CMF: La nueva normativa de Gestión de Seguridad de la Información y Ciberseguridad

Enable S.A., noviembre de 2020

El Capítulo 20-10 sobre Gestión de Seguridad de la Información y Ciberseguridad publicado por la Comisión para el Mercado Financiero CMF y que entrará en vigor el 1º de diciembre de 2020 contiene disposiciones, basadas en buenas prácticas, que deben ser consideradas como lineamientos mínimos a cumplir por las entidades fiscalizadas por la CMF para la gestión de la seguridad de la información y ciberseguridad.

La adhesión a estos lineamientos será parte de la evaluación de gestión que realiza este Organismo a los bancos en el ámbito de los riesgos operacionales, atendiendo al volumen y complejidad de sus operaciones.

ROL DEL DIRECTORIO

Fundamental es el rol del Directorio, en lo relativo a la aprobación de la estrategia institucional en esta materia y la autorización de los recursos presupuestarios suficientes para mitigar los riesgos asociados. Es responsabilidad de esta instancia asegurar que la entidad mantenga un sistema de gestión de la seguridad de la información y ciberseguridad, que contemple la administración específica de estos riesgos en consideración a las mejores prácticas internacionales existentes, el que debe ser concordante con el volumen y complejidad de las operaciones de la entidad.

En ese sentido, serán considerados como elementos necesarios que la entidad haya definido y aprobado:

- Contar con estructura organizacional con personal especializado y dedicado, e instancias colegiadas de alto nivel jerárquico, con atribuciones y competencias necesarias para gestionar la seguridad de la información y ciberseguridad.
- Contar con una función de riesgo, independiente de las áreas generadoras de riesgos, además de contar con un oficial de seguridad de la información y ciberseguridad a cargo de estas materias.
- Contar con una estructura de alto nivel para la administración de crisis. (Plan de actuación, canales de comunicación adecuados para informar de manera interna o externa.)
- Contar con políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad; el nivel de tolerancia al riesgo; una clara definición de los activos de información a resguardar; criterios para clasificar la información y la existencia de un inventario de activos de información permanentemente actualizado, consistente con el mapa de procesos de la entidad. Estas políticas deben ser ampliamente difundidas al interior de la organización, revisadas y aprobadas al menos anualmente por esta instancia.
- Niveles de disponibilidad mínimos aprobados por el Directorio para asegurar los servicios otorgados a través de plataformas tecnológicas.
- Promover una cultura de riesgos en materia de seguridad de la información y ciberseguridad, con políticas de conducta interna aprobadas por el Directorio.
- La entidad, como parte de la gestión de sus servicios críticos externalizados, ha implantado un proceso de verificación periódica de la aplicación y cumplimiento de sus políticas de seguridad de la información y ciberseguridad, de manera de garantizar la adecuada protección de los activos de información que son utilizados o administrados por proveedores externos. Asimismo, monitorea permanentemente la infraestructura conectada con proveedores externos, y analiza e implementa medidas para detectar y mitigar potenciales amenazas a la ciberseguridad de la entidad.
- Evaluar oportunamente los riesgos asociados a la seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades y/o definir nuevos procesos.
- Gestión de sus alertas o amenazas e incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.

- Asegurar el cumplimiento de las leyes y normativas vigentes, entre las que se encuentran, por ejemplo, la protección de los datos de carácter personal y los derechos de propiedad intelectual. Este aspecto deberá también ser exigido a sus proveedores que utilicen sus plataformas.
- Auditorías al proceso de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las entidades deberán contar con un proceso de gestión de los riesgos implementado. Considerando al menos los siguientes aspectos:

- Identificación de sus activos
- Identificación de las amenazas y vulnerabilidades
- Evaluación de los controles existentes
- Identificación de las consecuencias en pérdidas de confidencialidad, integridad y disponibilidad.
- Realizar un proceso de análisis de riesgos (probabilidad, ocurrencia y consecuencias, impactos, nivel de riesgos)
- Proceso de valoración del riesgo
- Plan de tratamiento del riesgo
- Proceso formal para asegurar que los riesgos resultantes sean concordantes con la tolerancia a los riesgos definida.
- Proceso formal de comunicación de los riesgos a la organización.
- Revisión anual de su proceso de gestión de riesgos de seguridad de la información y ciberseguridad, para ajustes en las metodologías y/o herramientas utilizadas.

GESTIÓN DE LA CIBERSEGURIDAD

Las entidades deben actuar con diligencia en la determinación de los activos críticos de ciberseguridad, y establecer funciones de protección de estos activos como:

- la detección de las amenazas y vulnerabilidades
- la respuesta ante incidentes y
- la recuperación de la operación normal de la entidad.

PROTECCIÓN DE LOS ACTIVOS CRÍTICOS DE CIBERSEGURIDAD Y DETECCIÓN DE AMENAZAS Y VULNERABILIDADES

Los procesos mínimos que deben estar instalados en la entidad para la protección de los activos críticos de ciberseguridad y la detección de amenazas y vulnerabilidades:

- Inventario de activos de ciberseguridad críticos clasificados desde una perspectiva de confidencialidad, integridad y disponibilidad
- Proceso de gestión del cambio
- Proceso de gestión de capacidades
- Proceso de gestión de la obsolescencia tecnológica
- Proceso de gestión de configuraciones
- Programa de gestión de parches
- Redes informáticas protegidas de ataques provenientes de Internet o de otras redes externas
- Segmentación de las redes informáticas de manera de implementar controles diferenciados

- La segmentación de redes alcanza los diferentes ambientes dispuestos por la entidad, (ej. desarrollo, pruebas y producción).
- Los controles establecidos deben permitir:
  - o Proteger, detectar y contener ataques a la infraestructura TI realizados a través del uso de códigos maliciosos.
  - o Mitigar los riesgos derivados del uso de dispositivos móviles y del trabajo a distancia realizado por personal interno o externo; así como también los dispositivos IoT .
- Mitigar los riesgos derivados de la adquisición, integración o desarrollo de aplicativos y sistemas, así como su puesta en producción. La gestión de identidades y de acceso físico y lógico contempla adecuados controles.
- Herramientas adecuadas para controlar, registrar y monitorear las actividades realizadas por los usuarios en general sobre los activos críticos, así como de aquellos con privilegios especiales.
- Mecanismos de control de accesos, en los canales electrónicos dispuestos por la entidad, con los que interactúan los clientes y usuarios de manera de mitigar, entre otros, los riesgos de suplantación o uso indebido por parte de terceros, de los productos y servicios puestos a su disposición.
- Normas y procedimientos que establecen la información que requiere ser protegida a través de técnicas de cifrado.
- Resguardos adecuados para la conservación, transmisión y eliminación de la información.
- Herramientas de monitoreo continuo que le permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y vulnerabilidades
- Proceso de administración de respaldos que le permite asegurar la integridad y la disponibilidad de su información y de sus medios de procesamiento, ante la ocurrencia de un incidente o desastre, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio. Los respaldos de la información se debiesen generar, mantener y utilizar en ambientes libres de códigos maliciosos, y adecuadamente controlados.
- Realización anual de pruebas de restauración de sus respaldos.
- Evaluación de mecanismos de cobertura destinados a cubrir los costos asociados a eventuales ataques cibernéticos.
- Contar con un Security Operation Center (SOC), propio o a través de un servicio externo, que opere las 24 horas del día, con instalaciones, herramientas tecnológicas, procesos y personal dedicado y entrenado, a fin de prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad.
- Identificar y evaluar regularmente los vectores de ataque de su infraestructura tecnológica, como por ejemplo la manipulación o interceptación de las comunicaciones, phishing, malware, elevación de privilegios, inyección de código, denegación de servicios, ingeniería social, etc.; distinguiendo claramente entre aquellos que pueden afectar la infraestructura física, la infraestructura lógica o el equipamiento de usuarios finales (end point).
- La entidad realiza en forma regular, con el suficiente alcance y profundidad, pruebas de seguridad a su infraestructura tecnológica para detectar las amenazas y vulnerabilidades que pudieran existir, tales como pentesting y/o ethical hacking

RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES

- Probar, al menos anualmente, los planes necesarios para enfrentar adecuadamente los escenarios que puedan afectar la ciberseguridad.
- Contar con un plan definido de actuación, que dependiendo de la severidad de un incidente de ciberseguridad permite escalar
- Contar con plan de comunicaciones, liderado por la alta administración, que opera ante incidentes de ciberseguridad de alto impacto.
- Contar con un proceso independiente de análisis forense para los ciberincidentes relevantes,

- Contar con una base de incidentes de ciberseguridad de los activos de información presentes en el ciberespacio suficientemente detallada que le permita perfeccionar la capacidad de respuesta de estos
- Considerar la base de incidentes como un insumo para la realización de pruebas
- Contar con una base de conocimientos y lecciones aprendidas
- Realizar autoevaluaciones en esta materia, al menos anualmente

GESTIÓN DE LA INFRAESTRUCTURA CRÍTICA DE CIBERSEGURIDAD DEL PAÍS

Las entidades deben contar con políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura critica de la industria financiera y del sistema de pagos, así como para el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad de la entidad, con otros integrantes que son parte de esta infraestructura crítica, cuidando siempre de cumplir con las exigencias legales de secreto y reserva legal, y de confidencialidad de la información personal de los clientes.

A fin de detectar y gestionar las amenazas y vulnerabilidades que pudieran afectar el funcionamiento del sistema financiero, las distintas entidades deben procurar la realización de pruebas conjuntas de