AUDITORIA Y ASEGURAMIENTO
ASESORAMIENTO TRIBUTARIO
CONSULTORIA GERENCIAL Y DE T.I.
BPO DE CONTABILIDAD Y NÓMINA

sfaicolombia sfaicolombia

SFAI

Boletín No. 321 - Septiembre 2023

LA GOBERNANZA DE LA CIBERSEGURIDAD

Por: *Rodrigo García Ocampo (CPA, MBA, MGE, MGR)*
Socio - Director
Email: *rgarcia@sfai.co*

La ciberseguridad, que es el conjunto de medidas, procesos y tecnologías que tienen como objetivo proteger la información, los sistemas y las redes de comunicaciones de posibles ataques, intrusiones o amenazas que puedan comprometer su confidencialidad, integridad o disponibilidad, se ha convertido en un tema crucial para las empresas de todos los sectores y tamaños, ya que los ataques informáticos pueden causar graves daños económicos y reputacionales. Según un informe de la ONU, el 40% de las pymes sufrieron algún tipo de incidente de seguridad en 2020, lo que evidencia la vulnerabilidad de este segmento empresarial. Por ello, es fundamental que las PyMes adopten medidas preventivas y correctivas para proteger sus datos, sistemas y redes de las amenazas cibernéticas dentro de sus estructura de gobernanza que no solo les permita proteger sus datos y procesos informáticos, sino, también, dar alcance a las con la normativa vigente en materia de protección de datos personales.

Las ciberamenanzas y las salvaguardas

Una ciberamenaza es cualquier acción, intencionada o no, que pueda causar un daño o un impacto negativo en la seguridad de la información, los sistemas o las redes de comunicaciones. Una ciberamenaza se puede tipificar según su origen (interno o externo), su naturaleza (accidental o deliberada), su intencionalidad (maliciosa o no maliciosa), su alcance (local o global), su persistencia (temporal o permanente) y su impacto (bajo, medio o alto), por lo que se hace necesario dentro del modelo de gobernanza de la empresa de adoptar salvaguarda en TIC, conforme los siguientes tópicos:

a. Salvaguardas organizativas, normativas y procedimentales:

- Políticas de seguridad de la información: son el conjunto de principios, directrices y normas que establecen el marco de referencia para la gestión de la seguridad de la información en una organización. Las políticas de seguridad de la información deben ser aprobadas por la dirección, difundidas entre el personal y revisadas periódicamente.
- Normativa interna: son el conjunto de reglas, procedimientos e instrucciones que regulan el uso, acceso y tratamiento de la información, los sistemas y las redes de comunicaciones la empresa. La normativa interna debe ser coherente con las políticas de seguridad de la información y debe ser de estricto cumplimiento por todos los usuarios.
- Procedimientos de seguridad: son el conjunto de pasos, actividades y controles que se deben seguir para garantizar la seguridad de la información, los sistemas y las redes de comunicaciones en una organización. Los procedimientos de seguridad deben estar documentados, actualizados y auditados.

Continuación de la Página No. 1

b. Salvaguardas tecnológicas:

- Fase de intrusión: es el momento en el que un atacante consigue acceder a un sistema o una red de comunicaciones sin autorización. Las salvaguardas tecnológicas que se pueden aplicar en esta fase son: el uso de cortafuegos, antivirus, antimalware, sistemas de detección y prevención de intrusiones, cifrado, autenticación y control de acceso.

- Fase de movimiento lateral: es el momento en el que un atacante se desplaza por un sistema o una red de comunicaciones buscando información sensible o vulnerabilidades que le permitan escalar privilegios o comprometer otros recursos. Las salvaguardas tecnológicas que se pueden aplicar en esta fase son: el uso de segmentación de redes, aislamiento de sistemas críticos, monitorización y registro de actividades, análisis forense y respuesta a incidentes.

- Fase de explotación o colonización: es el momento en el que un atacante consigue extraer, modificar o eliminar información sensible o ejecutar acciones maliciosas en un sistema o una red de comunicaciones. Las salvaguardas tecnológicas que se pueden aplicar en esta fase son: el uso de copias de seguridad, restauración de sistemas, borrado seguro, actualización y parcheo.

c. Vigilancia y auditorías continuas:

Estas actividades ejecutadas de manera apropiada permiten verificar el cumplimiento y la eficacia de las salvaguardas organizativas, normativas y tecnológicas implementadas en una organización. La vigilancia consiste en el seguimiento constante del estado y el funcionamiento de la seguridad de la información, los sistemas y las redes de comunicaciones, mientras que, las auditorías consisten en la evaluación periódica e independiente del nivel y la calidad de la seguridad de la información, los sistemas y las redes de comunicaciones.

d. Salvaguardas conductuales:

Son las acciones y actitudes que deben adoptar los usuarios para contribuir a la seguridad de la información, los sistemas y las redes de comunicaciones en empresa, las implican:

- Mejoras del nivel de la cultura en ciberseguridad: se refiere al conjunto de conocimientos, valores y hábitos que tienen los usuarios sobre la importancia y la responsabilidad de la seguridad de la información, los sistemas y las redes de comunicaciones, la que es posible obtener a través de procesos de sensibilización, formación y concientización.

- Cumplimiento de las normas y los procedimientos de seguridad: se refiere al respeto y la obediencia de los usuarios a las reglas, instrucciones y controles establecidos para garantizar la seguridad de la información, los sistemas y las redes de comunicaciones a través de procesos de comunicación asertiva, la motivación y los procesos de sanciones disciplinarias.

- Prevención y detección de incidentes: Es la capacidad y disposición de los usuarios para evitar o identificar situaciones que puedan poner en riesgo la seguridad de la información, los sistemas y las redes de comunicaciones. La prevención y la detección se facilita mediante el uso de buenas prácticas, el reporte de anomalías y la colaboración.

Marco de gobernanza de la ciberseguridad

Se debe entender como el conjunto de estructuras, procesos y mecanismos que permiten definir, implementar, supervisar y mejorar la gestión de la seguridad de la información, los sistemas y las redes de comunicaciones en una organización, el que debe estar alineado con los objetivos estratégicos, el contexto operativo y el nivel de riesgo empresarial.

Estructura organizativa del marco de gobernanza:

Está constituido normalmente por el: (1) Comité de seguridad TIC, encargado de definir, aprobar y supervisar la estrategia, las políticas y los planes de seguridad TIC de la organización. Entre sus funciones se encuentran: establecer los objetivos y las prioridades de seguridad TIC, asignar los recursos necesarios, evaluar los riesgos y las amenazas, supervisar el cumplimiento normativo, coordinar las acciones de prevención, detección y respuesta a incidentes, y promover la cultura de seguridad TIC entre los empleados y los proveedores; (2) Oficina de gobernanza y cumplimiento normativo de la seguridad TIC, quien es la responsable de implementar, gestionar y controlar el marco de gobernanza de la seguridad TIC. Entre sus funciones se encuentran: elaborar y mantener las políticas y los procedimientos de seguridad TIC, realizar el seguimiento y la medición de los indicadores de seguridad TIC, asesorar y apoyar a las unidades organizativas en materia de seguridad TIC, gestionar los proyectos y las iniciativas de mejora continua, y coordinarse con el órgano de auditoría técnica. La oficina de gobernanza y cumplimiento normativo de la seguridad TIC, también ofrece servicios de prevención proactiva los que consisten en: realizar análisis de riesgos y evaluaciones de impacto, identificar y aplicar medidas de mitigación, realizar audi-

Continuación de la Página No. 2

torías internas y externas, gestionar las vulnerabilidades y los parches, realizar pruebas de penetración y simulaciones de ataques, y formar y concienciar al personal sobre las buenas prácticas de seguridad TIC; (3) Órgano de auditoría técnica, es la entidad independiente que verifica el grado de cumplimiento del marco de gobernanza de la seguridad TIC por parte de la organización. Entre sus funciones se encuentran: realizar auditorías técnicas periódicas o bajo demanda, emitir informes con las conclusiones y las recomendaciones, comunicar los hallazgos al comité de seguridad TIC y a la oficina de gobernanza y cumplimiento normativo, y verificar la implantación efectiva de las acciones correctivas.

Modelo extendido de gobernanza:

El modelo extendido de gobernanza es una ampliación del modelo básico que incorpora otros actores relevantes para la seguridad TIC, como lo son: (a) el responsable o coordinador de seguridad TIC, quien es la persona que lidera la oficina de gobernanza y cumplimiento normativo; (b) el equipo o grupo operativo de seguridad TIC, que es el conjunto de profesionales que realizan las tareas operativas relacionadas con la seguridad TIC; (c) el responsable o coordinador del Centro Operativo o Sala Técnica (COCS). El COCS tiene una estructura funcional de cuatro áreas: (i) el área de monitorización, que se ocupa de supervisar el estado y el rendimiento de los sistemas e infraestructuras críticos; (ii) el área de gestión, que se ocupa de administrar y configurar los sistemas e infraestructuras críticos; (iii) el área de detección, que se ocupa de identificar y analizar las alertas y los eventos de seguridad TIC; y (iv) el área de respuesta, que se ocupa de contener y erradicar las amenazas y los incidentes de seguridad TIC. El equipo o grupo operativo del COCS, son los responsable o coordinador del Comité de Crisis.

Comité de crisis

El comité de crisis es el órgano encargado de gestionar las situaciones críticas que afecten a la seguridad TIC de la empresa. El comité se activa cuando se produce un incidente de seguridad TIC de alto impacto o cuando se prevé que pueda producirse. La activación del comité puede ser solicitada por el responsable o coordinador del COCS, por el responsable o coordinador de seguridad TIC, por el órgano de auditoría técnica, o por cualquier miembro del comité. Entre las funciones del Comité, se encuentran: evaluar la gravedad y el alcance del incidente o la situación crítica, establecer los objetivos y las estrategias para su resolución, asignar los recursos y las responsabilidades, coordinar las acciones y las comunicaciones internas y externas, supervisar el desarrollo y el resultado de las acciones, y cerrar la crisis y desactivar el comité cuando se haya restablecido la normalidad.

El comité de crisis está compuesto por su responsable o coordinador del comité de crisis, quien lo preside y lo dirige; el responsable o coordinador del COCS, que informa sobre el estado y la evolución del incidente o la situación crítica; el responsable o coordinador de seguridad TIC, que informa sobre las medidas preventivas y correctivas adoptadas; el representante del órgano de auditoría técnica, que informa sobre el grado de cumplimiento del marco de gobernanza; el representante del equipo jurídico, que informa sobre las implicaciones legales; el representante del equipo de comunicación, que informa sobre las acciones informativas y divulgativas; y otros miembros que puedan ser convocados en función de la naturaleza y la complejidad del incidente o la situación crítica.

El comité de crisis deberá reunirse periódicamente o bajo demanda para analizar la situación, tomar decisiones, asignar tareas y evaluar resultados. Si es bajo demanda, el Comité se desactiva al cierre del incidente de crisis que ocurre cuando se haya restablecido la normalidad en los sistemas e infraestructuras afectados por el incidente o la situación crítica, se han aplicado las medidas correctivas pertinentes, se han evaluado los daños y las lecciones aprendidas, y se ha elaborado un informe final con las conclusiones y las recomendaciones.

SFAI con el apoyo de nuestros partner en más de 300 oficinas en más de 115 países, somos conscientes del valor de la datos para que suministren información relevante en la gestión empresarial y, con ello, de su capacidad de generar valor, por lo que, nos dedicamos a desarrollar procesos consultivos, sin importar tipo y tamaño de empresa, para que nuestros clientes logren sus objetivos de negocio con el apoyo de SFAI Tech que con el uso de tecnologías emergentes como la Analítica de Datos, ML, IA y RPA generan confianza en los líderes que ahora se relacionan con información de calidad, por lo que la asegurabilidad de TIC es nuestro pilar.

CONTÁCTENOS | SFAI	+57 318 37 14 596