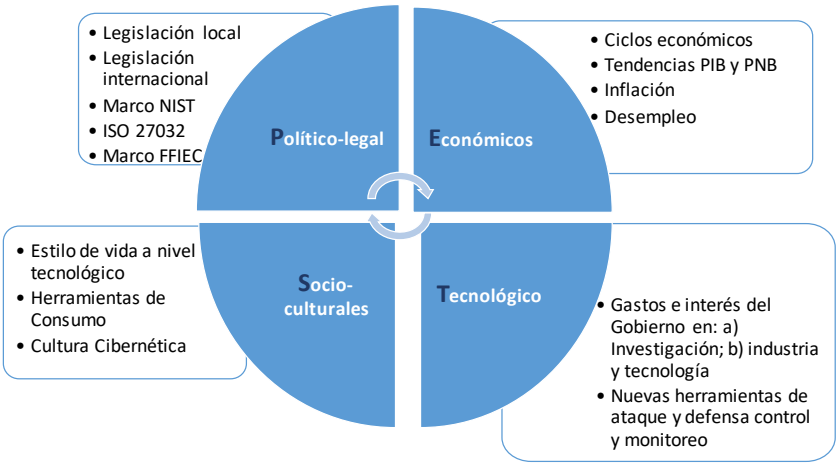
Para trabajar en este primer punto, hay que tener en cuenta la necesidad que se tiene como encargado de la Ciberseguridad de conocer la Organización, el negocio, su misión, objetivos y estrategia.

a) <u>Análisis de la Organización en su conjunto y herramientas tipo:</u>

Una vez hecho esto, debe llevarse a cabo un análisis PEST que permita identificar las condiciones del entorno bajo las cuales se tendrá que implementar la gestión de Ciberseguridad dentro de la Organización. La elección de esta técnica se basa en que permite tener un panorama integral del entorno, y los principales factores que afectan a la Ciberseguridad.

En el gráfico puede verse a modo de ejemplo algunos de los puntos centrales que deben ser abordados para este análisis PEST.

Gráfico 21. Análisis PEST: Entorno para la Ciberseguridad en Entidades Financieras.



Fuente: Elaboración propia en base a: **(Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012) (National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

Político/Legales:

Se sugiere que, en este punto, la Entidad Financiera revise el entorno político que lo rodea con la finalidad de identificar si su gobierno tiene a la Ciberseguridad como pilar de seguridad del Estado, de esta manera, podrá trabajar seguro respecto a la legislación y con referencia en la estrategia nacional.

La legislación nacional, siempre estará de la mano del Estado, por tanto, de ser la Ciberseguridad una prioridad para el gobierno, la Entidad Financiera deberá realizar la revisión del marco normativo general que la regula, partiendo de la protección de datos, y a continuación deberá realizar la revisión de la normativa sectorial financiera, con la finalidad de validar si está en línea con las exigencias regulatorias y el esfuerzo en recursos que representará su implementación. Finalmente deberá revisar las penalidades de cara al incumplimiento de la regulación nacional con la finalidad de valorar el riesgo legal y de cumplimiento normativo al que se expone.

De cara a la legislación internacional, deberá revisar como los diferentes Organismos Internacionales emiten mejores prácticas como referencia para la implementación de la Ciberseguridad, y deberán tener el deber de cuidado necesario con la finalidad de darse cuenta si estas mejores prácticas se van convirtiendo en requisitos para operar con sus pares de otras latitudes y así evitar verse encapsulados e imposibilitados de operar a nivel internacional, como ocurre cuando las Entidades Financieras no acatan las recomendaciones emitidas por el Comité de Basilea.

Económicos:

Será importante que la Entidad Financiera pueda identificar si se encuentra en condiciones económicas que le permitan invertir en herramientas de control cibernético, pero no solo a nivel interno, sino también evaluando factores macroeconómicos que le den una lectura respecto a la seguridad de inversión.

A nivel económico es muy importante que las Entidades Financieras vinculen la tecnología a la oportunidad de negocio de cara a la captación de un nuevo tipo de clientes (tanto en operaciones activas como pasivas) a quienes no les gusta ir a sus instalaciones, por lo que valorará la nueva forma de conectarse digitalmente, generando además una mayor capilaridad de mercado.

Socioculturales/Ambientales:

Las Entidades Financieras deben darse cuenta que el mundo está viviendo una tendencia de transformación digital, por lo que los clientes comparan su experiencia en otros servicios con la que experiencia que viven en una Entidad Financiera, en este sentido, es importante que la Organización pueda segmentar a su población bancarizada entre personas de generación digital, personas que no son digitales, pero podrían convertirse en tales, y aquellas que prefieren la lógica tradicional bancaria, para que una vez realizada la segmentación, pueda medir el riesgo inherente de Ciberseguridad y así gestionar la priorización y acciones de implementación para la gestión de Ciberseguridad (recursos humanos, tecnología).

Tecnológicos:

De la mano del punto anterior, la Entidad Financiera debe saber que la tecnología de transformación digital no solo está amparada en cuanto a la parte comercial, sino que debe ir acompañada de una inversión y transformación digital de la forma de gestionar el riesgo. Es así que, debe poder conocer, investigar e implementar herramientas tecnológicas que le permitan gestionar el riesgo cibernético de manera preventiva y contar también con herramientas que le permitan ser resiliente y recuperarse con el menor daño posible en caso de ataques cibernéticos.

Un factor importante que tocar en este punto, es la necesidad de que la tecnología vaya acompañada del equipo humano correcto que le permita poder analizar, identificar riesgos, así como poder priorizar y recomendar las medidas que deben ser adoptadas para proteger a la Organización en caso de ciberataques.

Por lo expuesto, es importante señalar que el encargado de implementar la gestión de Ciberseguridad en la Entidad Financiera a través de su conocimiento respecto al giro del negocio, riesgos y de la propia institución, pueda comprender como se interconectan las diferentes partes interesadas y cómo deben trabajar de forma conjunta con las demás áreas técnicas y del negocio para coadyuvar a la estrategia de Ciberseguridad.

Esta es la forma más asertiva de poder entender la pertinencia, urgencia y priorización de las acciones que deben tomarse para atender el riesgo específico al que se enfrenta

la Organización, toda vez que, no servirá de nada contar con herramientas de control de Ciberseguridad, por ejemplo, de cara a Banca Móvil si no se tiene habilitado ese canal.

b) Identificación Partes Interesadas:

Conforme a la definición expuesta en el capítulo 2 en el punto 2.1.8, en concordancia con la ISO 27032, la cláusula 4.44 las partes interesadas son “personas u organizaciones que pueden afectar, ser afectadas, o percibir que está afectada por una decisión o actividad”, en este caso las partes interesadas son todas aquellas que forman parte del ecosistema financiero relacionado a la Entidad Financiera, tal como puede verse en el siguiente cuadro.

Gráfico 22. Identificación de las Partes Interesadas.

Elaboración propia, en base a: **(Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012) (National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

Cuando se habla del análisis de las partes interesadas, debe trabajarse bajo los siguientes puntos:

- Identificar los requerimientos y expectativas:

  Identificar requerimientos y expectativas de todas las partes interesadas, estos pueden ser implícitos o explícitos. (ejemplo: Definir un límite máximo de inversión para Ciberseguridad).

- Validar los requerimientos y expectativas:

  - Analizar las necesidades de seguridad y confirmar si responde a las preocupaciones, intereses y realidad de la Organización.

  - Puede realizarse mediante un cuestionario a las gerencias de la Organización y consultas con los pares de otras organizaciones similares.

- Grupos focales donde participen funcionarios de las 3 líneas de defensa vía entrevistas y grupos focales. Se sugiere utilizar el siguiente esquema:

  - Se sugiere realizar al menos 5 entrevistas focales, mezclando a los funcionarios de las líneas de defensa.

  - De cara a las entrevistas, realizar al menos una de manera escalonada por equipo.

- Evaluar y relevar los procedimientos actuales a fin de verificar si las expectativas y líneas de trabajo están acertadas o no.

- Identificar roles y responsabilidades:

  - Definir que se espera de cada parte interesada, nivel de participación y apoyo.

  - Establecer un consenso durante la planificación, los cuales deben ser documentados y archivados.

  - Definir el plan de trabajo de los equipos en función a un cronograma común que permita a todos avanzar en la implementación de la gestión de Ciberseguridad, sin impactar en las tareas propias de la unidad.

Para finalizar la etapa de estudio de la Organización, debe elaborarse de cara a la gestión de la Ciberseguridad, una matriz DAFO[10] inicial, la cual deberá transformarse en una matriz DAFO final que pueda exponer las debilidades, amenazas, fortalezas y oportunidades de la Organización, así como las diferentes estrategias para afrontar los diferentes puntos identificados.

El análisis debe permitir contar con los siguientes resultados principales:

- Identificar las características de los factores internos y externos que influyen en la gestión de riesgo, la misión y visión de la Entidad, de la unidad, los actores y/o stakeholdes principales, la forma de organización interna.

- Identificar y analizar las amenazas conocidas y los requisitos de seguridad externa relacionados al sector financiero.

c) Identificación de procesos clave y actividades:

Antes que nada, es esencial que el gerente que lidere la implementación del programa de gestión de Ciberseguridad:

[10] *Proviene de las siglas en ingles SWOT (**S**trengths, **W**eaknesses, **O**pportunities y **T**hreats). Herramienta para identificar la situación real de una organización, empresa, o proyecto, y planear una estrategia de futuro. Técnica propuesta por Albert S. Humphrey en el Instituto de Investigaciones de Stanford. Estados Unidos.*

- Trabaje de forma conjunta con los líderes de las otras unidades que son estratégicas de cara a la implementación de la Ciberseguridad y así poder acordar y diseñar un marco de trabajo que les permita llegar a un objetivo común.

- Conozca toda la gama de productos y servicios de la Organización, debido a que, en función al modelo de negocio, la Organización puede estar expuesta a diferentes tipos de riesgos operativos, tecnológicos, crediticio, legales. En el mismo sentido, el líder del proyecto debe comprender los procesos operativos que soportan el negocio, debido a que es la ejecución de estos procesos la que expone a la Organización a riesgos de seguridad cibernética, es por este motivo que el gestor de riesgos quien debe analizar y comprender la naturaleza de los diferentes procesos e identificar los riesgos directos e indirectos a los que está expuesta la Organización durante el desarrollo de sus actividades.

A partir de los expuesto, es que se hace crucial de cara a una correcta gestión de la Ciberseguridad identificar los activos de información de la Entidad, toda vez que, a mayor complejidad de la gestión tecnológica de la entidad, existe mayor dificultad de cara a la protección de los activos, por tanto, será prioritario para los encargados de la gestión de Ciberseguridad:

- Identificar de forma inequívoca a los dueños de los activos y delegarles la responsabilidad de su gestión.

- Describir de forma inequívoca dónde se procesan, almacenan y como se transportan los activos a través de los sistemas de información.

- Determinar el valor que la Organización concede a los activos evaluados, ya sea absoluto (por ejemplo, el precio de compra, sustitución o desarrollo de un activo) o relativo (por ejemplo, costos directos e indirectos ocasionados por la pérdida de un activo).

Para poder realizar la identificación de los activos de información se recomienda que el Líder debe poder tener clara la trazabilidad de los activos de información a lo largo de todos los procesos de la Organización, para el caso de la Entidad Financiera utilizada como guía se realizó la evaluación a partir de los procesos determinados como críticos en función a:

- Procesos estratégicos: Aquellos alineados a los proyectos estratégicos de las unidades de la Entidad Financiera, los cuales forman parte de su Plan Estratégico anual.

- Procesos vitales: Aquellos considerados como de alto riesgo y críticos para la continuidad de las operaciones y servicios de la Organización, cuya falta o ejecución deficiente puede tener impacto significativo en la entrega de productos y servicios.

d) Identificación de la infraestructura:

Conforme lo señala en el Marco de Trabajo de Ciberseguridad del NIST, la ubicación de la infraestructura crítica debe estar debidamente identificada, valorada, documentada y

comunicada a los responsables de las 3 líneas de defensa y a la alta gerencia de la Organización.

Cuadro 18. Tabla guía de principales componentes de infraestructura.

CATEGORÍA	DEFINICIÓN	EJEMPLOS
HARDWARE	Elementos físicos que soportan los procesos TI	Servidores, Laptop, Impresora, etc.
SOFTWARE	Programas que contribuyen a procesar datos	Sistemas operativos, procesadores de texto, programas contables, etc.
REDES	Equipos de telecomunicaciones que conectan físicamente elementos de un sistema de información	Corta fuegos, cables de red, interruptores, puentes, etc.
SITIOS	Lugares físicos donde se realizan las operaciones	Oficinas, centros de datos, etc.

Elaboración propia en base a: **(Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012).**

5.3.2.2 Determinación de los Objetivos.

Como responsable de la Ciberseguridad y estar a cargo de definir los objetivos del programa de implementación para gestión de este riesgo, deben **analizarse** los siguientes factores:

- Eventos de riesgo histórico de la Organización y su tendencia;
- Incremento de costes y pérdidas derivadas de eventos anteriores;
- Definición de la exposición de riesgo inherente de la Entidad;
- El éxito o fracaso de proyectos anteriores de seguridad de información;
- Resultados de auditorías internas y/o externas que identifican vulnerabilidades;
- Cultura y sensibilización de la Organización de cara a la Ciberseguridad y la seguridad de información.

De forma complementaria al análisis anterior, deben realizarse tres preguntas clave a la interna del equipo responsable de implementar la gestión de la Ciberseguridad, con la finalidad de identificar el valor que le traerá a la Organización el gestionar este riesgo:

- ¿El gestionar la Ciberseguridad puede reducir o prevenir vulnerabilidades?
- ¿Puede la Ciberseguridad mejorar la eficacia en la gestión de la seguridad de la información?
- ¿La implementación de la gestión de la Ciberseguridad puede generar ventajas competitivas?

Una vez analizados tanto los factores como las tres preguntas, deben comenzar a elaborarse los objetivos, los cuales deben ser de diferentes tipos en función a lo que se

requiere para la implementación de la gestión de Ciberseguridad en la Organización. A continuación, y de manera enunciativa más no limitativa, se exponen algunos objetivos que pueden ser utilizados como guía:

- Definir el nivel de riesgo inherente de la Organización.
- Definir y establecer las políticas de gobierno de Ciberseguridad.
- Establecer los procedimientos y controles operativos que permitirán soportar las directrices de trabajo definidas.
- Implementar indicadores de Ciberseguridad:
    - Costo debido a incidentes de Ciberseguridad;
    - Tiempo de indisponibilidad por incidentes de Ciberseguridad;
    - Obsolescencia Tecnológica (Bases de datos y Sistemas Operativos fuera de soporte).
- Establecer y poner en marcha el programa de capacitación y cultura en la Organización.
- Establecer planes de respuesta de cara a la atención de emergencias y crisis.
- Asegurar el intercambio de información de amenazas de forma oportuna y precisa.
- Asegurar la implementación de tecnologías para la gestión preventiva, de monitoreo y de defensa.

Análisis de brecha y el nivel de madurez:

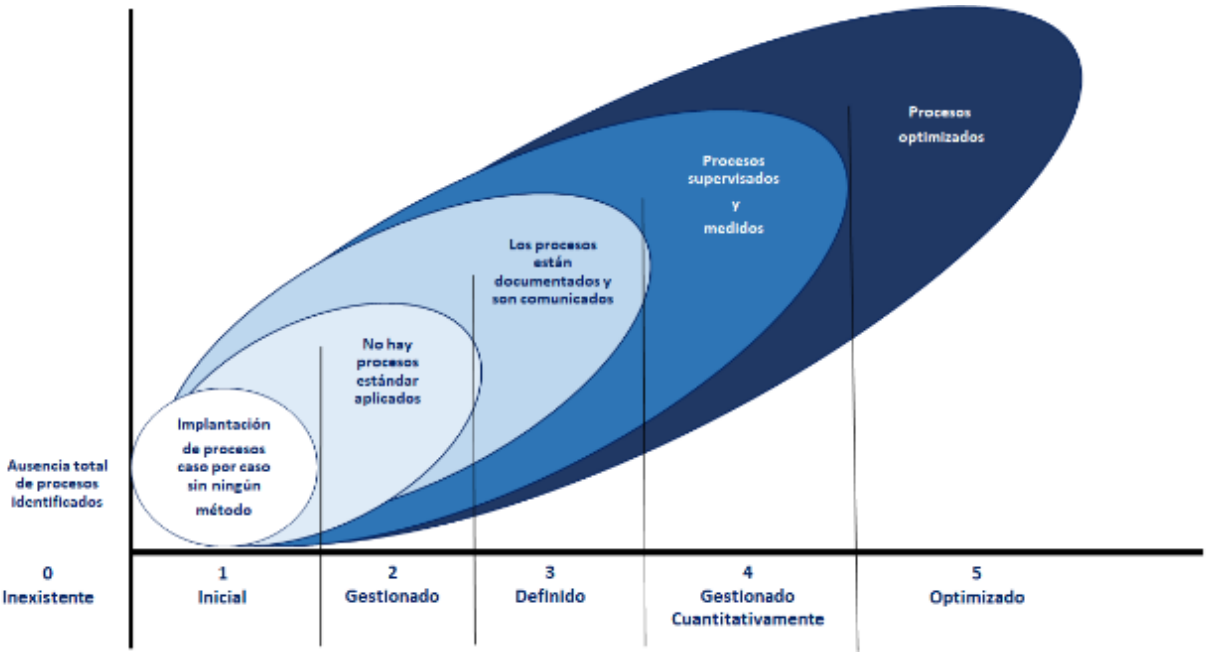
El análisis de brecha permite determinar los pasos para migrar de la situación actual a un estado futuro deseado, es así que, el análisis debe desarrollarse en las siguientes etapas:

1. Determinar el estado actual: Identificar procesos y controles de seguridad vigentes.
2. Identificación de objetivos: Determinar el nivel de madurez, se recomienda utilizar la metodología de la "*herramienta de evaluación de la seguridad cibernética (FFIEC)"*, la cual ha sido explicada en capítulos anteriores.
3. Análisis de las brechas: Permitirá identificar las diferencias entre los controles de seguridad actuales en la Organización y los definidos por la ISO 27032 (norma en la cual se basa la herramienta del FFIEC), con la finalidad de determinar los procesos que necesitan ser mejorados y robustecidos. Adicionalmente, el análisis de brecha proporciona la base para identificar y medir la inversión necesaria en tiempo, dinero, recursos humanos y herramientas tecnológicas para la aplicación efectiva de un programa de Ciberseguridad.

Gráfico 23. Mapa inicial del análisis de brecha esperado.

Elaboración propia, en base a: **(Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012).**

Gráfico 24. Mapa evolutivo de las etapas del análisis de brecha esperado.



Elaboración propia, en base a: **(Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012).**

5.3.2.3 Liderazgo del responsable de la gestión de Ciberseguridad.

El líder del proyecto de gestión de Ciberseguridad, debe elaborar un caso de negocio para coadyuvar a planificar y tomar decisiones respecto a las oportunidades, opciones y el momento adecuado para realizar las diferentes acciones que permitan llevar adelante el proceso. En esta etapa, lo que se busca es demostrar los beneficios que se pueden esperar como consecuencia del proyecto, incluyendo la metodología que permita cuantificar el proyecto y poder en función al riesgo priorizar la mejor forma de invertir en recursos humanos y tecnológicos. Señalar como aspecto importante que el caso de negocio debe poder mostrar más allá de una ventaja competitiva comercial, el cómo

puede ayudar a la Organización a verse impactada en cuanto al gasto por pérdidas, reputación, procesos legales y el respectivo costo de oportunidad que esto implica.

Una parte crucial del caso de negocio es poder determinar en función al presupuesto asignado la conformación del equipo que va trabajar en el programa, por lo que deberá decidir entre:

- Empleados Internos: Si bien a primera vista puede ser más económico, debe tomarse en cuenta la curva de aprendizaje, así como el tiempo de negociación para que los colaboradores puedan cambiar de área y un punto crucial será convencer a estos funcionarios de que migren voluntariamente a la nueva unidad, porque será la única forma de asegurar el compromiso de cada miembro del grupo de cara al éxito del programa.

- Consultor externo: Si bien es la más ágil de las opciones, permitirá un equilibrio entre avanzar en el proyecto de forma eficiente y sin cometer errores hasta la transferencia de conocimiento a los funcionarios que una vez se retire el consultor quedaron a cargo de la gestión de la Ciberseguridad. Sin embargo, para optar por esta opción primero hay que validar que se cuente con el presupuesto requerido para poder contratar al experto y por otro lado como desventaja se tendrá que tener claro que al inicio del proyecto el consultor deberá avanzar lento, debido a que tiene que aprender los procesos propios de la Organización.

  Finalmente, se recomienda esta opción solamente en caso de no contar dentro la Organización con un experto al menos en temas de riesgos, seguridad de información y sistemas.

- Empleados Internos y la guía de un experto externo: Es la opción más eficiente y recomendable, debido a que los equipos podrán trabajar juntos y la transferencia de conocimiento será más eficiente. Debe quedar claro que para que esta opción tenga resultados satisfactorios tanto el consultor como el equipo de trabajo deben funcionar cohesionados y bajo acuerdos previos de responsabilidades y tareas.

Presupuesto y Recursos:

El implementar un programa de gestión de Ciberseguridad requiere recursos y presupuestos, por lo cual será necesario que el responsable a cargo tome en cuenta los siguientes puntos:

Costo de los empleados y el tiempo:

Independientemente del trabajo diario, debe considerarse que la planificación, implementación y mantenimiento de un programa de gestión de Ciberseguridad toma tiempo de los funcionarios de cara a capacitaciones, elaboración de documentos, procesos, normas y controles.

Instalaciones, equipos y bienes consumibles, sistemas de tecnología de información y comunicación:

Será necesario que la Organización este consiente que debe realizar inversión de dinero en nuevas tecnologías y herramientas de cara a monitorear y prevenir los riesgos a los que se expone. Sin embargo, debe señalarse que en el caso de una Entidad Financiera y de acuerdo con su nivel de madurez deberían contar con herramientas ya en uso.

Una de las inversiones más importantes son las herramientas de recuperación de desastres, debido a que no suele ser la opción de compra inicial para ninguna Organización. El plan de recuperación de desastres, funciona con herramientas donde los datos y la tecnología están disponibles tanto en su ubicación en los servidores de resguardo habitual (sitio primario), como en un centro alterno (sitio secundario) utilizado en caso de desastres. Debido a la evolución de la tecnología, ya no es necesario contar con un servidor de respaldo en una ubicación alterna diferente a la del servidor primario, sino que puede encontrarse en la nube.

Dependiendo el análisis que se realizase respecto al perfil de riesgo y madurez de la Organización, la Entidad debe validar con que herramientas cuenta y posteriormente realizar un cronograma de tecnologías a implementar, de manera enunciativa, se presenta la priorización realizada por la Entidad Financiera Boliviana utilizada como guía:

Cuadro 19. Esquema de priorización de herramientas tecnológicas.

HERRAMIENTAS DE PRIORIDAD 1	
SOC	Definición IMF Business School: Centros de Operaciones de Seguridad, realiza seguimiento y análisis a la actividad en redes, servidores, bases de datos, sitios web y otros sistemas, buscando actividades anómalas que puedan indicar un incidente o compromiso de seguridad. Busca garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente.
Antimalwere	Tibor Moes, Fundador de Software Lab, lo define como, "Programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI". Los términos antivirus y antimalware se utilizan como sinónimos.
Antispam	El Diccionario de informática y tecnología, lo define como, "Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados". Su principal objetivo es lograr un buen porcentaje de filtrado de correo no deseado.
Virtual Patching	B - Secure lo describe como, "Protección de servicios y aplicaciones ante amenazas en el momento adecuado". Trabaja desde la capa de seguridad, analizando tráfico e interceptando ataques en tránsito, de forma tal que tráfico malicioso no alcance las aplicaciones y sistemas operativos. Permite recibir protección de parches de actualización sin tener que realizar su instalación y sin tener que interrumpir la operación normal.
Filtro Web de Contenido	Kaspersky lab lo describe como, "Elemento de software diseñado para restringir sitios web que un usuario puede visitar en su ordenador, pueden utilizar una lista blanca o una lista negra". Lista blanca: Ofrece acceso a sitios seleccionados específicamente; Lista negra: Restringe el acceso a sitios no deseados determinados por los estándares instalados en el filtro. Busca en la URL y en el contenido del sitio las palabras clave restringidas y a continuación bloquea o permite la conexión.
IDS/IPS	La empresa de seguridad INFOTECS, lo describe como: "Sistema de prevención de intrusos, dispositivo de seguridad fundamentalmente para redes, que se encarga de monitorear actividades a nivel de red y/o aplicación, con el fin de identificar comportamientos maliciosos, sospechosos e indebidos". Permite reaccionar ante ataques en tiempo real mediante una acción de contingencia

Fuente: Elaboración propia, en base a: **(Entidad Financiera Boliviana, 2019).**

Cuadro 20. Esquema de priorización de herramientas tecnológicas (continuación).

HERRAMIENTAS DE PRIORIDAD 1	
DLP	TechTarget España lo define como: "Prevención de pérdida de datos (DLP) es una estrategia para asegurar que los usuarios finales no envíen información sensible o crítica fuera de la red corporativa. Monitorea y controla las actividades de punto final y se utilizan para filtrar flujos de datos en la red corporativa y proteger los datos en reposo.
SIEM	SOFECOM, describe al SIEM (información de seguridad y gestión de eventos) como: "Tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas". Centraliza el almacenamiento y permite un análisis casi en tiempo real de lo que está sucediendo, detectando patrones anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad.
NAC	SECUTATIS, establece: "El Control de Acceso a la Red (Network Access Control) asegura que todos los dispositivos que se conectan a las redes internas de la organización cumplen con las políticas de seguridad definidas a fin de evitar amenazas y ataques".
WAF	Web Application Firewall se conoce como "Dispositivo hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques específicos en Internet". 2 tipos de WAF: Los que se residen en la red y los que se basan en el servidor de aplicaciones
Vulnerability scanner	El Diccionario de informática y tecnología, lo describe como: "Escáner de vulnerabilidad diseñado para evaluar computadoras, sistemas informáticos, redes o aplicaciones en busca de debilidades conocidas".
IDS/IPS	El Diccionario de informática y tecnología lo describe como: "Sistema de prevención de intrusos, dispositivo de seguridad fundamentalmente para redes, encargado de monitorear actividades a nivel de red y/o aplicación, con el fin de identificar comportamientos maliciosos, sospechosos e indebidos, a fin de reaccionar ante ellos en tiempo real mediante una acción de contingencia". La ventaja respecto a firewalls tradicionales es que toman decisiones de control de acceso basadas en el tráfico y no en direcciones IP.

Fuente: Elaboración propia en base a: *(Entidad Financiera Boliviana, 2019)*.

Cuadro 21. Esquema de priorización de herramientas tecnológicas (Continuación 2).

HERRAMIENTAS DE PRIORIDAD 2	
Anti-DDOS	CLARO, a través de su departamento de soluciones de negocio, lo describe como: "Servicio que permite mitigar un ataque distribuido de denegación del servicio a un sistema de computadoras o red que están expuestos a la red pública de Internet".
EMM	Computer World de soluciones de negocio TI, lo define como: "Conjunto de servicios y tecnologías diseñados para proteger los datos corporativos en los dispositivos móviles de los empleados". Protegen la propiedad intelectual y los procesos específicos que garantizan la seguridad de los datos
Wireless Controler	Control y monitoreo de la red de conexión inalámbrica y los usuarios que la utilizan, así como los accesos a la misma.
PAM	Joxan Crego, Identity and Access Management IT Specialist, lo describe como: "Gestión de accesos privilegiados que limita al máximo el uso de cuentas con privilegios administrativos de los sistemas core a través de la herramienta.
IAM	Sail Point de soluciones de negocio la describe como: "Gestión de la identidad y el acceso, busca garantizar que solo las personas adecuadas puedan acceder a los datos y recursos adecuados, en el momento adecuado y por las razones adecuadas".
DAM	Se conoce como "herramienta utilizada para apoyar la identificación y reporte de comportamiento inapropiado, ilegal o de otra forma indeseable en las Bases de Datos, con mínimo impacto en las operaciones y la productividad del usuario".
CASB	Gartner lo define como: "Puntos que refuerzan políticas de seguridad utilizadas en la nube, ubicados entre los usuarios y los proveedores de servicios cloud, para combinar e intercalar políticas de seguridad, relacionadas con la manera en la que se accede a los recursos"

Elaboración propia, en base a: **(Entidad Financiera Boliviana, 2019)**.

5.3.2.4 Elaboración del plan del proyecto:

Realizar un plan con la finalidad de contar con:

- Guía para la ejecución del proyecto;
- Mantener un registro escrito de la planificación;
- Tener clara la información de cara a la toma de decisiones;
- Facilitar la comunicación entre las unidades involucradas;

- Planificar las revisiones principales de seguimiento, alcance, contenido y fechas;

- Proporcionar un punto de referencia para medir la evolución del proyecto.

Contar con un programa de gestión de Ciberseguridad: La ISO 27003 en el punto 5 y cláusulas siguientes, define la necesidad de obtener la aprobación de la gestión para iniciar cualquier proyecto de Sistema de Gestión de Seguridad, debido a que el compromiso, comprensión y apoyo de la alta dirección son esenciales de cara al desarrollo e implementación del programa de gestión de Ciberseguridad de forma eficaz.

Los beneficios que se pueden obtener del apoyo de la alta dirección de cara al programa son:

- Mayor conocimiento respecto a la regulación, obligaciones contractuales y legales de la Organización, con la finalidad de evitar multas y sanciones de los reguladores.

- Asignación adecuada de recursos de cara a la seguridad de información y la Ciberseguridad.

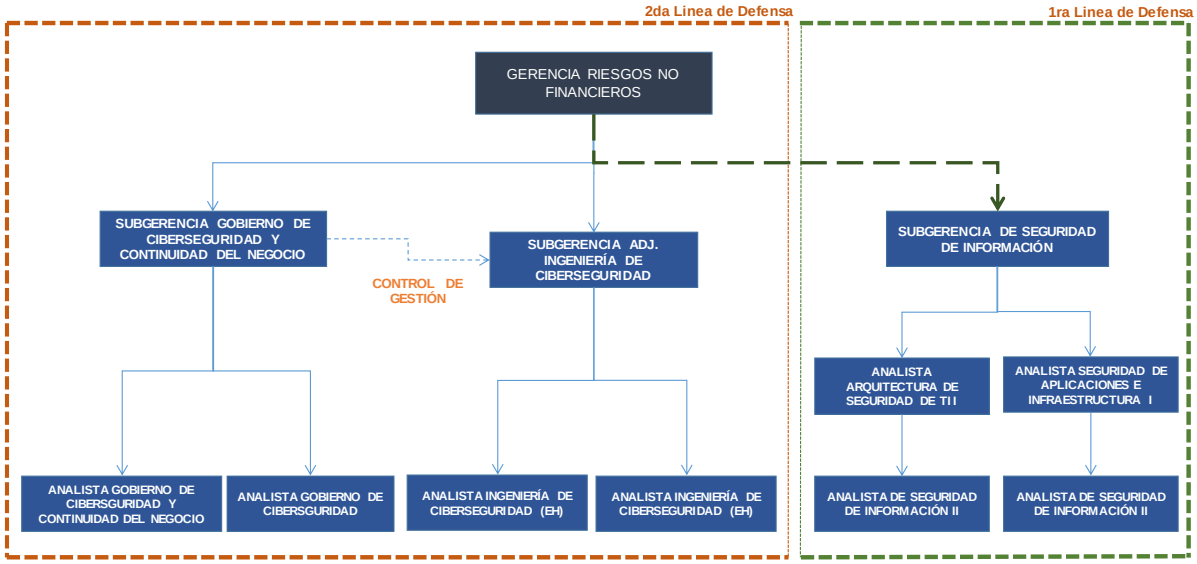
- Permitir que la alta dirección identifique los activos críticos y este alineado en cuanto a su adecuada protección.

- Contar con el respaldo de toda la Organización, con la finalidad de contar con acceso a información clara y precisa de cara a obtener el nivel de exposición al riesgo y gestionarlo adecuadamente.

Estructura Organizacional:

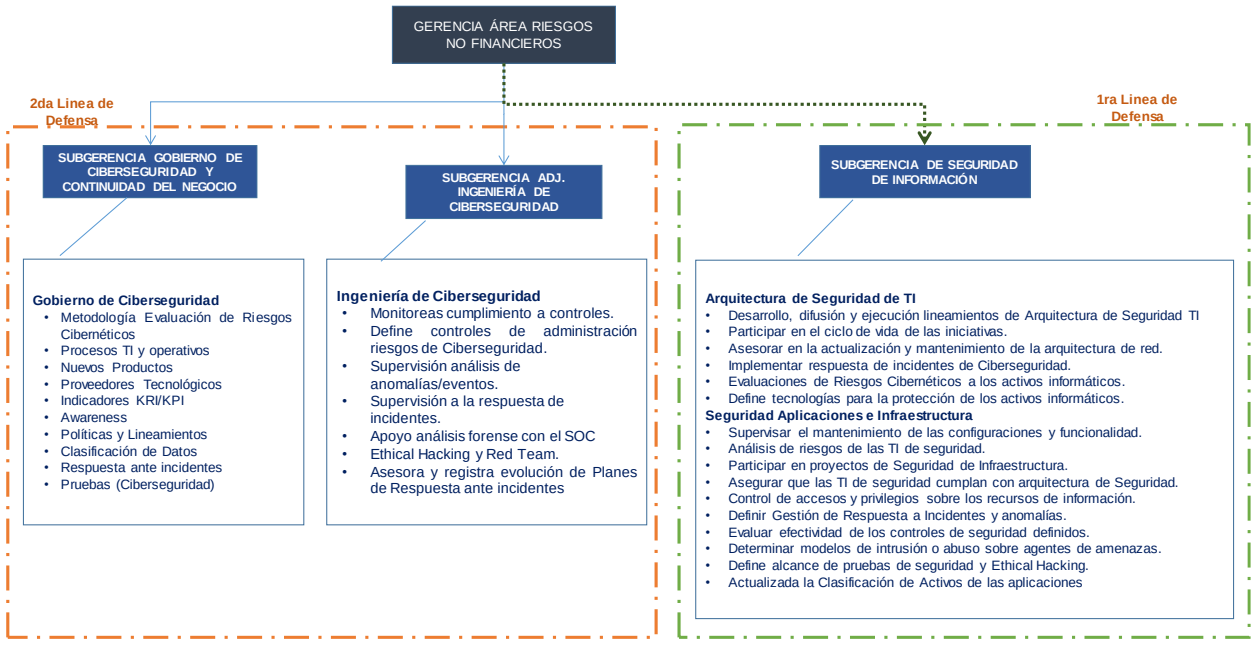
Más allá de que sea un requisito de la ISO 27001, contar con roles y responsables para garantizar la seguridad de la información es importante que la Organización cuente con una adecuada y ordenada asignación de funciones, manteniendo la independencia entre las líneas de defensa expuestas anteriormente. La estructura organizacional, se sugiere evolucione de acuerdo a lo expuesto en los gráficos siguientes según el nivel de avance del programa de implementación de la Ciberseguridad.

Gráfico 25. Estructura de Gestión de Riesgo - nivel Baseline.



Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019).**

Gráfico 26. Propuesta Estructura de Gestión de Riesgo – Evolving.



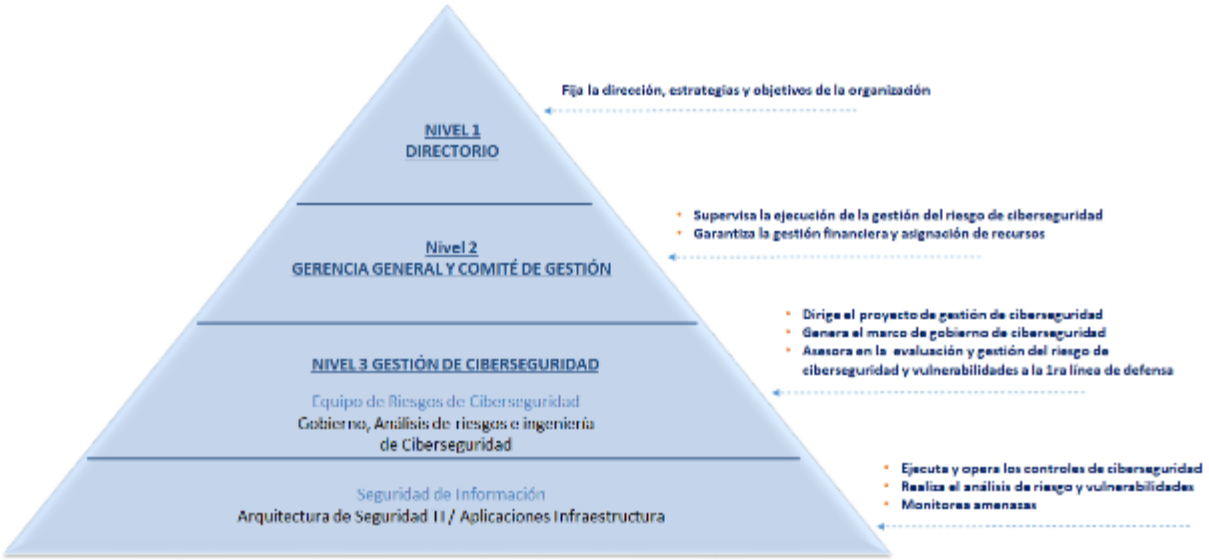
Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019).**

En cuanto a la estructura expuesta en el gráfico 26, señalar que la unidad de Seguridad de Información se mantiene dentro de la División de Sistemas y Tecnología, debido a que tienen a su cargo labores de primera línea la cuales son técnicas y especializadas, sin embargo la segunda línea estará dentro de la división de riesgos de la Organización, con la finalidad de controlar y verificar que se cumplan los controles, asesorar en la identificación de nuevas vulnerabilidades y riesgos dentro de la Organización. Cabe aclarar que la línea verde punteada de la gerencia de riesgos no financieros hacia

seguridad de información, establece más que una dependencia directa un rol de control indirecto que permita a esta gerencia tener claridad sobre las tareas y herramientas de gestión que administra la primera línea de defensa.

Finalmente, señalar que las organizaciones no solo deben contar con unidades específicas de gestión, sino también con un gobierno propio que coadyuve al programa de Ciberseguridad, monitoreo y supervisión de la gestión de este riesgo, por tanto, se propone la siguiente estructura:

Gráfico 27. Propuesta Estructura de Gobierno.



Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019).**

5.3.3 Política de Ciberseguridad.

Las políticas en una Organización y sobre todo en una Entidad Financiera, definen para el personal, sin describirla sistemáticamente, los diferentes lineamientos que deben seguir mientras trabajen en la Organización, es así que las políticas suelen tener tres niveles de manera general:

1. Políticas generales: Definen el marco general dentro el cual serán proporcionadas la seguridad de información, los aspectos centrales de cara a la continuidad del negocio y aquellos objetivos que busquen prevenir daños potenciales a los activos e incidentes de seguridad de la Organización a un nivel eficiente y eficaz. Ejemplo: Política de seguridad, Política de gestión de riesgos.

2. Políticas respecto a temas específicos: Definen el conjunto de normas o prácticas de marco general, relacionados a un tema específico. Ejemplo: Política de Ciberseguridad.

3. Políticas detalladas: Son aquellas que apoyan distribuyendo por sectores o temas específico las políticas señaladas anteriormente. Ejemplo: Política de control de accesos, uso de internet, destrucción de documentación o archivos, Evaluación de riesgo de Ciberseguridad y su metodología.

Debe señalarse que dependiendo el tamaño de la Organización y/o de la Entidad financiera, las políticas relacionadas a la gestión de la Ciberseguridad pueden estar relacionadas a otras ya vigentes (gestión de riesgos, continuidad de negocios, etc.), por lo tanto, pueden ser una referencia cruzada en lugar de armar un documento nuevo que pueda causar confusión.

La razón de ser la política de Ciberseguridad, es dar a conocer de forma clara e inequívoca, los objetivos y límites de la gestión de la Ciberseguridad, así como, definir el rol y alcance que tendrá dicha gestión como parte de la seguridad de información en la Organización.

Es importante señalar que las políticas de cara a la gestión de Ciberseguridad que se emitan, deben estar alineadas a la estrategia y objetivos de la Organización, además de incluir un compromiso de revisión y mejora continua respecto no solo a la Ciberseguridad en cuanto a su gestión de riesgo, sino también de cara a la seguridad de información de forma integral.

Cuadro 22. Esquema de políticas a implementar – Nivel Baseline.

Tipo	Politica Grupo 1	Tipo	Politica Grupo 2
Identity and Access	Autenticación y Autorización	Network	Segmentación Segura de Red
	Gestión de Credenciales		Inventario de Equipos de Red
	Identificación el nventario de Identidades		Seguridad de Acceso a Red
	Control de Accesos		Seguridad de Equipos de Red
Data Security	Clasificación de Datos		Seguridad Perimetral
	Uso Aceptable de Recursos Informáticos e Información	Cloud	Seguridad para SaaS
	Big Data y Analytics		Seguridad para PaaS
	Cifrado de Datos		Seguridad para IaaS
	Privacidad de Datos	Threat Intelligence	Registros de Auditoria
	Borrado Seguro de Información		Pruebas de Ciberseguridad
	Compartir y Trasferir Datos Interna y Externamente		Gestión de Vulnerabilidades
	Uso de Datos por partes Externas		Comunicación de Inteligencia de Amenazas
	Respaldo y Retención de Información		Identificación de Agentes de Amenaza
Software and Apps	Desarrollo de Software Seguro	Security Analytics and Orchestration	Identificación de Tecnologías de Seguridad
	Inventario de Software		Integración y Orquestación de Tecnologías de Información
	Software Seguro		Eventos y Anomalías
Endpoint and Mobile	Identificación de Endpoint		Respuesta a Anomalías e Incidentes de Seguridad
	Seguridad de Estaciones de Trabajo		Análisis Forense
	Seguridad de Servidores		
	Seguridad de Equipos Desatendidos		
	Seguridad de Equipos IoT		
	Seguridad de Servicios de Infraestructura		
	Seguridad de Dispositivos Móviles		

Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019) (Federal Financial Institutions Examination Council's (FFIEC), 2015).**

De cara al proceso de redacción y conciencia que dicha tarea requiere tiempo de carácter operativo se recomienda aplicar el siguiente flujo de trabajo:

Gráfico 28. Flujo de trabajo redacción de Políticas y Lineamientos.

Fuente: Elaboración propia en base a: **(Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001)**

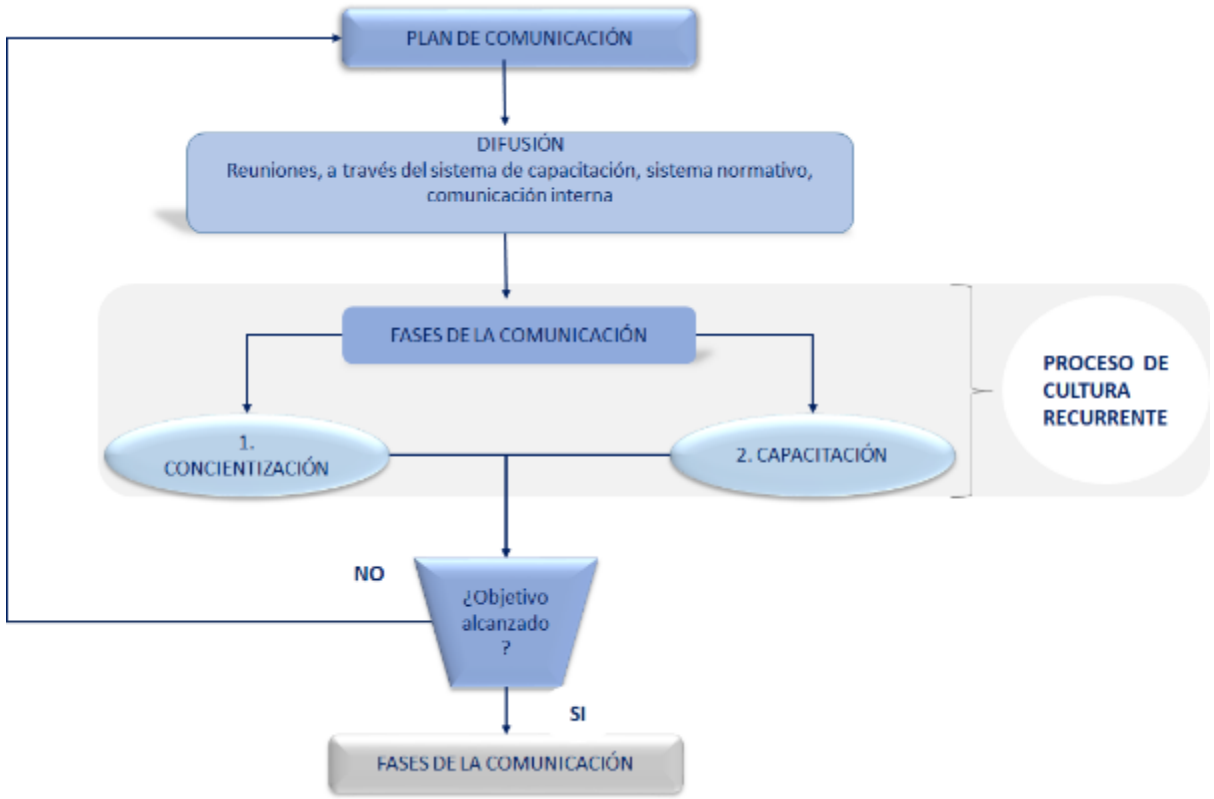
(International Organization for Standardization ISO/IEC 27032, 2012) (National Institute of Standards and Techonology U.S. Department of Commerce, 2019).

Una vez aprobada la política comienza la segunda etapa la cual todo gerente o responsable a cargo de la implementación del programa gestión de Ciberseguridad debe tener claramente identificado es el de la publicación y divulgación, con la finalidad de conseguir la comprensión de parte no solamente de los actores involucrados que han participado en la elaboración de la política, sino también de todo el conjunto de la Organización.

Es aconsejable que, para la primera publicación de la política general de Ciberseguridad, la misma sea puesta en conocimiento y si es posible firmada (al menos digitalmente), por todos los funcionarios de la Organización, incluyendo la alta gerencia y dirección. Otro punto importante, es concientizar a la Organización y a todo nuevo funcionario respecto a la política general de Ciberseguridad y su importancia en la Organización y cumplimiento.

En este sentido, y en línea con lo establecido por el Marco NIST y la ISO 27032, se aconseja la siguiente estrategia de comunicación y concientización de cara a la gestión de la Ciberseguridad.

Gráfico 29. Propuesta de Estrategia de Comunicación y cultura.



Fuente: Elaboración propia en base a: (Federal Financial Institutions Examination Council's (FFIEC), 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012) (National Institute of Standards and Techonology U.S. Department of Commerce, 2019).

5.3.4 Gestión del Riesgo de Ciberseguridad.

Es importante señalar que la gestión del riesgo de Ciberseguridad dentro de la Organización es vital y continua, debido a que permitirá desde identificar las vulnerabilidades que deben ser tratadas, gestionarlas y por ende reducir su probabilidad de ocurrencia, debido a que debe tenerse claro que los riesgos a los que se expone la institución no se eliminan al ser gestionados, sino que, se controlan reduciendo así ya sea su exposición, su probabilidad de ocurrencia o ambos, es por este motivo que surgen los conceptos de riesgo inherente[11] y riesgo residual[12].

Es de vital importancia que lo señalado anteriormente quede claramente comprendido por todos los responsables de riesgo de Ciberseguridad y a todos los niveles de la Organización a fin de tener a momento de que el gestor de riesgos y la unidad responsable del mismo se pongan de acuerdo en la evaluación y selección de controles y procesos adecuados de cara a la gestión de un riesgo conforme los niveles de tolerancia de la Organización para este tema en particular.

Para poder cumplir con una adecuada gestión de riesgos es necesario que la Organización defina su metodología y enfoque para la evaluación de riesgos, además de su apetito, considerando metas y objetivos que en este caso van en función a la Ciberseguridad.

La evaluación y tratamiento de riesgos debe ser la piedra angular de la gestión de la Ciberseguridad y debe procurarse que todas las medidas y/o acciones se tomen basadas en la gestión de riesgos, por tanto, elegir el método de análisis debe incluir enfoques tanto cualitativos como cuantitativos, con la finalidad de que para cada evaluación de riesgos se tenga la seguridad de que se está trabajando para coadyuvar a la estrategia, metas y objetivos de la Organización.

A momento de realizar una evaluación de riesgo es importante comprender:

- El entorno de negocio, la coyuntura, las condiciones culturales y contrastarlas con el apetito de riesgo de la Entidad Financiera. Precisar que, los aspectos culturales pueden llegar a tener un impacto significativo en una organización, tal es el caso de las Entidades Financieras que suelen tener estructuras formales y reguladas donde la selección de controles y su implementación son más estrictos al ser más adversas de cara a asumir riesgos, versus otro tipo de Organizaciones como las startup o fintech.

- No se trata de un proceso estático, por lo que la gestión de riesgos debe ser continua, debido a la evolución de las organizaciones en cuanto a la regulación y en especial al giro de negocio, los cuales van migrando en el tiempo, en especial de cara al mundo digital y el ciberespacio en busca de procesos más ágiles y menos costosos,

[11] *Riesgo inherente: Riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un choque negativo afecte la rentabilidad y el capital de la compañía.* **(Rodríguez)**

[12] *El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.* **(Rodríguez)**.

los cuales están generando nuevos riesgos y vulnerabilidades que deben ser atendidas de manera oportuna y ágil.

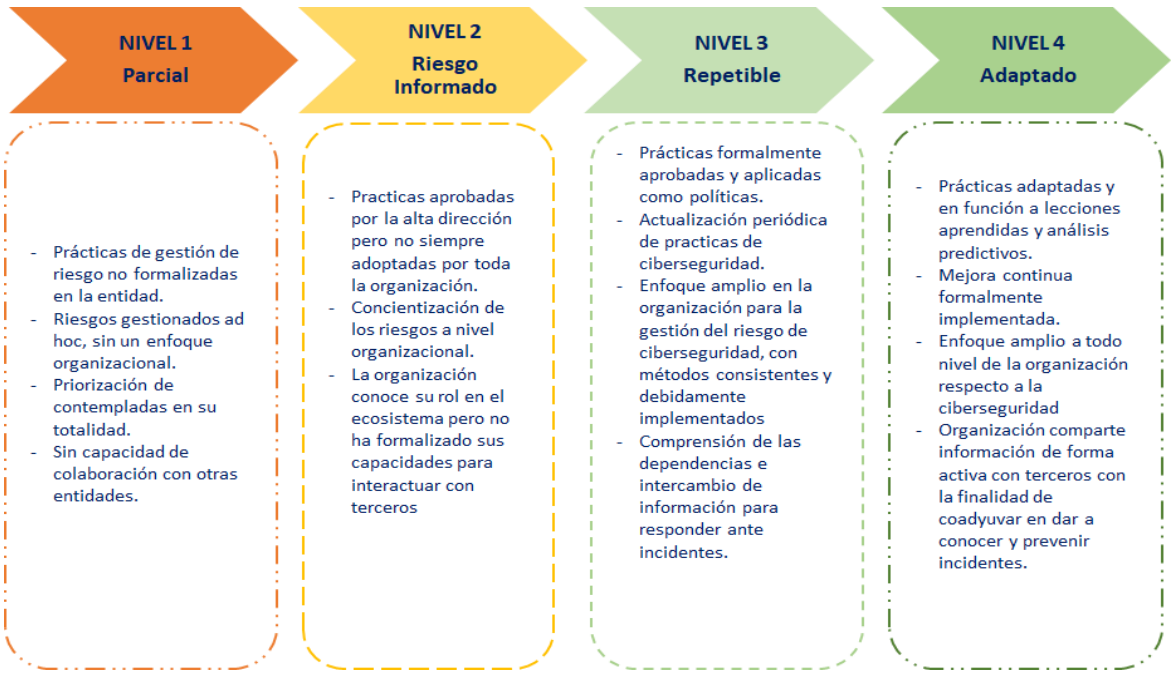
5.3.4.1 Marco de gestión del riesgo.

El Marco de gestión del riesgo establecido por el Marco de referencia NIST, detalla los niveles de implementación (Tiers), proporcionando el contexto acerca de cómo una Organización considera los riesgos y procesos de Ciberseguridad. El rango de los niveles empieza en el Parcial (Nivel 1) y llega hasta el Adaptable (Nivel 4), de esta forma se va describiendo la evolución de la Organización en función al rigor y sofisticación de las prácticas de gestión del riesgo de Ciberseguridad y la extensión en la cual debe ser informado a partir de las necesidades del negocio y es integrado dentro de las prácticas de gestión integral de riesgo de la Organización.

El proceso de selección de niveles o Tiers toma en cuenta las diferentes prácticas de la gestión de riesgos actuales, ámbito de las amenazas, requerimientos legales y regulatorios, objetivos de negocio/misión, cabe señalar que tiene especial similitud con la gestión del riesgo operacional al ser ambos de carácter no financiero y tener una estructura de causa, evento y consecuencia.

Señalar que la implantación exitosa del marco de referencia del NIST en una Organización, se basa en el logro de los resultados que se describen en el Perfil objetivo definido por la Organización y no sobre la determinación de los niveles. Dicho esto, señalar que, si bien mientras las organizaciones identificadas en el Nivel 1 o Parcial son alentadas a avanzar hacia niveles siguientes en busca de una mayor protección y de la reducción del riesgo de Ciberseguridad, parte fundamental de la decisión de cada Organización para evolucionar se encuentra en la relación favorable costo-beneficio.

Gráfico 30. Mapa de gestión del riesgo del NIST.



Fuente: Elaboración propia en base a: **(National Institute of Standards and Techonology U.S. Department of Commerce, 2019).**

Para comenzar a describir el programa de gestión es importante hacer referencia a la ISO 27005 y la ISO 31000, las cuales inicialmente señalan que los criterios para evaluar riesgos tecnológicos y de seguridad de información deben ser desarrollados considerando los siguientes aspectos:

- Valor estratégico del proceso de información del negocio;
- Naturaleza y tipo de causas que pueden producir un incidente o evento;
- Método de definición de probabilidades;
- Método para determinar el nivel de riesgo y tolerancia;
- Criticidad de los activos de información involucrados;
- Regulación legal vigente, reglamentos y obligaciones contractuales;
- Importancia de las disponibilidad, confidencialidad e integridad tanto operativa como del negocio;
- Tomar en cuenta las expectativas y percepciones de las partes interesadas, así como las consecuencias negativas para la Organización (perdidas económicas, sanciones, reputación, procesos legales).

Gráfico 31. Enfoque de la gestión de identificación de riesgos.

Fuente: Elaboración propia en base a: **(International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012).**

1. Identificación de los activos críticos:

Debido a que por un lado proteger todos los activos tiene un costo muy alto para cualquier Organización, es esencial que los activos críticos sean claramente identificados conjuntamente a sus líderes usuarios (responsables), con el objetivo de que se tome especial cuidado en su protección y monitoreo. La clasificación debe hacerse considerando:

a) Aspectos de negocio, tipo de información y datos almacenados, importancia de cara a la continuidad del servicio, consecuencias legales e impacto en pérdidas económicas y deterioro del activo.

b) Los criterios básicos que deben ser tomados en cuenta señalados por la ISO 27000 son la confidencialidad, integridad, disponibilidad y adicionalmente pueden incluirse a la autenticación, autenticidad, responsabilidad, no repudio y confiabilidad.

Será necesario que se desarrollen y especifiquen los criterios de impacto en términos del grado de daño y los costos, considerando para ellos la clasificación de los activos de información impactados, las diferentes brechas de la seguridad de información (como ser la pérdida de la confidencialidad, integridad y disponibilidad), operaciones que hayan sido degradadas, pérdida de valor económico de la Organización, daño reputacional, incumplimientos normativos y contractuales.

La forma utilizada por la Entidad Financiera boliviana es a través de un cuestionario que permite clasificar los activos de la siguiente manera la siguiente:

Gráfico 32. Esquema de clasificación de Activos.

Fuente: Elaboración propia en base a: **(International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001).**

Para llegar a esta clasificación que determina la clasificación del activo entre público, uso interno y restringido para luego valorar su proceso de custodia y control, el cuestionario cuenta con una evaluación por activo bajo los criterios descritos a continuación y en función a la nota obtenido se pondera y genera la clasificación.

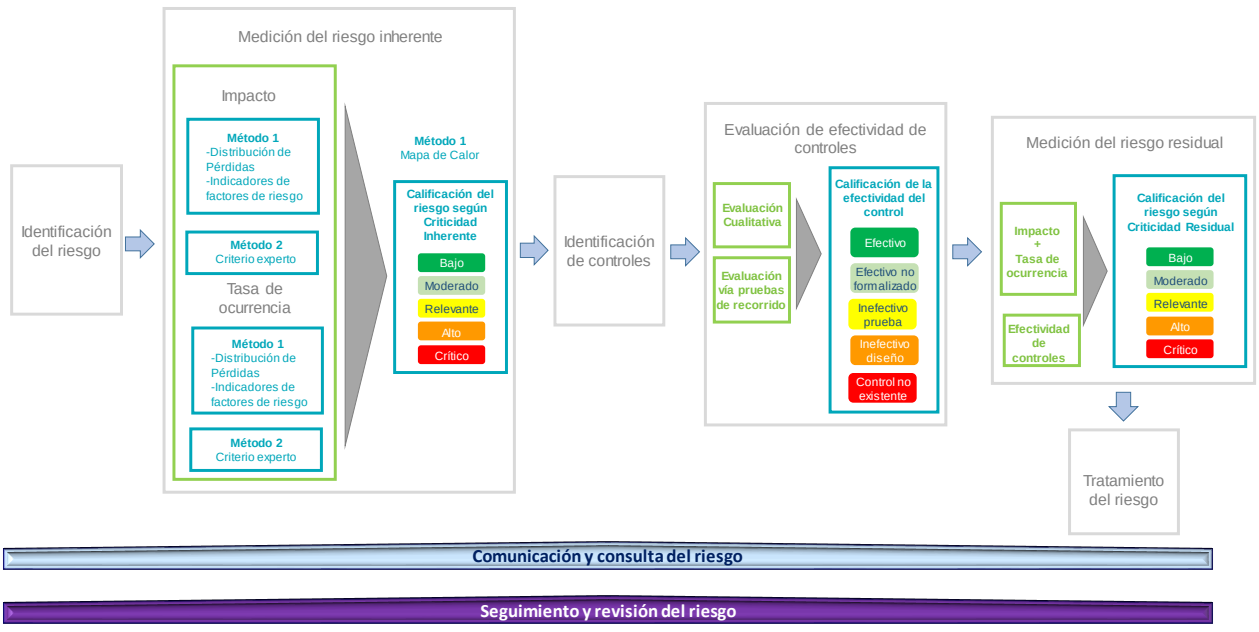
Gráfico 33. Esquema de identificación impacto y criticidad.

Fuente: Elaboración propia en base: **(International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001).**

2. Identificación de riesgos:

De cara al proceso de identificación de riesgos, se recurrirá al marco de referencia practicado por el Banco Boliviano guía que se utiliza en el presente trabajo, por lo que es importante señalar que su marco de gestión de riesgo está basado en la norma ISO 27005, la cual describe de forma clara los pasos a seguir que debe realizar una Organización de cara a contar con un proceso de gestión de riesgos, además de los procesos a utilizar para reaccionar en caso de un incidente.

Gráfico 34. Propuesta Marco de evaluación de riesgos.



Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019) (Comité de Supervisión Bancaria de Basilea, 2003) (Comité de Basilea en Supervisión Bancaria, Banco Internacional de Pagos, 2004).**

La identificación de un riesgo, se basa en una correcta descripción del mismo considerando como fuente su causa, evento y consecuencia, y se sugiere sea descrito en el siguiente orden:

- Causa y/o Vulnerabilidad: Motivo o razón que podría generar que el evento (riesgo identificado) se materialice dando como resultado pérdidas para la Organización.

- Evento y/o Amenaza: Es el riesgo identificado en las tareas o actividades del proceso y/o sistema evaluado.

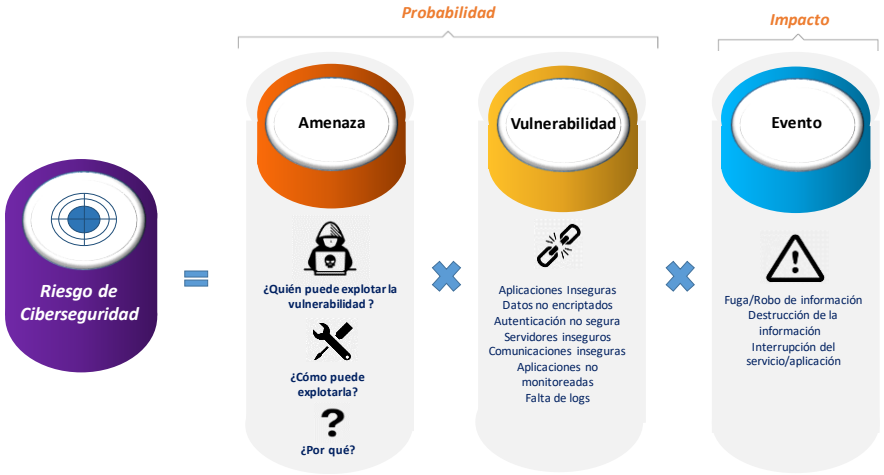
- Consecuencia: Es la posibilidad de pérdida o materialización del evento, pudiendo generar un impacto financiero, por pérdidas o daños en activos, sanciones y multas por incumplimiento regulatorio, Litigios, Indemnizaciones a Clientes.

Gráfico 35. Triangulo de identificación de riesgo.

Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019) (Comité de Supervisión Bancaria de Basilea, 2003) (Comité de Basilea en Supervisión Bancaria, Banco Internacional de Pagos, 2004).**

Finalmente, para lograr realizar la vinculación de cara a un análisis de riesgo de Ciberseguridad con la metodología de Riesgos de Operación antes expuesta, se sugiere al igual que la Entidad Financiera Boliviana sumar la *"Metodología Common Vulnerability Scoring System CVSS"* de la forma expuesta a continuación.

Gráfico 36. Metodología de evaluación y medición.



Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019) (Mell, Scarfone, & Romanosky, 2007).**

3. <u>Criterios evaluación del riesgo:</u>

Todo criterio de aceptación o apetito de riesgo debe incluir varios umbrales con niveles de riesgo deseados como objetivo, y los arreglos para que la alta dirección y los responsables de cada riesgo los acepten y convivan por debajo por encima de un nivel determinado o si hay que tratarlo mediante planes de acción que implementen controles de cara a reducir su exposición.

Los criterios de aceptación y medición pueden ser expresados como relación entre impacto económico y tasa de ocurrencia, como por ejemplo la utilizada por el banco boliviano estudiado.

a) Impacto:

Es el importe económico estimado de pérdida al materializarse el riesgo. Es la consecuencia que genera la materialización del riesgo de Ciberseguridad y será medido en 'Puntos de Riesgo'. La Entidad Financiera boliviana asignar un valor monetario para el 'Punto de Riesgo' con el objetivo de que la criticidad de los riesgos esté de acuerdo con el volumen de negocios que procesa.

Para determinar el impacto, se definen 2 formas para la estimación que son excluyentes y que deben de realizarse en el siguiente orden:

- Determinar el impacto de un riesgo identificado es la revisión de la Base de Datos de Eventos de Pérdida, por medio de la revisión de la historia de eventos o incidentes que estén relacionados con el riesgo de Ciberseguridad y determinar el impacto materializado del evento o nivel de exposición asumido en el incidente. Este ejercicio va a permitir al evaluador tener una medición del impacto del riesgo con datos objetivos. Se recomienda se considere el importe promedio del último año, si es que se contara con dicha información, caso contrario se sugiere remitirse a información del mercado conocida.

- El ‘Juicio de Experto’, para lo cual se debe consultar al experto la siguiente información, y en la medida de lo posible que dichas respuestas sean validadas con información histórica de fuentes conocidas:

    - El importe mínimo de impacto de materializarse el riesgo (Eje. importe mínimo de transacciones afectadas o servidores comprometidos).

    - El importe máximo de impacto de materializarse el riesgo (Eje. Importe máximo de transacciones afectadas, valorización de la información comprometida).

    - El importe promedio de impacto de materializarse el riesgo (tomar el promedio ponderado, considerando el volumen de operaciones, en la medida de lo posible).

A fin de evitar subestimar o sobre estimar un riesgo, se recomienda considerar el importe promedio de impacto definido.

Con los valores determinados ya sea por la primera forma o la segunda, se deberá colocar el importe de la exposición para ubicarlo dentro del rango que corresponda en la escala de impactos de la matriz de evaluación.

Tipos de Impacto:

- *Financiero:* Los efectos negativos en el cumplimiento de los objetivos financieros y rentabilidad esperada es de suma importancia y un evento de Ciberseguridad podría afectar sin lugar a duda este criterio.
- *Legal / Regulatorio:* Posibilidad de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos como ciberataques que decanten en responsabilidad civil y/o penal para la Organización.

b) Tasa de ocurrencia:

Número estimado de veces que un riesgo de Ciberseguridad identificado puede materializarse en un año. Para determinar la tasa de ocurrencia, se definen 2 formas para la estimación que son excluyentes y que deben de realizarse en el siguiente orden:

- Determinar la Tasa de Ocurrencia de un riesgo identificado a través de la revisión de la Base de Datos de eventos de pérdida por Ciberseguridad, mediante la revisión de la historia de eventos o incidentes, Es recomendable, considerar el promedio de tasa de ocurrencia anual que se tenga registrada y de no tener eventos compararlas con el mercado. De manera paralela, se recomienda también revisar el conjunto de indicadores de Ciberseguridad monitoreados por la Organización, de esta forma podrá tenerse visualización preventiva de los eventos.

Cuadro 23. Propuesta indicadores de monitoreo.

INDICADORES	DESCRIPCIÓN
KPI (key performance indicator)	1. Bases de datos y sistemas operativos fuera de soporte 2. Actualizaciones (parches) de seguridad no aplicadas a estaciones y servidores 3. Vulnerabilidades detectadas en Ethical Hacking 4. Estaciones o Servidores sin Antivirus 5. Estaciones sin validación de controles para acceder a la red corporativa 6. Pruebas de contingencia fallidas 7. Backups no ejecutados en el tiempo definido 8. Estaciones sin herramienta de prevención de fuga de información (DLP)
KRI (Key Risk Indicator).	1. Costo debido a incidentes de Ciberseguridad 2. Compromiso de registros críticos 3. Tiempo de indisponibilidad por incidentes de ciberseguridad 4. Nuevas aplicaciones o servicios que no cumplen con las políticas de Ciberseguridad 5. Controles que no cumplen los proveedores críticos respecto de seguridad

Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019).**

- El 'Juicio de Experto', Se debe consultar al experto las veces que de acuerdo con su experiencia se materializan los riesgos a través de eventos de pérdida y/o incidentes y así poder determinar la 'Tasa de Ocurrencia' estimada. De la siguiente tabla seleccionar la descripción que se aproxime a la tasa de ocurrencia identificada:

Cuadro 24. Tabla de tasa de ocurrencia identificada.

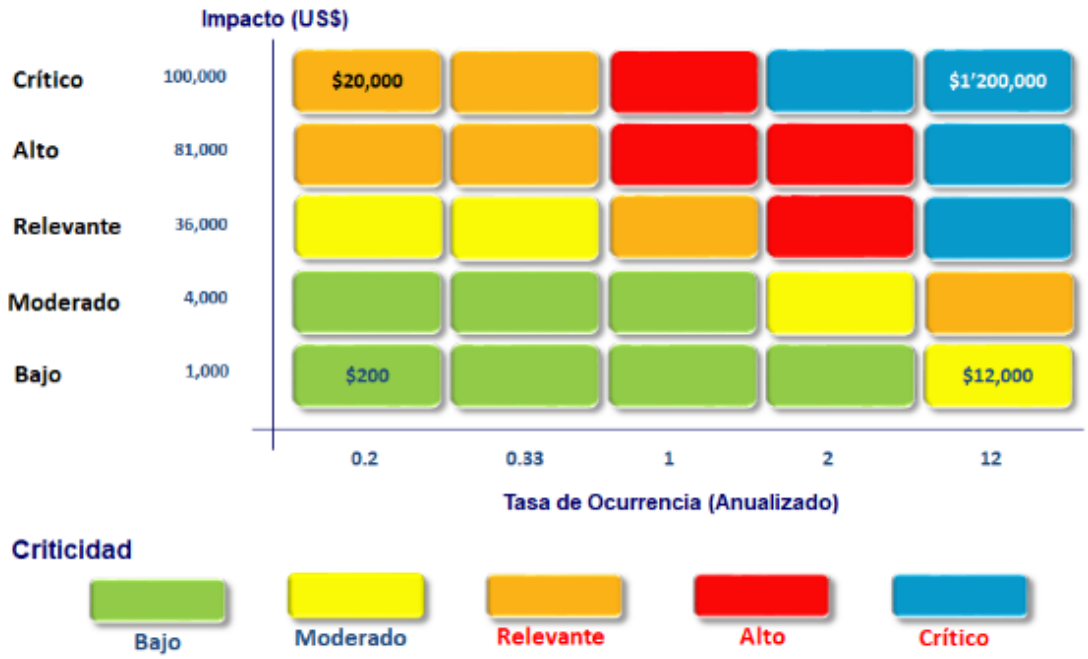
Nivel	Descripción
Casi Certeza	Eventos similares ocurren o pueden ocurrir todos los meses
Probable	Eventos similares ocurren o pueden ocurrir cada 6 meses
Posible	Eventos similares ocurren o pueden ocurrir 1 vez al año
Improbable	Eventos similares ocurren o pueden ocurrir 1 vez cada 3 años
Raro	Eventos similares ocurren o pueden ocurrir 1 vez cada 5 años o no existe registro del evento

Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019) (Comité de Supervisión Bancaria de Basilea, 2003) (Comité de Basilea en Supervisión Bancaria, Banco Internacional de Pagos, 2004).**

Estos dos criterios definirán la Matriz de Criticidad de Riesgos de la Organización, de tal manera que sobre éstas serán calificados los riesgos de Ciberseguridad que se identifiquen en las evaluaciones realizadas.

La multiplicación de los valores de impacto y de la tasa de ocurrencia da por resultado el nivel o grado de criticidad del riesgo, conocido como el Riesgo Residual. Los valores resultantes son: Bajo, Moderado, Relevante, Alto o Crítico.

Gráfico 37. Matriz de criticidad de riesgo.



Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019) (Comité de Supervisión Bancaria de Basilea, 2003) (Comité de Basilea en Supervisión Bancaria, Banco Internacional de Pagos, 2004).**

4. <u>Identificación de amenazas, vulnerabilidades (causas):</u>

a) Identificación de amenazas.

Será necesario identificar y tener claro los diferentes puntos de entrada para identificar las amenazas (que posteriormente puedan traducirse en riesgos), estos pueden darse de forma interna o externa, como ser:

- Propietarios o usuarios de los activos;
- Funcionarios de la Organización (a todo nivel);
- Especialistas de seguridad de información;
- Proveedores de servicio;
- Autoridades de gobierno;
- Clientes;
- Servidores, bases de datos y/o sistemas obsoletos o mal diseñados.

Una vez identificadas las amenazas y sus fuentes de acceso a la Organización, será necesario elaborar una base con la identificación de la amenaza su fuente u sus controles mitigantes, así como realizar un monitoreo de las fuentes de entrada

a través del SOC y en paralelo evaluar la necesidad de contar con firewall o antimalware, encriptación de datos, etc.

b) Identificación de vulnerabilidades o causa.

Para el caso específico de la Ciberseguridad es necesario tener claridad respecto a que las vulnerabilidades que, si bien son identificadas de la misma forma que los riesgos, a diferencia de los últimos no causan un daño en sí mismo, debido a que dependen de una amenaza o riesgo real que las explote.

Cabe señalar que en caso de existir una vulnerabilidad que no esté relacionada a una amenaza actual, puede no requerir la implementación de un control, pero si debe ser reconocida y monitoreada, con la finalidad de que en cuanto se identifique la amenaza se implemente un plan de remediación de la vulnerabilidad. Asimismo, es necesario señalar que un control incorrectamente implementado o funcionando mal puede constituirse en una vulnerabilidad.

Cuadro 25. Matriz de Identificación de vulnerabilidades y causas – Baseline.

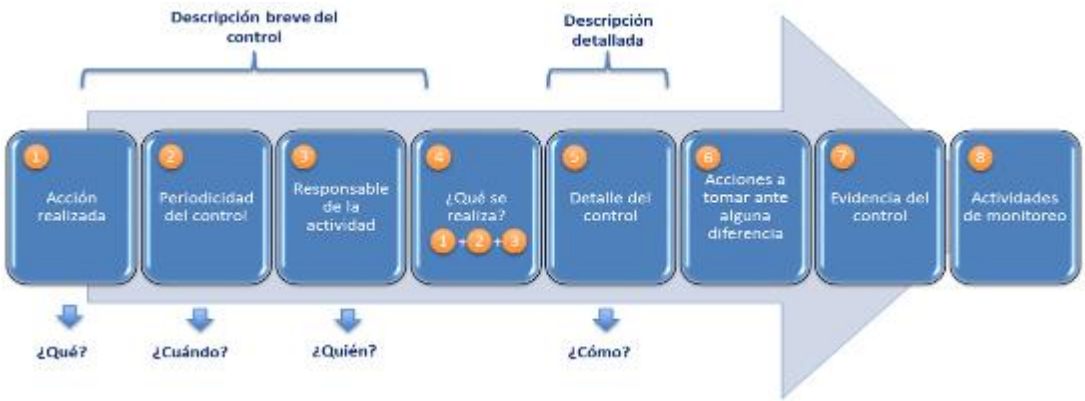
EVENTO / AMENAZA	CAUSA Y/O VULNERABILIDAD	CONSECUENCIA
Robo de equipo	Almacén sin supervisión	Pérdida monetaria
Corrosión	Sensibilidad a la humedad	Falla del equipo
Error de entrada de datos	Interfaz de usuario compleja	Base de datos corrompida
Escuchas telefónicas	Línea de comunicación si protección	Intercepción de las comunicaciones
Pirata informático	Transferir contraseña sin codificarla	Robo de información
Corrupción de datos	Ningún proceso de gestión documental	Documentación de Seguridad de Información obsoleta

Fuente: Elaboración propia, en base a: **(Comité de Supervisión Bancaria de Basilea, 2003) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012).**

5. <u>Identificación de controles:</u>

Una vez identificados los riesgos, será necesario que se solicite a la unidad incluya los controles respectivos para su mitigación, en este sentido, cuando se habla de Ciberseguridad dependerá del presupuesto y el apetito de riesgo de la Organización para definir el tipo de control a implementar que puede ir desde una solución tecnológica hasta un control manual. Es así que, para una mejor precisión, la identificación y redacción de los controles debe ser tal que nos permita responder siempre cuatro preguntas ¿Qué?, ¿Cuándo?, ¿Quién? y ¿Cómo?

Gráfico 38. Proceso de identificación y redacción de un control desde el punto de vista de riesgos.



Fuente: Elaboración propia, en base a: **(International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012) (Graham, 2015).**

Cuadro 26. Clasificación de controles.

Nivel	Sub Nivel	Descripción
Preventivo	**De aplicación (automático)**	***Procedimiento o actividad que previene que un error, vulnerabilidad, ataque o evento de riesgo ocurra.*** **- Un programa de una aplicación computarizada que ejecuta el control.**
	Manual	***Procedimiento o actividad que previene que un error, vulnerabilidad, ataque o evento de riesgo ocurra.*** - Si la ejecución está a cargo de alguna persona.
Detectivo	**De aplicación (automático)**	***Procedimiento o actividad que identifica un error, vulnerabilidad, ataque o evento de riesgo después que la transacción ha ocurrido***. - Un programa de una aplicación computarizada que ejecuta el control.
	Manual	***Un procedimiento o actividad que identifica un error vulnerabilidad, ataque o evento de riesgo después que la transacción ha ocurrido.*** - Si la ejecución está a cargo de alguna persona.

Fuente: Elaboración propia en base a Entidad Financiera Boliviana. **(Graham, 2015) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO/IEC 27032, 2012).**

Una vez identificadas las amenazas y sus controles, el nivel y el sub nivel de los mismos, será necesario realizar una base que permita vincular riesgos y controles, con la finalidad de llevar un inventario por proceso de los riesgos a los que se expone la Organización. Señalar que de existir controles que mitiguen un determinado riesgo identificado, éste será residual y no inherente, siendo clasificado en función a la robustez y efectividad del control.

La calificación resultante de la evaluación de efectividad de controles, debe realizarse a partir de los siguientes aspectos:

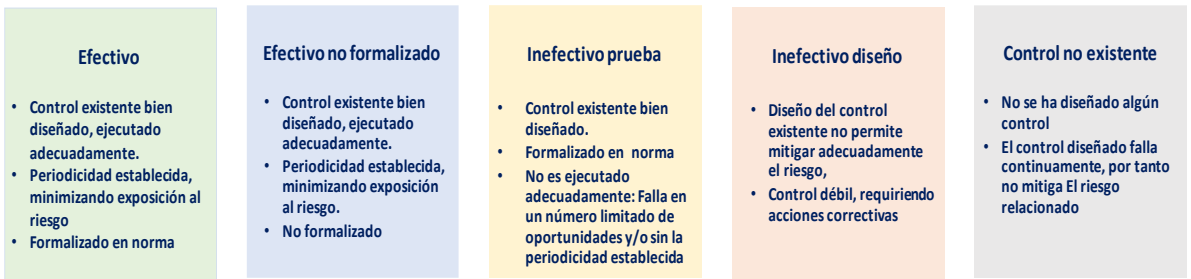
- Diseño: El control está bien diseñado para mitigar el riesgo;
- Ejecución: El control está funcionando tal y como está diseñado;

Para realizar esta evaluación, se han definido los siguientes criterios:

- Dirigido al objetivo: Está claramente definido qué riesgo se requiere mitigar y si el control mitigará impacto, frecuencia o ambos;
- Oportunidad: Hace referencia al momento que se ejecuta el control en relación a la ejecución de la acción o actividad a la cual es inherente el riesgo identificado;
- Alcance: Hace referencia al alcance del control para la validación y mitigación del riesgo;
- Frecuencia: Periodicidad con que se ejecuta la actividad de control;
- Madurez: hace referencia a la experiencia y conocimientos de la persona que ejecuta el control, así como antigüedad de implementación;
- Formalización: hace referencia a si el control está documentado y formalizado;
- Costo: En el caso de la Ciberseguridad es muy importante conocer el costo de implementación del control, buscando equilibrar la relación costo del control de seguridad respecto al riesgo.

La calificación resultante permitirá clasificar los controles de acuerdo al gráfico expuesto a continuación.

Gráfico 39. Definiciones de control.

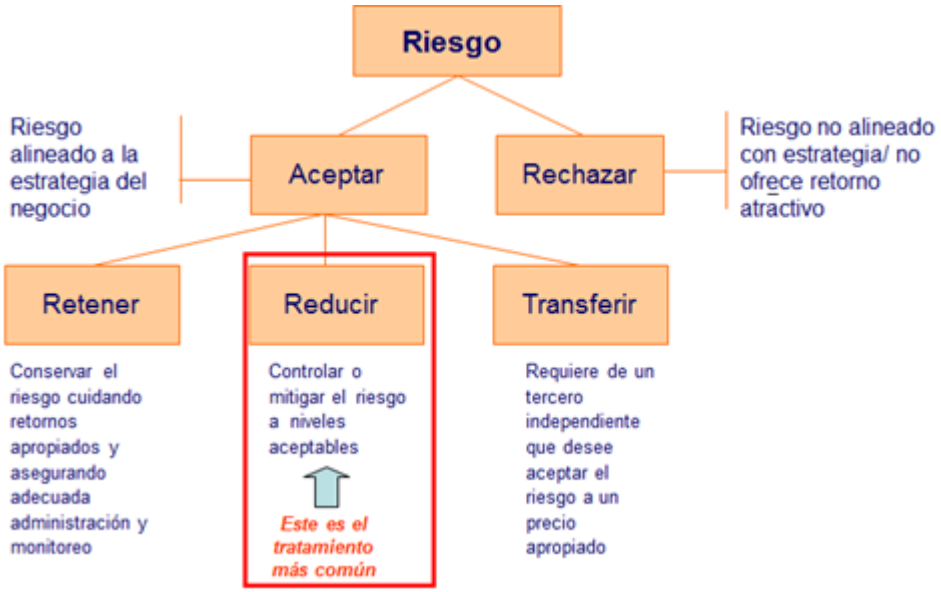


Fuente: Elaboración propia en base a: **(Entidad Financiera Boliviana, 2019). (Graham, 2015) (International Organization for Standardization ISO/IEC 27005 , 2001) (International Organization for Standardization ISO 31000 , 2009) (International Organization for Standardization ISO/IEC 27032, 2012).**

6. Tratamiento del riesgo:

Las estrategias de tratamiento para los riesgos de Ciberseguridad se usarán dependiendo de su contexto y nivel de criticidad calculado para el mismo, estos son:

Gráfico 40. Esquema de tratamiento de riesgo.



Fuente: Elaboración propia en base a **(Entidad Financiera Boliviana, 2019) (Comité de Supervisión Bancaria de Basilea, 2003) (Graham, 2015) (International Organization for Standardization ISO 31000 , 2009).**

El tipo de tratamiento Reducir se aplicará para aquellos riesgos residuales que resultan con un nivel de criticidad Relevante, Alto o Crítico. Para poder lograr el objetivo de este tratamiento de reducir el riesgo se requiere identificar y proponer planes de acción o controles. Los responsables de proponer y darle seguimiento a la ejecución de los planes de acción es el dueño del riesgo identificado.

7. Responsabilidad:

Al participar en el ciberespacio, las partes interesadas, deben aceptar y comprender la responsabilidad agregada respecto hacia terceros interesados o intervinientes ya sea de forma directa o indirecta, esto incluye los siguientes puntos:

- Reconocimiento: Reconocer el posible riesgo de que terceros puedan introducirse y/o intervenir en nuestro ciberespacio, sistemas de información, activos de información sin autorización.

- Notificación: Será necesario incluir a todas las partes interesadas externas a la Organización a momento de distribuir informes relacionados a la gestión de riesgos, incidentes y amenazas.

- Intercambio de información: Será necesario que las partes interesadas compartan un sistema o canal de comunicación en el que intercambien información referida a ciberataques, vulnerabilidades, etc. Para esto existen

sistema como el CSIRT que permite a las entidades compartir información sin exponer a la Organización de forma tal que los participantes del CSIRT puedan prevenir ataques similares.

- Apreciación del riesgo: Determinar el alcance en que las acciones y la presencia de las partes interesadas en el ciberespacio se convierte o contribuye a un riesgo para otra parte interesada.

- Riesgos legales y regulatorios: Al conectarse al ciberespacio, los diferentes límites legales y regulatorios definidos originalmente, son difíciles de distinguir y gestionar, por lo que es necesario validar la aplicación de este estamento legal.

8. Retiro del servicio o del sistema:

   Una vez que un sistema o servicio ya no es necesario, debe ser retirado de forma segura y monitoreada garantizando que los servicios e interfaces relacionadas no se vean afectadas. Es así que, toda la información que contenía debe ser clasificada y de ser el caso copiada para resguardo, respecto a información relacionada con la seguridad debe ser invalidada, con la finalidad de garantizar que los sistemas con los que se interconecta no hayan sido comprometidos.

   Cabe señalar que, en el caso de monitorear obsolescencia tecnológica de los sistemas y aplicaciones es una buena práctica contar con un indicador que permita identificar preventivamente los sistemas, servidores que se quedaran obsoletos o que simplemente ya cumplieron su ciclo de vida, esto con el objetivo de tener un cronograma de trabajo y remplazo en función al riesgo y su soporte al negocio.

9. Coherencia:

   Debe tenerse claridad en toda la Organización que el enfoque a la gestión de riesgos se aplica en todo el ciberespacio, y dentro este enfoque, se les asignan responsabilidades tanto a los consumidores como a los proveedores del ciberespacio con actividades específicas, como la planificación de escenarios de contingencia, recuperación de desastres y el desarrollo e implementación de programas de protección de sistemas que estén bajo su control y/o administración.

6. El costo de no contar con una estrategia de Ciberseguridad

El presente capítulo se realiza con el interés de evaluar y cuantificar la exposición del riesgo de Ciberseguridad al no disponer de una estrategia y metodología en un entorno digital que recién está comenzando a exponerse.

Para llevar adelante el análisis, se utiliza el estudio de Accenture Security, denominado The Cost of Cibercrime emitido el año 2019, dicho análisis permitirá a los líderes de la Ciberseguridad en las organizaciones financieras contar con una herramienta base que les permita justificar frente a la alta dirección e incluso a la junta de accionistas el porqué es necesario invertir en herramientas que permitan proteger a la Organización de los ciberataques y más aún tener a la Ciberseguridad como un pilar de la transformación digital.

6.1. Evolución del Cibercriminen.

Debido al panorama digital en constante cambio, las Entidades Financieras deben más que nunca seguir el ritmo de las ciberamenazas, es así que previo a exponer los puntos de la Ciberseguridad que agregan valor a una Organización, es necesario tener claro:

- **Objetivos en evolución:** Si bien el robo de información está situado como el ataque más ágil y costoso, los datos ya no son el único objetivo, debido a que los ciberatacantes están buscando acceder a los sistemas centrales de información, servidores, de control, de contingencias, etc., con la finalidad de interrumpir y destruir el servicio y la continuidad del negocio.

- **Impacto en evolución:** Si bien los datos siguen siendo un objetivo, el robo no siempre es lo que se busca, toda vez que una nueva ola de ciberataques ve que la vulneración de los datos ocasiona desconfianza y daña la reputación de la Entidad Financiera y por otro lado buscan dañar o alterar la integridad de esos datos para destruir la estructura base de la Entidad Financiera ocasionando daños económicos y de negocio graves de no ser restituidas de manera rápida.

- **Técnicas en evolución:** los cibercriminales están adaptando sus métodos de ataque, utilizando la capa humana (al ser esta el eslabón más débil) como un camino a los ataques. Los tipos de vulneración que han ido en aumento son la suplantación de identidad (phishing) y la información maliciosa.

Según el informe de Accenture "Asegurando la economía digital", las empresas de todos los rubros cada vez dependen más de la tecnología, por lo que contar con una adecuada gestión de las herramientas digitales es crítica para su crecimiento y sostenibilidad, es así que, según el mencionado estudio, el 90% de los principales negocios de cara a la innovación digital generan riesgos inherentes nuevos a los que antes no se estaba expuesto, en el mismo sentido, el 68% de los líderes empresariales señalaron que estos nuevos riesgos de Ciberseguridad incrementan su probabilidad de ocurrencia a la par de la innovación digital que se va incorporando al negocio.

El ser humano como el eslabón más débil.

De los diferentes estudios utilizados y de los equipos ejecutivos encuestados por Accenture en el año 2018, se pudo identificar a la publicación accidental de información confidencial y los ataques internos dolosos realizados por los colaboradores como las principales causas de ciberataques exitosos.

Dicho esto, es que el rol de seguridad está en gran parte centralizado en generar cultura a través de capacitación continua y refuerzo de habilidades (por ejemplo, pruebas de phishing). Toda vez que los colaboradores, necesitan las herramientas e incentivos para ayudar prevenir, identificar y mitigar los riesgos cibernéticos, toda vez que la nueva coyuntura actual genera que la Organización ya no dependa solo de sus propias herramientas de protección para sentirse seguro, toda vez que hay nuevos factores como los proveedores, el trabajo remoto de los colaboradores, por lo tanto, capacitar a los empleados para que piensen y actúen teniendo en cuenta la seguridad es lo más urgente e importante, sin embargo las organizaciones suelen no otorgar los fondos suficientes en los presupuestos de Ciberseguridad.

6.2. La Ciberseguridad como inversión.

A medida que se incrementa el número de ataques cibernéticos, y toma un mayor tiempo poder resolverlos, el costo del cibercrimen sigue en aumento. Como ya se expuso en capítulos anteriores se ha podido observar muchos sigilosos, sofisticados y dirigidos ciberataques contra organizaciones públicas y privadas, en este sentido señalar que las diferentes organizaciones (no solo financieras), están sufriendo un incremento constante de violaciones de seguridad que van desde 130 en el año 2017 a 145 en 2018, es decir un incremento del 11%.

El impacto del cibercrimen en los diferentes tipos de organizaciones sean financieras, industriales y a la sociedad en general es sustancial, debido a que junto al creciente número de violaciones de seguridad, el costo total por ciberataques incremento por Organización de $us 11,7 millones en 2017 a $us 13.0 millones en 2018, lo cual equivale a un 12%, señalar que en cuanto al riesgo reputacional, el daño puede generar pérdida de credibilidad y confianza en la Organización, ocasionando pérdida de clientes, excesos de auditorías regularías, fuga de capitales de inversión, entre otros, es por eso que de cara al presente análisis solo se toma en cuenta el factor de pérdida de dinero efectiva la cual impacta en los Estados Financieros de la Organización.

Como puede verse en el cuadro 17 expuesto líneas abajo, el sector bancario y las industrias de servicios públicos siguen teniendo el costo más alto del cibercrimen con un incremento del 11% y 16% respectivamente entre 2017 y 2018.

Gráfico 41. Costo promedio anual delitos cibernéticos por industria (Millones de dólares).

Fuente: **(Accenture Security, 2019).**

Referencias de Inversión en Ciberseguridad.

Existen diferentes formas para poder evaluar el costo beneficio para una Entidad Financiera de invertir en la Ciberseguridad, sin embargo, una de las maneras más aconsejables es valorar en función al riesgo, pero viéndolo como una oportunidad de ingreso vinculada a mejoras en la protección de Ciberseguridad.

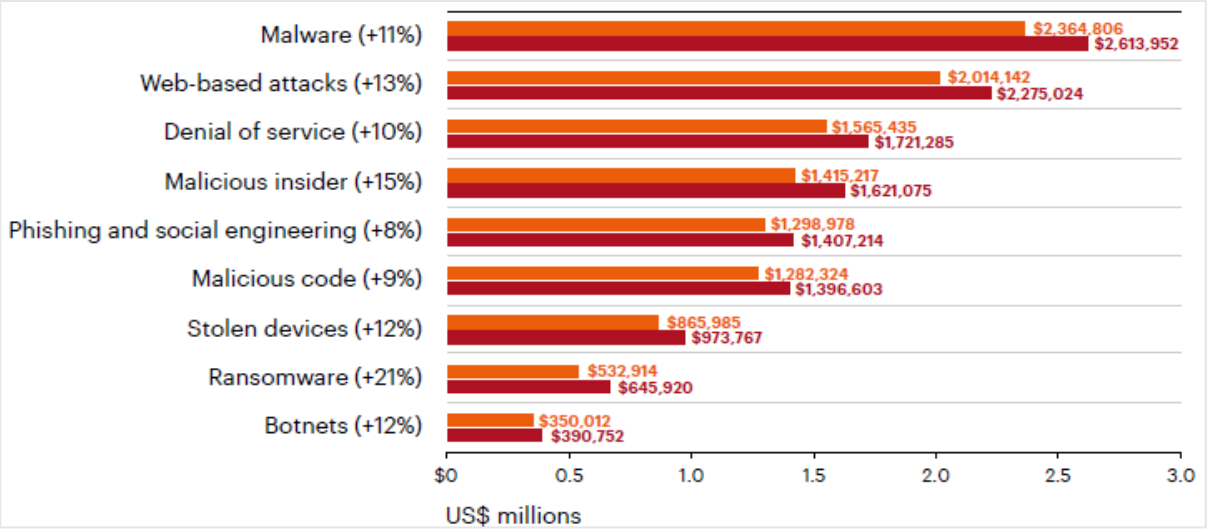
El criterio mencionado se explica en función a que mientras la protección mejora, menos ataques recibe la Organización, reduciendo así el costo de acción de defensa para soportar un ciberataque, y el costo de la pérdida por el delito cibernético. Asimismo, un factor difícil de medir cuantitativamente, pero que de forma cualitativa es vital para cualquier Organización y en especial para las Entidades Financieras, es la confianza de los consumidores financieros, el cual se considera combustible que impulsa la economía digital, por lo que al tener una Entidad Financiera reputación de ser digitalmente segura, dicha reputación lo posiciona de forma favorable en el mercado conduciéndolas a nuevas oportunidades de generación de ingresos.

Como puede verse en el cuadro 42 expuesto líneas abajo, el costo anual total de los diferentes tipos de ciberataques está aumentando, es así que si bien el Malware y los ataques basados en la web siguen siendo los más costos de cara a las pérdidas de la Entidad Financiera, el costo del ataque de ransomwere (21%) y de ataques por intrusos maliciosos o “malicious insider” (15%) han crecido más rápido en el último año.

Desglosando aún más el cuadro 42 expuesto a continuación, el malware sigue siendo el ataque que más dinero le cuesta a las organizaciones en un promedio de $us. 2.6 millones anuales, por otra parte, se encuentran los ya mencionados ataques internos

maliciosos los cuales cuestan alrededor de un promedio de $us. 1.6 millones anualmente por Organización.

Gráfico 42. Costo promedio anual: Tipo de ataque cibernético 2018 (Millones de dólares).



Fuente: **(Accenture Security, 2019).**

Por lo expuesto, señalar que los costos totales por delitos cibernéticos para una Organización en 2018 rondaron los $us. 13,0 millones, situación que trae a la mesa de la alta gerencia y la junta de accionistas la imperiosa necesidad de priorizar la inversión en la Ciberseguridad sobre otras necesidades de la Entidad Financiera, con la única finalidad de evitar pérdidas cuantiosas que superarían por mucho lo invertido en esta unidad o área de la Organización.

7. Consideraciones y Recomendaciones

7.1. Consideraciones

Los cambios tecnológicos y los riesgos a los cuales se enfrenta la Banca, son una consecuencia de las necesidades de la evolución y transformación tecnológica en la sociedad moderna, la cual exige una nueva forma de hacer negocio, en este entendido de cara a las personas individuales, si bien la tecnología y la interconectividad ha mejorado la calidad de vida, a su vez, han generado nuevas amenazas con las que deben aprender a convivir y gestionar. Algunas de estas nuevas amenazas son el robo, secuestro y el uso sin consentimiento de datos personales, el robo de dinero a través del hackeo de cuentas, además del poder de las grandes empresas tecnológicas como Facebook, WhatsApp, Google, incluso las Entidades Financieras respecto al manejo y mercadeo de información, los cuales lamentablemente las personas autorizan habitualmente sin saber ni leer los términos y condiciones.

Es así que, los principales riesgos de seguridad digital que merecen mayor atención de parte de las Entidades Financieras en el continente Latinoamericano son:

- El robo de base de datos en especial data crítica;
- El compromiso de credenciales de usuarios privilegiados.

Como ha logrado evidenciarse, los estudio realizados por la Organización de Estados Americanos (OEA), en 2018 demuestran que el 92% de las Entidades Financieras aceptaron haber sufrido ciberataques, siendo los principales ataques el Malware o código malicioso en el 80% de las Entidades Financieras y los siguientes ataques la violación de políticas clear desk (63%) y el phishing (57%), es así que, consultando la estadística brindada por Karspersky Lab entre enero y junio de 2018, América Latina recibió 510.671 ataques, con un promedio por día de 2.837.

Por lo expuesto, se ha podido dejar en claro que la Seguridad de Información y Ciberseguridad están tomando cada vez un lugar relevante en las mesas de decisión de las juntas de accionistas y la alta dirección de las Entidades Financieras, debido a que los hackers han identificado no solo a este tipo de organizaciones como fuente directo de ataques para el robo de dinero, sino más importante aún han podido identificarlas como una de las principales fuentes de información de datos a nivel mundial, situación que lleva a los diferentes reguladores y legislaciones a regular la responsabilidad de control y resguardo que deben tener estas organizaciones respecto a los datos que gestionan.

7.2. Recomendaciones

De cara a la Junta de Accionistas y la Alta Gerencia.

- Apoyar e incentivar un diagnóstico claro del nivel de protección y control que tienen respecto al riesgo inherente al que se exponen en función a la digitalización de su negocio.

- Por ningún motivo deben tomar la implementación y gestión de la Ciberseguridad solamente como un tema de cumplimiento normativo.

- La alta gerencia debe designar como responsable de la implementación en la Entidad Financiera a una persona que tenga influencia a todo nivel dentro de la Organización, de tal forma que pueda movilizar a la Entidad hacia el nivel de madurez deseado.

- Empoderar al Líder de la Ciberseguridad con la finalidad de que este pueda tener el poder de decisión necesario para llevar adelante el proyecto y posteriormente la gestión del riesgo de forma continua.

- Llevar adelante un seguimiento específico y esquematizado respecto al avance en la implementación de la gestión de la Ciberseguridad al interior de la Organización.

- Facilitar al Líder de la Ciberseguridad el presupuesto, equipo y las herramientas necesarias para llevar adelante una adecuada gestión de la Ciberseguridad.

- Aprobar el alcance de evaluación de auditoría en función al programa NIST.

De cara al Líder de la Ciberseguridad:

Al ser el actor principal, debe tener claro que necesita el apoyo de la alta gerencia y el directorio de la Organización, es así que debe contar con un plan de trabajo en función a un diagnóstico de la situación real de la Organización respecto al riesgo de Ciberseguridad, conociendo claramente el negocio y la operativa de la Entidad Financiera, con la finalidad de que su gestión aporte un valor real desde el punto de vista de la gestión del riesgo.

Debe tener claridad la diferencia entre su rol como líder de la Ciberseguridad versus la Seguridad de Información, tomando especial atención en que la Ciberseguridad es una disciplina que forma parte de la seguridad de Información, en este sentido, debe estar claro el alcance de cada rol:

- **Seguridad de Información:** Trata con la información y sus mecanismos de control y prevención, independientemente de su formato, ya sea física o digital.

- **Ciberseguridad:** Se refiere de manera específica a la protección de los activos digitales de la Organización, por lo que la información procesada, almacenada o transportada.

El Líder de Ciberseguridad debe tener claridad de:

- Las diferentes categorías de amenazas y prestar mayor atención a las que se relacionan con la actividad humana y/o maliciosa.

- Los actores definidos desde la literatura liderada por la ISO 27032 y estos se interrelacionan en la gestión del riesgo y controles.

Debe liderar conjuntamente con el equipo de auditoría el diagnóstico de la Entidad Financiera de cara al perfil de riesgo que su Organización tiene, para tal motivo se sugiere utilizar el Framework de Ciberseguridad del FFIEC, debido a que al ser un marco auditable que da absoluta claridad del nivel de madurez tecnológico y el perfil de riesgo que debe tener la Entidad.

Tendrá la responsabilidad de llevar adelante la creación de un gobierno y estructura para la atención de la Ciberseguridad delimitando de manera precisa y acordada las funciones y responsabilidades en cada línea de defensa.

Llevar adelante un análisis específico respecto a la identificación de las partes interesadas con la finalidad de generar una estrategia de comunicación y negociación con las mismas para realizar cambias de forma estratégica y asegurar el éxito de esta labor.

Identificar a través de un análisis PEST de la Organización, identificando claramente:

- Entorno político - legal sobre el cual habrá que trabajar, en cuanto este factor es necesario que se tenga el cuidado suficiente para delimitar los temas orden interno y externo.

- Entorno económico, deberá poder identificar el ciclo económico de la Organización con la finalidad de poder realizar el presupuesto de cara a la compra de herramientas tecnológicas de control, monitoreo y capacitación, así como para la contratación y/o capacitación de los recursos humanos especializados que llevaran adelante la tarea. Este punto es clave, debido a que la inversión en estos recursos es costosa por lo que de no estar económicamente solidos el Líder de Ciberseguridad deberá priorizar la adquisición de las mismas en función al riesgo con el que convive la Entidad.

- De cara a al tema Socio-Cultural, es importante entender la cultura de la Organización, en función a sus pilares estratégicos, así como a su público objetivo, misión y visión, toda vez que, de ser una Entidad Financiera que tiene su foco en atención de segmentos presenciales, naturalmente su nivel de exposición al riesgo tecnológico será menor, en consecuencia, su nivel de inversión será bajo, esta situación será inversamente proporcional si el pilar estratégico y el segmento de la Entidad está enfocado en potenciar un banco digital.

- De cara al aspecto tecnológico va muy de la mano de lo establecido en puntos anteriores, sin embargo, será importante a través del Framework propuesto del FFIEC, evaluar el nivel de madurez de Ciberseguridad, para tener claridad puntual sobre el nivel tecnológico que la Organización requiere en función al riesgo del negocio actual.

- Llevar a delante la generación de una metodología de evaluación de riesgos base como la de riesgos de operación, la cual permitirá dar las base y pilares iniciales que permitan a la Entidad identificar los activos críticos, así como sus riesgos y vulnerabilidades, para después de un análisis evaluarlos con la finalidad de encontrar controles mitigantes que permitan reducir y/o proteger a la Organización respecto a la probabilidad de un evento, para finalmente y no menos importante poder realizar

el seguimiento correspondiente a nivel de toda la Entidad, para esta tarea es fundamental el respaldo de los altos ejecutivos y el directorio, asegurando a través de un seguimiento mensual de parte del equipo designado a cargo de la gestión de este riesgo, que las unidades atiendan y trabajen en los controles mitigantes de las vulnerabilidades identificadas, de acuerdo a una priorización en función a un mapa de calor y criticidad asignada.

Finalmente, de manera puntual, el líder de Ciberseguridad, deberá elaborar y presentar a la alta gerencia y a su directorio, el cronograma de trabajo y priorización de tareas para la implementación de la gestión de la Ciberseguridad, tomando en cuenta el *Marco de Trabajo de Ciberseguridad del NIST* NIST, sin descuidar el Framework del FFIEC, el cual servirá de apoyo en cuanto a la especificidad de los controles que se necesitan en los diferentes procesos que forman parte del proceso tecnológico que soporta la gestión del negocio de la Entidad Financiera.

8. Conclusiones

El análisis realizado en materia de Ciberseguridad en el presente trabajo de tesis establece las siguientes conclusiones:

- Existe una evolución importante en cuanto a la regulación de la Ciberseguridad en América Latina, gracias al involucramiento de los Gobiernos para proteger a su sociedad de amenazas, sin embargo, el desarrollo no es uniforme en todos los países, ni en lo normativo, ni en lo tecnológico, por lo que existen brechas importantes de un país a otro que pueden llegar a afectar a todo el sistemas, debido a que en la actualidad debido a la globalización la conexión entre países u sistemas financieros es fluida y constante.
- En comparación con la legislación española, queda claro la importancia que los países desarrollados le han dado al tema, y marcando el paso para el resto de países, generando metodologías y buenas prácticas, Códigos de Ciberseguridad, tipificación precisa de delitos en esta materia con el afán de prevenirlos y lograr juzgarlos, además de la generación a nivel de la Unión Europea de leyes de aplicación obligatoria todos los países miembros en temas puntuales, asegurándose así los gobiernos a que todos los países deban por un lado robustecer sus sistemas cibernéticos, compartir información de manera confidencial, generar una cultura a nivel continente respecto a la Ciberseguridad y por otro a uniformar y hacer respetar los derechos de los usuarios que es finalmente aquello que las entidades (financieras o no) deben proteger, debido a que hoy por hoy es el objetivo de los ciberatacantes.
- La Organización de los Estados Americanos (OEA), la Comunidad Andina de Naciones (CAN), la Federación Latinoamericana de Bancos (FELABAN) y demás entes que conforman la comunidad internacional, deben tomar el ejemplo de la Unión Europea y comprender que en el mundo digital todos los Estados y Organizaciones están conectados y es necesario trabajar en equipo generando un marco regulatorio común, sistemas de colaboración mutua entre Estados y Organizaciones, sistemas de comunicación e información de manera confidencial, asegurándose de esta forma a que todos los actores puedan desarrollar sistemas de defensa de forma homogénea reduciendo así la posibilidad de sufrir ciberataques y combatir el cibercrimen de forma eficaz y eficiente.
- Finalmente, queda en mano de los líderes de la Ciberseguridad el concientizar y lograr evangelizar no solo a sus organizaciones, sino también a sus asociaciones de Entidades Financieras, reguladores e incluso a sus gobernantes, respecto a la urgente necesidad de atender un Marco de Ciberseguridad como un riesgo a nivel sistémico en sectores claves para la sociedad, el cual, de cara al sector bancario es vital para llevar adelante productos financieros de forma segura respetando los derechos y la confidencialidad de los datos de los usuarios.

Como es posible observar a través de todo el documento, la tesis contribuye al sistema financiero en general otorgándoles a las unidades de riesgos:

- La visualización de los puntos claves a tomar en cuenta a nivel de liderazgo, estructura y herramientas, permitiendo focalizar los esfuerzos al momento de llevar adelante un proyecto de implementación, de forma tal que no se descuide ningún punto crítico de cara al éxito de la implementación en la fase inicial y que además les permita conseguir el respaldo de la alta dirección de la Organización.

En complemento a lo anterior es necesario considerar que el desarrollo del documento de tesis, entrega una guía general para llevar adelante la implementación de un modelo de Ciberseguridad, el cual:

- Establece los puntos necesarios que debe seguirse de cara a identificar cambios en el gobierno corporativo de riesgos que permita incluir la gestión de la Ciberseguridad como un pilar más dentro del proceso de gestión integral de riesgos.
- Establece además de la justificación un esquema de comunicación que es necesario de cara a incorporar un programa de Cultura continua de Ciberseguridad, basado en que el ser humano es el eslabón más débil a ser vulnerado, con la finalidad de que pueda ser utilizada en las siguientes situaciones:
  - Medio de difusión de capacitaciones y acciones preventivas que todo colaborador debe aplicar para protegerse a sí mismo y a la Organización de un ciberataque.
  - Forma de notificación, alerta o reporte de eventos de Ciberseguridad
- Entrega y propone una estrategia de análisis de riesgo cibernético a partir de la metodología de riesgos de operación, el cual puede verse reflejado en el Marco de trabajo NIST sumado a la metodología de riesgos propuestas, en función a la experiencia real llevada adelante por una Entidad Financiera Boliviana.

Junto con ello el presente trabajo de tesis, entrega recomendaciones específicas de cara al líder de la gestión de implementación de la Ciberseguridad, que le permitan estructurar el programa de gestión de Ciberseguridad de forma efectiva.

Finalmente establece recomendaciones para la junta de accionistas y alta gerencia quienes juegan un rol de apoyo y toma de decisión principal a la hora de generar espacios de poder, recursos y herramientas que permitan llevar delante de manera efectiva el desafío de la Ciberseguridad en Entidades Financieras.

Bibliografía

1. *Accenture. (2020). Accenture. Obtenido de Accenture.com: https://www.accenture.com/cl-es/insight-banking-distribution-marketing-consumer-study*
2. *Accenture Security. (2019). The Cost Of Cybercrime. Traverse City, Michigan: Ponemon Institute.*
3. *ALEGSA. (noviembre de 2019). Diccionario de Informática y Tecnología. Obtenido de Alegsa.com.ar: https://www.alegsa.com.ar/Dic/conexion.php*
4. *Asociación Bancaria y de Entidades Financieras de Colombia. (2018). La gestión de la ciberseguridad: Un asunto de supervivencia para las organizaciones. Edición 1133 Semana Económica, 7.*
5. *Asociación Bancaria y de Entidades Financieras de Colombia. (2019). Riesgo cibernético y el futuro de la estabilidad financiera. Edición 1178 Semana Económica, 3.*
6. *Asociación de Auditoría y Control sobre los Sistemas de Información, ISACA. (2019). Normas ISO 27032.*
7. *Asociación de Bancos de Bolivia . (2019). Estudio Comité Especial de Seguridad ASOBAN. La Paz, Bolivia.*
8. *Autioridad de Supervisión del Sistema Financiero ASFI. (2018). Reglamento para el Envío de Información. La Paz: Autioridad de Supervisión del Sistema Financiero ASFI.*
9. *Autoridad de Supervisión del Sistema Financiero ASFI. (2013). Circular 193: Reglamento para la gestión de seguridad de la información . La Paz: Autoridad de Supervisión del Sistema Financiero ASFI.*
10. *B - Secure . (s.f.). B - Secure .*
11. *Barrios Achavar, V. (2018). Política Nacional de Ciberseguridad: 2017-2022. Santiago de Chile: Biblioteca del Congreso Nacional de Chile.*
12. *Club Seguridad. (Julio de 2018). Caso Cambridge Analytica y sus posibles implicaciones políticas, económicas y Sociales en Guatemala. Guatemala: Formación y Networking Inteligente.*
13. *Comisión Europea, Unión Europea. (2007). PSD: Payment Services Directive. PSD: Payment Services Directive.*

14. *Comisión Europea, Unión Europea. (2013). PSD 2: Payment Service Directive 2. Comisión Europea, Unión Europea.*
15. *Comité de Basilea en Supervisión Bancaria, Banco Internacional de Pagos. (julio de 2004). Implementación de Basilea II: Consideraciones Prácticas. Basilea, Suiza: Asociación de Supervisores Bancarios de las Américas, ASBA.*
16. *Comité de Supervisión Bancaria de Basilea. (2003). Buenas Prácticas para la Gestión y Supervisión del Riesgo Operativo . Basilea: Banco de Pagos Internacionales.*
17. *Comité Interministerial sobre Ciberseguridad Política Nacional de Ciberseguridad. (2018). Política Nacional de Ciberseguridad. Santiago de Chile: Gobierno de Chile.*
18. *Congreso de Colombia. (1999). Ley 527: Comercio Electrónico. Bogotá D.C.: Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia.*
19. *Congreso de Colombia. (2012). Ley 1581 Protección de Datos Personales. Bogotá D.C.: Ministerio de Tecnologíasde la Información y las Comunicaciones, Colombia.*
20. *Congreso Nacional de Chile. (1999). Ley 19.628 sobre Protección de la vida privada, regula la protección de datos. Santiago de Chile : Gobierno de Chile.*
21. *Consejo de Seguridad Nacional, Gobierno de España. (noviembre de 2019). Política Nacional de Ciberseguridad. Madrid, España: Gobierno de España.*
22. *Consejo Nacional de Política Económica y Social de Colombia. (2011). Documento Conpes 3701. Bogotá D.C.: Departamento Nacional de Planeación.*
23. *Consejo Nacional de Política Económica y Social de Colombia. (2016). Documento Conpes 3854. Bogotá D.C. Bogotá D.C.: Departamento Nacional de Planeación.*
24. *Departamento de Seguridad Nacional, Gobierno de España. (octubre de 2019). Sitio oficial del Departamento de Seguridad Nacional Ciberseguridad. Obtenido de https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad*
25. *Diccionario de informática y tecnología. (s.f.). Diccionario de informática y tecnología. Diccionario de informática y tecnología.*

26. *Entidad Financiera Boliviana. (2019). Metodología de Adecuación de Gestión de Riesgos de Ciberseguridad. La Paz.*
27. *Equipos de Ciberseguridad y Gestión de Incidentes españoles. (Enero de 2020). Foro CSIRT.es. Obtenido de https://www.csirt.es/index.php/es/sobre-csirt-es*
28. *Evans, D., & IBSG, C. (Abril de 2011). Internet de las cosas. San Jose, CA: CISCO Systems, Inc.*
29. *Federal Financial Institutions Examination Council's (FFIEC). (2015). Herramienta de Evaluación de la seguridad cibernética FFIEC. Federal Financial Institutions Examination Council's (FFIEC).*
30. *Fundación de la Innovación Bankinter. (2011). El internet de las Cosas, En un mundo conectado de objetos inteligentes. Obtenido de Organización de Estados Iberoamericanos: https://www.oei.es/historico/cienciayuniversidad/?article2256&debut_convocatorias=100*
31. *Gobierno de Chile. (20 de Noviembre de 2019). Ciberseguridad. Obtenido de Política Nacional de Ciberseguridad: https://www.ciberseguridad.gob.cl/*
32. *Gobierno de España. (2020). Código de Derecho de la Ciberseguridad. Madrid: Boletín del Estado.*
33. *Graham, L. (2015). Internal control audit and compliance: documentation and testing under the new COSO framework. John Wiley & Sons.*
34. *Grupo de Respuesta a Emergencias Cibernéticas de Colombia. (2019). COLCERT Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Obtenido de http://www.colcert.gov.co/*
35. *IMF Business School. (s.f.). Centros de Operaciones de Seguridad.*
36. *INFOTECS, E. d. (s.f.). Empresa de seguridad INFOTECS.*
37. *International Organization for Standardization ISO 31000 . (2009). Gestión de Riesgos - Principios y directrices. ISO.*
38. *International Organization for Standardization ISO/IEC 27000. (2014). Tecnología de la Información - Técnica de seguridad - Sistema de gestión de seguridad de la información - Información general y vocabulario. ISO/IEC.*

39. *International Organization for Standardization ISO/IEC 27001 . (2013). Sistema de Gestión de Seguridad de la Información - Requisitos. ISO/IEC.*
40. *International Organization for Standardization ISO/IEC 27005 . (2001). Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información. ISO/IEC.*
41. *International Organization for Standardization ISO/IEC 27032. (2012). Tecnología de la información - Técnicas de seguridad - Directrices para ciberseguridad. ISO/IEC.*
42. *Kaspersky Lab. (Julio de 2019). Kaspersky Lab. Obtenido de https://latam.kaspersky.com/enterprise-security/cybersecurity-services*
43. *Labs, McAfee. (Julio de 2018). McAfee Labs. Obtenido de https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs.html*
44. *Mell, P., Scarfone, K., & Romanosky, S. (2007). A complete guide to the common vulnerability scoring system version 2.0. (Vol. 1). FIRST-forum of incident response and security teams.*
45. *Moes, T. (s.f.). Software Lab.*
46. *National Institute of Standards and Techonology U.S. Department of Commerce. (1 de Agosto de 2019). Cybersecurity Framework. Obtenido de National Institute of Standards and Techonology: https://www.nist.gov/cyberframework/framework*
47. *Organización de los Estados Americanos. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. Washington: Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo.*
48. *Parlamento Europeo. (6 de julio de 2016). DIRECTIVA (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Diario Oficial de la Unión Europea.*
49. *Parlamento Europeo. (27 de abril de 2016). REGLAMENTO (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea.*

50. *Ramirez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocio. Ingeniería, 16(2), 55-56.*
51. *Real Academia Española. (Agosto de 2019). rae.es. Obtenido de https://www.rae.es/obras-academicas/diccionarios/diccionario-de-la-lengua-espanola*
52. *Rodríguez , I. (s.f.). Auditoría y Control Interno. AUDITOOL.*
53. *Rodriguez, B. E. (Octubre de 2018). III Congreso de Gestión de Riesgo Bancario. Gestión del Riesgo Ciber-Seguridad, Un asunto Estratégico. República Dominicana: Superintendencia de Bancos (SIB) de la Republica Dominicana.*
54. *Superintendencia de Bancos e Instituciones Financieras de Chile. (2018). Circular 3.640 Lineamientos para la gestión de la Ciberseguridad y reporte de incidentes operacionales. Santiago de Chile: Superintendencia de Bancos e Instituciones Financieras de Chile.*
55. *Superintendencia Financiera de Colombia. (2018). CIRCULAR EXTERNA 007 Imparte requerimientos mínimos de gestión de ciberseguridad. Superintendencia Financiera de Colombia.*
56. *Wiener-Bronner, D. (22 de marzo de 18). CNN en Español. Obtenido de https://cnnespanol.cnn.com/2018/03/22/que-es-cambridge-analytica-guia-para-entender-el-polemico-caso-del-que-todo-el-mundo-habla/*