Technology Risk Control Assurance

Noviembre 2020

MNEMO: Somos especialistas, y contamos con profesionales expertos, en la implantación de un modelo completo de **Gobierno y Gestión de Riesgos no Financieros**

Nuestra oferta contempla entre otras las siguientes actividades y funciones:

- Diseño y conceptualización de órganos de Gobierno de Gestión del Riesgo Operacional en las entidades
- Cumplimiento Regulatorio y Legislativo TI
- Gestión del Riesgo Operacional en terceras partes
- Análisis de Riesgos TI
- Procesos de admisión de Riesgo TI
- Diseño e implantación de Controles sobre Riesgo Operacional
- Gestión y Coordinación de Auditorías Externas e Internas
- Diseño y comunicación de indicadores de Riesgo TI
- Asesoría, conceptualización e implantación de servicios de protección de datos
- Concienciación sobre Seguridad
- Servicios de Reporting asociados

MNEMO un equipo preparado

- Certificaciones en Seguridad de la Información y Gestión de Riesgos (CRISC, CISA, CISM, CDPSE, ISO 27K Lead Auditor…)
- Gobierno TI (ISO 20000, ITIL, CobIT, CGEIT…).
- Experiencia en uso de las principales herramientas en gestión de riesgos, tales como Pilar, RSA Archer, Globalsuite y similares.
- Experiencia en la implantación de marcos de referencia como NIST Cybersecurity Framework (CSF), CobIT etc.
- Experiencia en la aplicabilidad de Normas, Regulaciones y Buenas Prácticas (RGPD. LOPDGDD, PSD2, PCI DSS Directrices EBA,...)

MNEMO ha colaborado con la entidad en los procesos de Gestión del Riesgo Tecnológico desde su lanzamiento en 2016 hasta la actualidad.

- **Riesgo no Financiero:**
  - **Riesgo Operacional**: Riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los generados en su ámbito de actuación. Incluye el Riesgo Tecnológico.
  - **Riesgo reputacional**

La necesidad de un modelo de gestión del Riego Tecnológico

- ✓ Mejores prácticas
- ✓ Un sector fuertemente regulado en el que se exige el mantenimiento de un Modelo de Gestión del Riesgo Tecnológico

El Modelo de Tres Capas

El modelo de las Tres Capas o Líneas de Defensa distingue tres grupos de funciones en la gestión efectiva de los riesgos:

TERCERA LINEA DE DEFENSA: AUDITORÍA INTERNA

SEGUNDA LINEA DE DEFENSA: FUNCIONES DE GESTIÓN DE RIESGOS Y CUMPLIMIENTO: Se ocupan de diseñar y mantener el modelo de Riesgo Operacional de la Entidad ,y de verificar su correcta aplicación en el ámbito de las distintas Áreas.

PRIMERA LINEA DE DEFENSA: LA GESTION OPERATIVA: Gestión en las Áreas de Negocio y de soporte de los Riesgos Operacionales en sus productos, actividades, procesos y sistemas, identificando y evaluando riesgos, estableciendo el riesgo objetivo, llevando a cabo los controles y ejecutando los planes de mitigación de aquellos riesgos con nivel de riesgo residual superior al asumible

Procesos de Aseguramiento del Control del Riesgo Tecnológico

Factores de Éxito

- ✓ Flexibilidad
- ✓ Implicación
- ✓ Confianza
  - ✓ Equipo
  - ✓ Formación
  - ✓ Retención
  - ✓ ….

MNEMO

Las Funciones y Tareas

MNEMO ha ayudado en la implantación de la función de admisión de riesgos a través de las siguientes actividades:

- Censo de Iniciativas, proyectos y procesos. Recopilación de información
- Participación en la confección del Marco de Control en los aspectos relacionados con Tecnología (Fraude, Ciberseguridad, Continuidad, Gestión de Cambios, Gestión de Proveedores, Privacidad y Protecciónd el Dato entre otros)
- Funciones de Soporte y Reporting al Comité de Admisión de Riesgo Operacional

Análisis de Riesgos:

MNEMO ha colaborado en el desarrollo e implantación una metodología propia basada estándares internacionales y mejores prácticas como ISO 27K series , ISO 31000, NIST 800-30 NIST CSF COBIT entre otras sin olvidar la normativa vigente aplicable (RGPD. LOPD-GDD, LPIC,...)

Con carácter general, se considera como riesgo cualquier *amenaza* de que un evento, acción u omisión pueda impedir a una organización sus objetivos y ejecutar sus estrategias con éxito.

La metodología implantada rompe con los esquemas tradicionales:

- ✓ ***Las áreas son las mejores conocedoras de los riesgos que les afectan y de las debilidades que tienen.***

MNEMO colabora con el cliente en el proceso de Gestión y Coordinación de Auditorías.

- Censo de Auditorías y Acciones.
- En el caso de Auditores Externos, Gestión de la demanda. Interlocución con los equipos técnicos en la solicitud de evidencias y revisión de las mismas. Respuesta al equipo auditor.
- Colaboración con las áreas afectadas en la definición de planes de acción para mitigar las debilidades levantadas por Auditoría Interna.
- Seguimiento con las áreas resolutoras de los planes de acción.
- Solicitud de implantación de planes de acción.
- Identificación de problemas y gestión de replanificaciones.

Modelo de Control del Riesgo Tecnológico

Para tener una correcta **gestión del riesgo en la Organización**, **MNEMO** colabora llevando a cabo un proceso continuo de revisión de los procesos de TI, para identificar los riesgos existentes y garantizar su correcta mitigación.

El resultado de la revisión de los procesos da como resultado **el modelo de control para el mismo**, identificando los riesgos, los controles existentes que mitigan los mismos y en caso de existir alguna debilidad se establecerá un plan de acción con los interlocutores.

Como labores de soporte de la actividad se realizan las siguientes actividades adicionales:

- Adaptación del modelo de control a normativas y regulaciones
- Evaluación y testing del modelo de control
- Seguimiento de debilidades
- Escalado a los comités de Gobierno
- Reporting

La Función de Verificación de implantación de medidas de seguridad

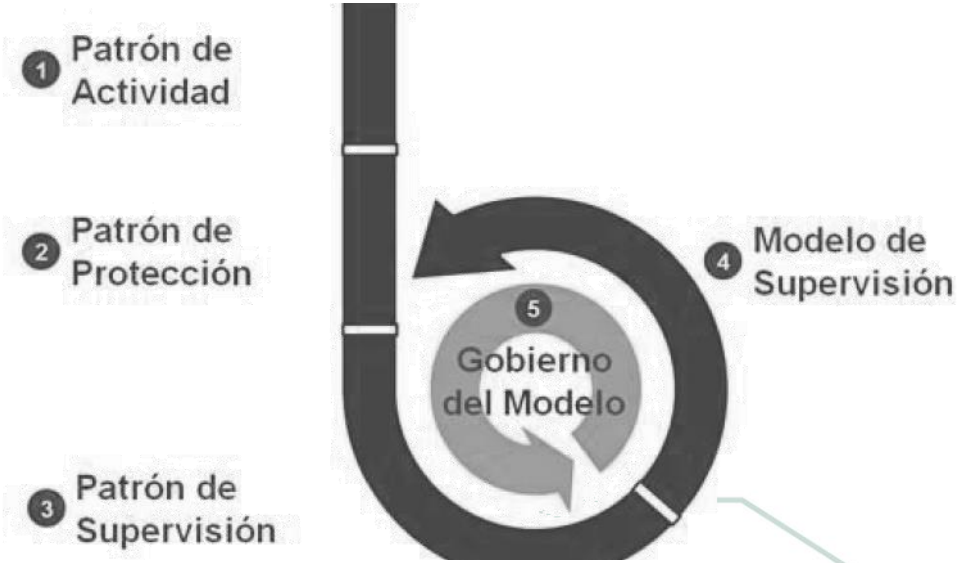
Los equipos Arquitectura de Seguridad en Proyectos emiten para las iniciativas con un nivel de riesgo Alto o Muy alto un informe que recoge de los requisitos de seguridad dictaminados por las áreas especialistas y validadas por los comités creados a tal efecto

- ✓ La función verifica el grado de cumplimiento de dichas medidas de seguridad a través de un análisis de estado de implantación de las misma en el que se valora el porcentaje de mitigación del riesgo.

- ✓ El área emite un informe con el posicionamiento del Departamento de Seguridad de la Información respecto a la conveniencia de implantación del proyecto en la situación de seguridad analizada

Gestión del Riesgo en Terceros

“Determinar los patrones de protección necesarios para supervisar la actividad desarrollada por los proveedores de servicios externos a la entidad”



Con este proceso se optimiza el control de la información que se encuentre en manos de terceros mediante revisiones de estos comprobando que estas cumplen con los requisitos de seguridad establecidos contractualmente y siguen las recomendaciones establecidas por las mejores prácticas.

Se divide en dos subprocesos:

- Precontratacion.
- Revisión de Proveedores.

MNEMO colabora en la Realización de actividades **de Concienciación y Formación** sobre la seguridad de la información:

- Apoyo en charlas sobre medidas de seguridad de la información
- Realización de contenidos referentes a la seguridad de la información a publicar en redes sociales:
    - o Consejos de seguridad
    - o Advertencia de posibles fraudes.
    - o Información sobre seguridad TI.
- Apoyo y/o realización de postales, publicidad, presentaciones sobre difusión y formación sobre seguridad TI.

MNEMO, dentro de la función de **Protección del Dato y Cumplimiento**, ha desarrollado las tareas siguientes:

- Análisis de accesos a ficheros con información sensible (GDPR - LOPDGDD) y gestión de incidentes relacionados con dichos accesos.
- Emisión de medidas seguridad sobre datos para iniciativas.
- Registro, seguimiento y gestión de incidentes de Seguridad TI, así como comunicación al DPO.
- Cuadro de mando de indicadores GDPR / DLP.
- Mantenimiento de Sites.
- Mantenimiento del cuerpo normativo de Seguridad.
- Apoyo a Auditorías Regulatorias.
- Comunicación de Incidentes a reguladores.
- Análisis de peticiones de accesos a datos y salida de información.
- Análisis de reglas de securización sobre flujo de Datos.

Gracias

Ángel A. Arévalo Bermúdez
Director de Operaciones
Sector Finanzas y Seguros

+34 91 417 67 76
a.arevalo@mnemo.com
www.mnemo.com
Cardenal Marcelo Spínola 14, 5ª planta, 28016 Madrid