Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

Curso Ciberseguridad para Auditores Internos

Aplicando COBIT5 al Gobierno de la Ciberseguridad

Santiago, 18 de octubre de 2018

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia

Ciberseguridad

Carlos Silva

Certified Information Systems Auditor (CISA), Licenciado en Informática, Master en Gestión de Proyectos

Consultor Internacional

Sobre el conferencista

Carlos Silva

Certified Information Systems Auditor (CISA)

Consultor Internacional

<

- 2018 a la fecha Gerente de Infotecnología, Dirección Adjunta de Rentas Aduaneras
- 2016 -2017 Cowater-Sogema Internacional Inc. Latin America Audit ExpertOttawa, Canadá, Consultor Experto para Latinoamérica de Auditoría de Sistemas de Información y Comunicaciones, Implementación de Gobierno y Gestión de las Tecnologías de la información (TI), Análisis y Evaluación de Riesgos y elaboración de Planes de Contingencia.
- 2017, Banco Nacional de Desarrollo Agrícola, Gerente de Tecnología, • Implementación de mejoras en el Core Bancario BYTE e implementación de nuevos servicios financieros
- • Implementación de gobierno y gestión de TI empresarial, • Análisis y evaluación de riesgos y elaboración de Planes de Contingencia, • Soporte para la creación de políticas institucionales de TI, asesoramiento para la creación de comités tecnológicos de información, evaluación de procesos y controles de TI, elaboración de procesos de planificación de TI, implementación de medidas de seguridad informática, • Supervisión y monitoreo de la plataforma tecnológica del banco
- 2016-2017 Contraloría General de la República de Cuba, La Habana, Cuba, • Facilitador COBIT5, • Implementación del marco comercial para la gobernanza y la gestión de las TI empresariales
- - 2005 – 2017, TRIBUNAL SUPERIOR DE CUENTAS; Director de Tecnología, Experiencia en realización de auditorías informáticas integrales y evaluación de estructuras de gobierno de Tecnologías de la Información (TI) en varias entidades gubernamentales del Gobierno de Honduras

Aplicando COBIT 5 al Gobierno de Ciberseguridad

El marco y los componentes de COBIT 5 — aplicados a la ciberseguridad — cubren el gobierno, la gestión y la auditoría. Para asegurar el gobierno adecuado y exhaustivo se deben usar los cinco principios básicos de COBIT 5 como punto de partida.

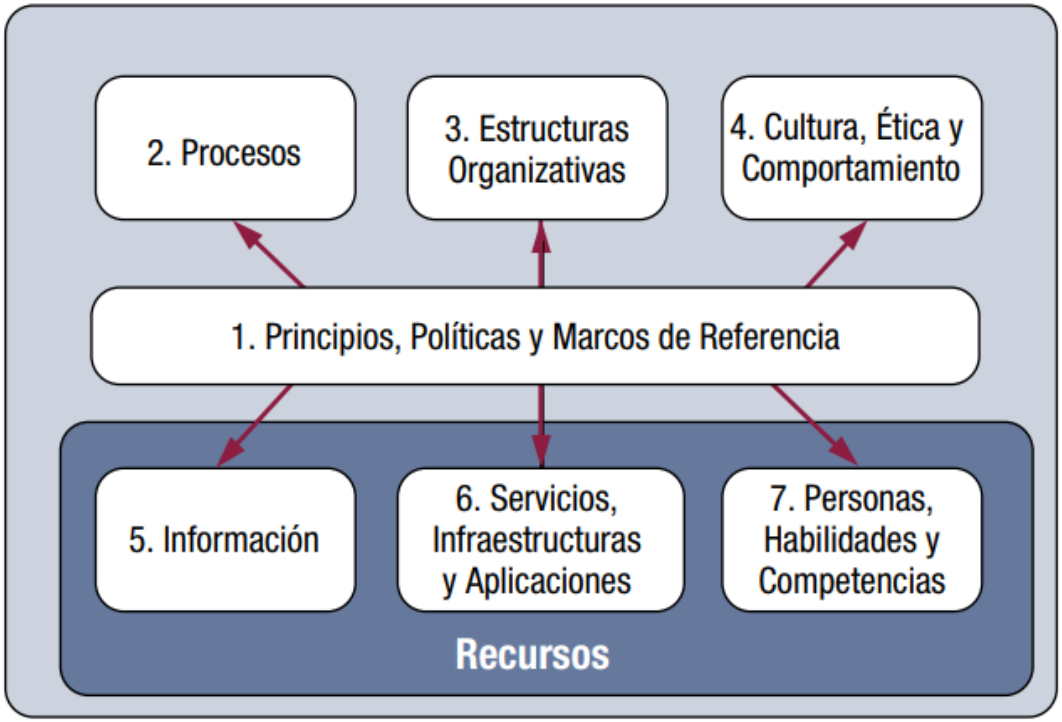
Fuente: ISACA, COBIT 5, EE.UU, 2012, figura 2

Gestión de la Ciberseguridad

Se aborda la gestión de la seguridad desde la perspectiva estratégica de las prácticas del día a día y las actividades necesarias para implementar y mantener la ciberseguridad en el contexto de la organización.

Para gestionar de forma eficiente todos los aspectos de la seguridad, es necesario estructurarla en línea con COBIT. COBIT 5 define un conjunto de catalizadores que son utilizados para construir una gestión holística de la seguridad que aborde la ciberseguridad desde un punto de vista amplio y que esté estrechamente conectada con otras prácticas GRC de la empresa.

Catalizadores de COBIT 5



Fuente: ISACA, COBIT 5, EE.UU., 2012, figura 12

Principios, Políticas y Marcos

En ciberseguridad, los principios, políticas y marcos forman una importante base para especificar medidas y actividades dentro de la empresa y en las relaciones con los socios, los clientes y otros terceros. Este catalizador además establece los requisitos de documentación para la ciberseguridad, incluyendo los ataques y las infracciones reales.

Principios de Seguridad de la Información

Principio	Objetivo (Resumen)	Ciberseguridad
Foco en el negocio.	Asegurar que la seguridad de la información se integra en los procesos de negocio principales.	• Analizar el riesgo de negocio de ataques/violaciones de seguridad para los procesos de negocio y priorizar la ciberseguridad en consecuencia. • Establecer el nivel tolerado de ataques y violaciones según una perspectiva de negocio.
Entregar calidad y valor a las partes interesadas.	Asegurar que la seguridad de la información entrega valor y está alineada con los requisitos de negocio.	• Desarrollar un análisis de las partes interesadas (internas y externas) y derivar los requisitos de ciberseguridad. • Desarrollar un análisis de requisitos (internos y externos) de negocio (y legales/regulatorios) y derivar requisitos específicos de ciberseguridad. • Definir los objetivos de alto nivel de ciberseguridad y obtener aprobación de la alta dirección.

Principios de Seguridad de la Información

Principio	Objetivo (Resumen)	Ciberseguridad
Cumplir con los requisitos legales y regulatorios relevantes.	Asegurar que se cumplen las obligaciones estatutarias, se gestionan las expectativas de las partes interesadas y se evitan las penalizaciones civiles o criminales.	• Identificar leyes, regulaciones y reglas de gobierno para la ciberseguridad y definir los requisitos. • Hacer obligatorios estos requisitos en todo el sistema de ciberseguridad y sus componentes.
Proporcionar de manera oportuna y exacta información sobre el desempeño de la seguridad de la información.	Dar soporte a los requisitos de negocio y gestionar el riesgo de la información.	• Establecer los indicadores clave de desempeño (KPIs) de ciberseguridad y elaborar informes regularmente. • Establecer los indicadores clave de riesgo (KRIs) de ciberseguridad y elaborar informes regularmente.
Evaluar las amenazas de información actuales y futuras.	Analizar y evaluar las amenazas de seguridad de información emergentes para que cuando sean informadas, puedan tomarse las medidas oportunas para mitigar el riesgo.	• Identificar las amenazas para todas las partes de la empresa (ver anterior). • Anticipar las amenazas futuras provenientes del cibercrimen y la ciberdelincuencia. • Recopilar los datos y las evidencias sobre incidentes, ataques y violaciones de seguridad. • Aplicar un escaneo horizontal y técnicas detalladas de análisis de datos para obtener un panorama razonablemente sólido sobre el futuro de la ciberseguridad. • Aprovechar la experiencia externa cuando sea apropiado.
Promocionar la mejora continua en seguridad de la información.	Reducir costes, mejorar la eficiencia y eficacia y promocionar una cultura de mejora continua en seguridad de la información.	• Establecer un proceso de mejora continua, basado en la experiencia pasada y las tendencias futuras. • Establecer un proceso de ciberseguridad tolerante a fallos/ errores. • Fomentar una cultura que promueva la mejora y un pensamiento adaptativo.

Principios de Seguridad de la Información

Principio	Objetivo (Resumen)	Ciberseguridad
Adoptar un enfoque basado en el riesgo.	Asegurar que el riesgo es tratado de una manera consistente y eficaz.	• Definir un proceso de identificación y evaluación de riesgos apropiado. • Validar las opciones de tratamiento del riesgo en ciberseguridad. • Alinear el riesgo con el modelo seleccionado de gobierno general. • Incluir incidentes anteriores y aprendizajes técnicos/ organizacionales. • Identificar y evaluar nuevos riesgos derivados del cibercrimen y la ciberguerra.
Proteger la información clasificada.	Evitar la divulgación de información clasificada (p.ej., confidencial o sensible) a personas no autorizadas.	• Establecer la clasificación de datos en materia de cibercrimen. • Establecer la clasificación de datos con respecto a la ciberguerra. • Incluir el almacenamiento y los servicios basados en la nube, así como los datos que residen o que fluyen a través dispositivos móviles o públicos. • Proporcionar información relacionada con la ciberseguridad para la gestión de identidad y de accesos.
Concentrarse en aplicaciones críticas de negocio.	Priorizar los escasos recursos de seguridad de la información protegiendo las aplicaciones de negocio en las que un incidente de seguridad de la información tendría mayor impacto en el negocio.	• Identificar las aplicaciones críticas de negocio mediante la realización de un análisis de impacto en el negocio (BIA) con una perspectiva de ciberseguridad. • Realizar un análisis de dependencia en profundidad desde la capa de aplicaciones críticas hacia abajo para identificar puntos de entrada potencialmente vulnerables. • Enfocar la ciberseguridad en el "eslabón más débil de la cadena" y alinear con el BIA general. • Asignar recursos y financiación en consonancia con las amenazas reales de cibercrimen y ciberguerra, y considerar los vectores y enfoques de ataque indirectos. • Adoptar la mentalidad del atacante - mayor estrago con mínimo esfuerzo.

Principios de Seguridad de la Información

Principio	Objetivo (Resumen)	Ciberseguridad
Desarrollar sistemas de forma segura.	Construir sistemas con calidad y rentables en los que la gente de negocio pueda confiar (p.ej., que sean consistentemente robustos, precisos y fiables).	• Establecer controles en el ciclo de vida de software para aplicaciones de desarrollo propio y personalizadas. • Definir un proceso de incorporación de ciberseguridad para aplicaciones y sistemas potencialmente críticos. • Involucrar a los proveedores para conseguir controles de ciberseguridad en origen. • Involucrar a los proveedores para gestionar las vulnerabilidades de día-cero y los puntos de entrada.
Actuar de manera profesional y ética.	Asegurar que las actividades relacionadas con la seguridad de la información se llevan a cabo de una manera confiable, responsable y eficaz.	• Aplicar el gobierno (ver el capítulo anterior) a las políticas, normas y procedimientos operativos clave (KOPs) de ciberseguridad. • Introducir rutinas de autoevaluación y de evaluación entre pares para el personal expuesto (aseguramiento de la integridad). • Realizar verificaciones de antecedentes (de forma optativa) para el personal de ciberseguridad. • Definir e implementar controles y verificaciones adecuadas para los nuevos empleados en puestos sensibles. • Definir e implementar procedimientos adecuados para la finalización de la relación laboral. • Asegurar el reconocimiento del personal de ciberseguridad mediante incentivos y reconocimientos apropiados.
Fomentar una cultura positiva de seguridad de la información.	Proporcionar una influencia positiva de seguridad de la información sobre el comportamiento de los usuarios finales, reducir la probabilidad de ocurrencia de incidentes de seguridad de la información que se producen y limitar su impacto potencial en el negocio.	• Definir una guía de comportamiento en ciberseguridad. • Fomentar la concienciación sobre ciberseguridad y cibercrimen. • Proporcionar ejemplos y casos prácticos de ataques / violaciones. • Resaltar el impacto en el negocio de los ataques / violaciones. • Enlazar con los principios rectores (ver más adelante) para la ciberseguridad.

Conjunto de Políticas de COBIT 5 para Seguridad de la información

Fuente: ISACA, *Securing Mobile Devices*, EE.UU., 2012, figura 26

Política de Ciberseguridad

El propósito de una política de ciberseguridad es expresar claramente y sin ambigüedad las metas y los objetivos así como los límites para la gestión de seguridad y las soluciones de seguridad. Como tal, la política también sirve para definir el rol y el alcance de la ciberseguridad dentro de la seguridad de la información general

Establecer la ciberseguridad de extremo a extremo es una parte esencial del catalizador Principios, Políticas y Marcos.

Componentes de la Política de Ciberseguridad

- Analizar el riesgo de negocio de ataques/ violaciones de seguridad para los procesos de negocio y priorizar la ciberseguridad en consecuencia
- Establecer el nivel tolerado de ataques violaciones según una perspectiva de negocio.
- Desarrollar un análisis de las partes interesadas (internas y externas) y derivar los requisitos de ciberseguridad.
- Desarrollar un análisis de requisitos (internos y externos) de negocio (y legales/ regulatorios) y derivar requisitos específicos de ciberseguridad.

Componentes de la Política de Ciberseguridad

- Definir los objetivos de alto nivel de ciberseguridad y obtener aprobación de la alta dirección.
- Identificar (global y localmente) leyes, regulaciones y reglas de gobierno para la ciberseguridad y definir los requisitos.
- Hacer obligatorio estos requisitos en todo el sistema de ciberseguridad y sus componentes.
- Establecer KPIs de ciberseguridad e informes regulares.

Componentes de la Política de Ciberseguridad

- Identificar las amenazas para todas las partes de la empresa
- Anticipar las amenazas futuras provenientes del cibercrimen y la ciberguerra.
- Recoger datos y evidencias sobre incidencias, ataques y violaciones de ciberseguridad.
- Aplicar escaneo horizontal y técnicas detalladas de análisis de datos para obtener un panorama razonablemente sólido sobre el futuro de la ciberseguridad.

Componentes de la Política de Ciberseguridad

- Aprovechar la experiencia externa cuando sea apropiado.
- Establecer un proceso de mejora continua, basado en la experiencia pasada y las tendencias futuras.
- Establecer un proceso de ciberseguridad tolerante a fallos/errores.
- Fomentar una cultura que promueva la mejora y el pensamiento adaptativo.
- Definir un proceso de identificación y evaluación de riesgos apropiado
- Validar las opciones de tratamiento del riesgo en ciberseguridad

Componentes de la Política de Ciberseguridad

- Alinear el riesgo con el modelo seleccionado de gobierno general.
- Incluir incidentes anteriores y aprendizajes técnicos/ organizativos.
- Identificar y evaluar nuevos riesgos derivados del cibercrimen y la ciberguerra.
- Establecer una clasificación de datos en materia de cibercrimen.
- Establecer una clasificación de datos con respecto a la ciberguerra.

Componentes de la Política de Ciberseguridad

- Incluir el almacenamiento y los servicios basados en la nube, así como los datos que residen o que fluyen a través de dispositivos móviles o públicos

- Proporcionar información relacionada con la ciberseguridad para la gestión de identidad y de accesos.

- Identificar las aplicaciones de negocio críticas mediante la realización de un BIA con una perspectiva de ciberseguridad.

- Realizar un análisis de dependencias en profundidad desde la capa de aplicaciones críticas hacia abajo para identificar puntos de entrada potencialmente vulnerables.

Componentes de la Política de Ciberseguridad

- Enfocar la ciberseguridad en el “eslabón más débil de la cadena” y alinearse con el BIA general
- Asignar recursos y financiación en consonancia con las amenazas reales de cibercrimen y ciberguerra, y considerar los vectores y enfoques de ataque indirectos.
- Adoptar la mentalidad del atacante — mayor estrago con mínimo esfuerzo.
- Establecer controles en el ciclo de vida de software para aplicaciones de desarrollo propio y personalizadas.
- Definir un proceso de incorporación de la ciberseguridad para aplicaciones y sistemas potencialmente críticos.

Componentes de la Política de Ciberseguridad

- Involucrar a los proveedores para conseguir controles de ciberseguridad en origen.
- Involucrar a los proveedores para gestionar vulnerabilidades día-cero y puntos de entrada
- Aplicar gobierno (ver capítulo anterior) a las políticas, normas y KOPs de ciberseguridad
- Introducir rutinas de autoevaluación y de evaluación entre pares para el personal expuesto (aseguramiento de la integridad)
- Realizar verificaciones de antecedentes (de forma optativa) para el personal de ciberseguridad.

Componentes de la Política de Ciberseguridad

- Definir e implementar controles y verificaciones apropiadas para los nuevos empleados en puestos sensibles
- Definir e implementar procedimientos adecuados para la finalización de la relación laboral.
- Asegurar el reconocimiento para el personal de ciberseguridad mediante incentivos y reconocimientos apropiados
- Definir la guía de comportamiento en ciberseguridad.
- Fomentar la concienciación sobre la ciberseguridad y el cibercrimen.

Componentes de la Política de Ciberseguridad

- Proporcionar ejemplos y casos prácticos de ataques / violaciones de seguridad.
- Destacar el impacto en el negocio de ataques / violaciones de seguridad
- Enlazar con los principios rectores para la ciberseguridad (ver el texto a continuación).

Procesos

El catalizador Procesos de COBIT 5 está estrechamente relacionado con el modelo de referencia de procesos en el marco COBIT 5. En la gestión de la ciberseguridad, tanto los procesos de gestión como los de supervisión son necesarios para lograr y mantener un nivel adecuado de seguridad.

Procesos de Gestión de la Ciberseguridad

Procesos COBIT 5	Procesos de Gestión de la Ciberseguridad
APO01 Gestionar el marco de gestión de TI.	Integrar la ciberseguridad en el marco de gestión de TI.
APO02 Gestionar la estrategia.	Alinear la estrategia de ciberseguridad con la estrategia general de seguridad de la información.
APO03 Administrar la arquitectura empresarial.	Definir e integrar los componentes de arquitectura de ciberseguridad como parte de la arquitectura general en materia de seguridad de la información.
APO05 Gestionar la cartera.	Proceso subsidiario para identificar y obtener fondos para la gestión de la ciberseguridad.
APO06 Gestionar el presupuesto y los costes.	Presupuesto subsidiario para ciberseguridad, incluyendo la financiación de contingencia para situaciones reales de ataque/violación de seguridad.
APO07 Gestionar los recursos humanos.	Proceso subsidiario para formar en ciberseguridad a usuarios y personal de TI.
APO09 Gestionar los acuerdos de servicio.	Proceso para ANSs y acuerdos de nivel operativo (OLAs) de ciberseguridad en línea con el escenario general de gobierno seleccionado.
APO10 Gestionar los proveedores.	Elementos de proceso añadidos para la gestión de proveedores y terceros en materia de ciberseguridad.

Procesos de Gestión de la Ciberseguridad

Procesos COBIT 5	Procesos de Gestión de la Ciberseguridad
APO12 Gestionar el riesgo.	Proceso subsidiario para identificación, evaluación y tratamiento de riesgos de ciberseguridad.
APO13 Gestionar la seguridad.	Integrar la ciberseguridad como parte del SGSI.
BAI02 Gestionar la definición de requisitos.	Proceso subsidiario para definir requerimientos de ciberseguridad.
BAI03 Gestionar la identificación y la construcción de soluciones.	Proceso subsidiario para identificar soluciones específicas en materia de ciberseguridad.
BAI05 Gestionar la habilitación del cambio organizativo.	Vincular con la transformación de la ciberseguridad, e integrar los pasos de transformación dentro de la gestión del cambio en general.
BAI06 Gestionar los cambios.	Proceso subsidiario para cambios y cambios de emergencia en ciberseguridad.
BAI07 Gestionar la aceptación del cambio y de la transición.	Vincular con la transformación de la ciberseguridad, e integrar los pasos de transformación dentro del cambio general.
BAI08 Gestionar el conocimiento.	Proceso subsidiario de gestión del conocimiento para ciberseguridad.
DSS01 Gestionar las operaciones.	Proceso subsidiario de operaciones para ciberseguridad, relacionado con las operaciones generales de TI, incluyendo servicios externalizados y supervisión de infraestructuras críticas.
DSS02 Gestionar las peticiones y los incidentes de servicio.	Proceso subsidiario de ciberseguridad para identificar, clasificar, escalar y gestionar incidentes relacionados.
DSS03 Gestionar los problemas.	Proceso subsidiario de ciberseguridad para identificar causas raíz, prevenir la recurrencia y recomendar mejoras.

Procesos de Supervisión de la Ciberseguridad

Procesos COBIT 5	Procesos de Supervisión de la Ciberseguridad
APO01 Gestionar el marco de gestión de TI.	Componente del proceso para supervisar el cumplimiento en ciberseguridad
APO02 Gestionar la estrategia.	Componente del proceso para analizar las deficiencias en ciberseguridad
APO04 Gestionar la innovación.	Componente del proceso para supervisar y escanear el entorno tecnológico; componente adicional para supervisar el uso de tecnologías emergente e innovaciones
APO07 Gestionar los recursos humanos.	Componente del proceso para supervisar el cumplimiento contractual del personal
APO09 Gestionar los acuerdos de servicio.	Componente del proceso para revisar los acuerdos en términos de requisitos de ciberseguridad
APO10 Gestionar los proveedores.	Componente de proceso para supervisar el cumplimiento de las condiciones de ciberseguridad por parte del proveedor
APO12 Gestionar el riesgo.	Componente de proceso para mantener un perfil de riesgo de ciberseguridad en base a la supervisión de indicadores
MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad.	Proceso subsidiario para supervisar la ciberseguridad (dentro de los límites legales y reglamentarios)
MEA02 Supervisar, evaluar y valorar el sistema de control interno.	Proceso subsidiario para autoevaluar el control (CSAs) en ciberseguridad, incluyendo informes de ataques/violaciones de seguridad y otras actividades sospechosas
MEA02 Supervisar, evaluar y valorar el cumplimiento con requerimientos externos.	Proceso subsidiario para identificar e interpretar el cumplimiento con requerimientos externos en ciberseguridad

Procesos Relativos a la Continuidad

Procesos COBIT 5	Procesos de Gestión de la Ciberseguridad
DSS02 Gestionar las peticiones y los incidentes del servicio.	Componente del proceso para integrar la respuesta a incidentes con la gestión de incidentes/crisis general.
DSS04 Gestionar la Continuidad.	Componente del proceso para integrar la respuesta a incidentes, recuperación y reanudación con el BCM general.

Estructuras Organizativas

La función de seguridad de la información, incluyendo sus roles y responsabilidades de gestión, se define generalmente como parte de TI o, en algunos casos, de la seguridad corporativa.

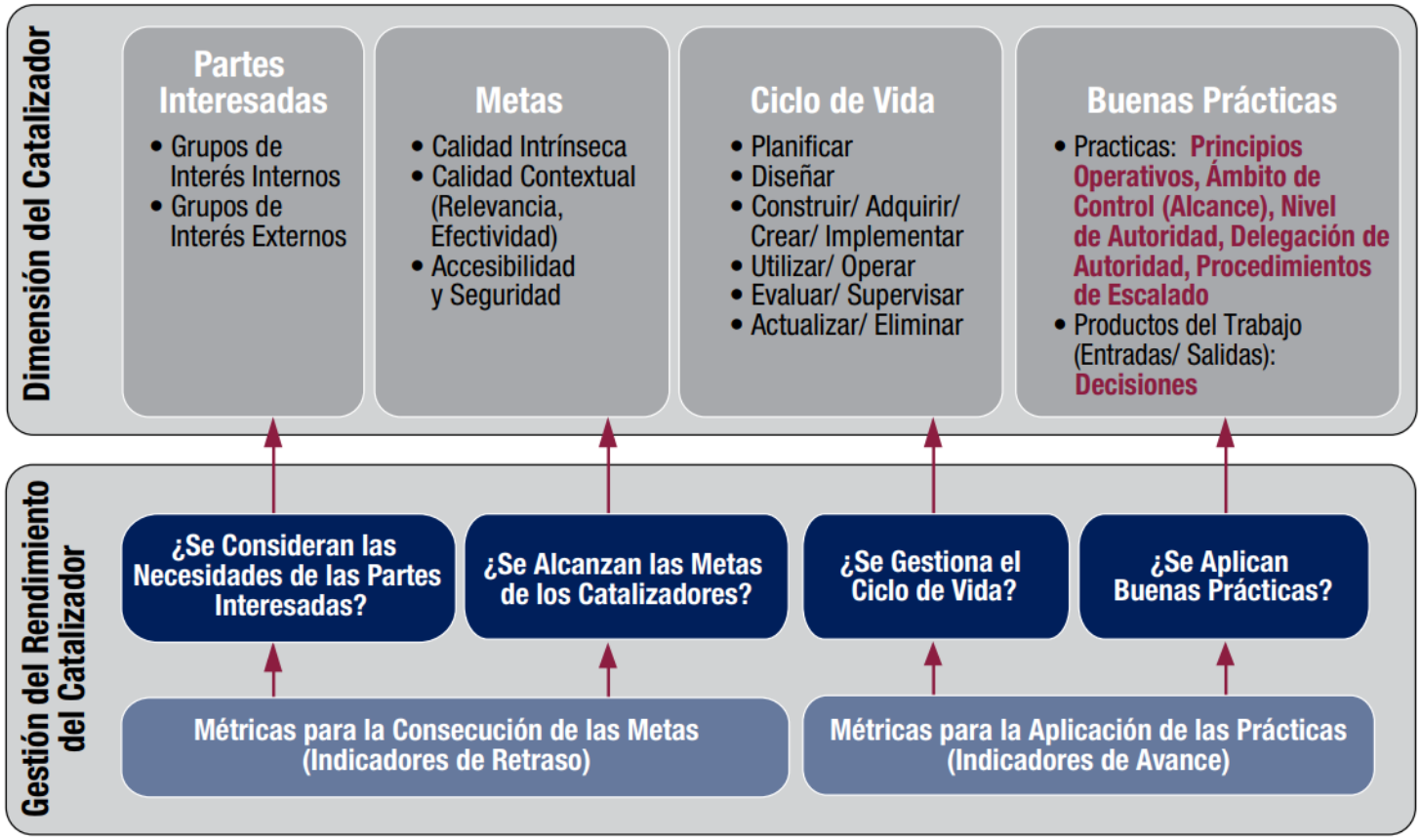
La empresa por lo general coloca la seguridad de la información y sus partes constituyentes bajo un CISO y un Comité de Seguridad.

Estructuras Organizativas

Este catalizador identifica grupos de interés internos y externos, objetivos, el ciclo de vida requerido y buenas prácticas de una manera genérica.

En términos de gestión de la ciberseguridad, esto signifca que los gestores de seguridad deben proyectar el catalizador en sus áreas de responsabilidad y campos de experiencia.

Estructuras Organizativas



Fuente: ISACA, COBIT 5, EE.UU., 2012, figura 32

Cultura, Ética y Comportamiento

Los ataques, las violaciones de seguridad y los incidentes suponen un enorme reto para la cultura de las organizaciones. La evidencia de la ocurrencia de un ataque crea, a menudo, un clima de incertidumbre y sentimientos de vulnerabilidad, así como de inadecuación por parte de los atacados.

El catalizador Cultura, Ética y Comportamiento de COBIT 5 define un conjunto de modelos de comportamiento y valores culturales que deben ser aplicados a la gestión de la ciberseguridad

Modelos de Comportamiento de COBIT 5 en Ciberseguridad

Modelo de Comportamiento de COBIT 5	Aplicación a la Ciberseguridad
La seguridad de la información se ejercita en las operaciones cotidianas.	• Los principios y prácticas de ciberseguridad se aplican en las operaciones cotidianas. • Todos los socios comprenden y aplican por completo y en el momento oportuno las medidas de ciberseguridad.
Las personas respetan la importancia de los principios y políticas de seguridad de la información.	• Todos los usuarios entienden las prioridades definidas en ciberseguridad y cómo aplicarlas en su entorno de TI personal y de negocio. • Todos los usuarios son conscientes, e idealmente están involucrados, en la definición de las políticas y principios de ciberseguridad. • Se actualizan frecuentemente los principios, políticas, estándares y procedimientos de operación críticos de ciberseguridad para reflejar la realidad de la empresa en la práctica.
Las personas cuentan con orientación suficiente y detallada sobre la seguridad de la información y se les anima a participar y afrontar los retos de la situación actual de la seguridad de la información.	• La ciberseguridad es un proceso de transformación con desafíos habituales desde todas las partes de la empresa. • La orientación sobre ciberseguridad es simple, va al grano y se refiere a los típicos riesgos del día a día. • El estado en relación con la ciberseguridad se evalúa constantemente de forma conjunta por los usuarios y los directores de seguridad.
Todo el mundo es responsable de la protección de la información dentro de la empresa.	• Los gerentes de seguridad y los usuarios comparten la responsabilidad en la ciberseguridad. Esto incluye tanto el ámbito del negocio, como el de viajes y el doméstico. • Los usuarios tienen un entendimiento claro de sus responsabilidades y actúan de forma responsable. • La empresa actúa en un entorno tolerante a fallos y evita usar chivos expiatorios.

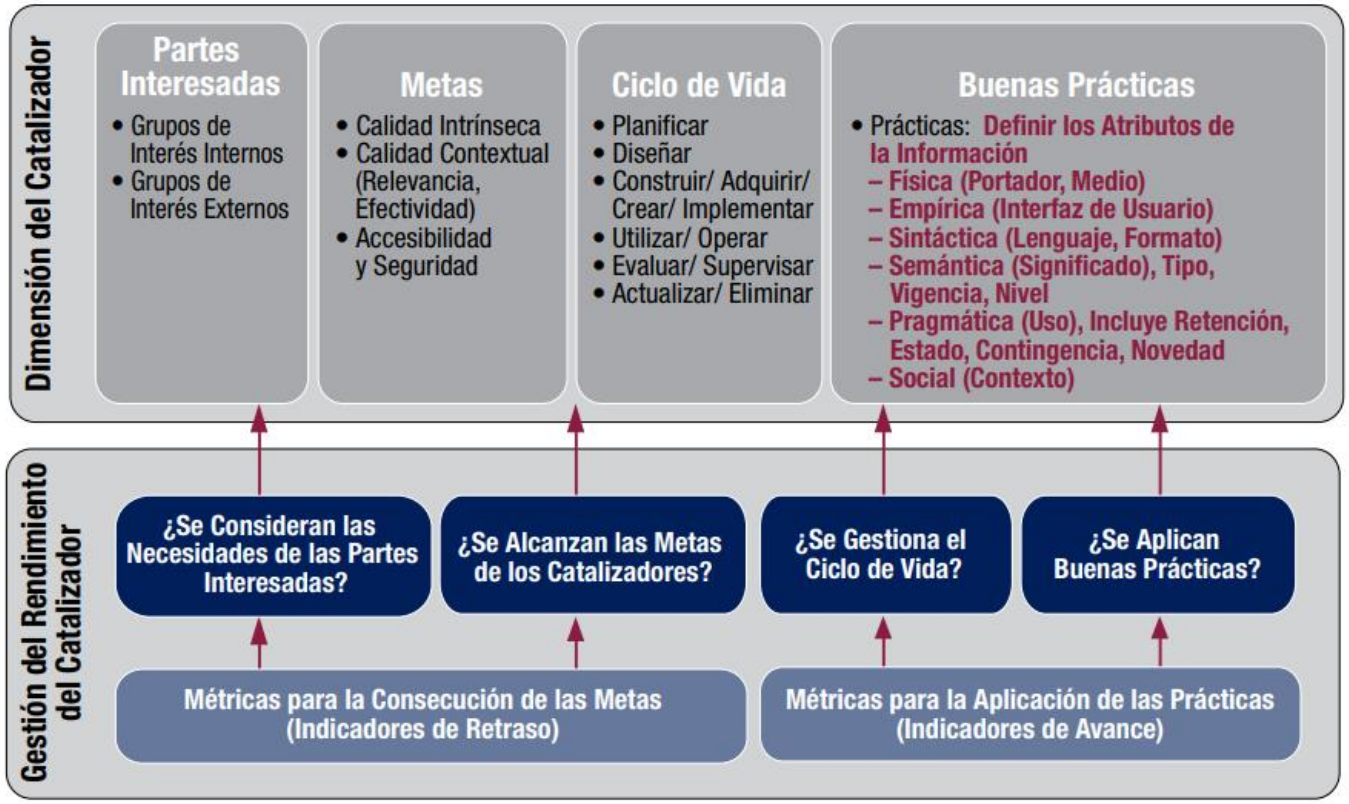
Modelos de Comportamiento de COBIT 5 en Ciberseguridad

Modelo de Comportamiento de COBIT 5	Aplicación a la Ciberseguridad
Las partes interesadas son conscientes de cómo identificar y responder a las amenazas para la empresa.	• Todos los usuarios, independientemente de su nivel jerárquico en la empresa, son partes interesadas en la ciberseguridad. • Los usuarios son suficientemente conscientes del riesgo, amenazas y vulnerabilidades asociadas con los ataques/violaciones de seguridad. • La respuesta ante incidentes y amenazas se entiende correctamente, y se practica habitualmente y se audita.
La dirección sostiene y anticipa de forma proactiva las innovaciones en seguridad de la información y las comunica a la empresa. La empresa es receptiva a tener en cuenta y tratar nuevos retos en seguridad de la información.	• Los gerentes de seguridad y usuarios finales identifican, prueban y adoptan de forma cooperativa innovaciones en ciberseguridad. • La dirección y los usuarios finales identifican y adoptan nuevos casos de negocio aplicables a la tecnología, prácticas de seguridad y otros tipos de valor añadido para la ciberseguridad. • De manera explícita, la empresa desea estar a la vanguardia en ciberseguridad
La dirección del negocio está comprometida en una colaboración multi-funcional continua para lograr programas de seguridad de la información efectivos y eficientes.	• Los programas de ciberseguridad están implantados y forman parte de la estrategia global de innovación. Las innovaciones en seguridad se incorporan como proyectos claves. • Las funciones del negocio cooperan con la seguridad de la información para maximizar la eficiencia y eficacia de la ciberseguridad.
La dirección ejecutiva reconoce el valor de negocio de la seguridad de la información.	• La dirección ejecutiva actúa como usuarios finales y reconoce el valor de la ciberseguridad. Participa activamente en las actividades de formación y concienciación.

Información

El activo central a proteger del cibercrimen y de la ciberguerra es la información de la empresa en sí, incluyendo información de identificación personal y demás activos privilegiados.

Información



Fuente: ISACA, COBIT 5, EE.UU., 2012, figura 36

Información

La primera dimensión se refiere a cualquier dato o información de negocio que deba ser protegido mediante medidas y prácticas de gestión de ciberseguridad.

En muchas empresas, el SGSI general contiene una clasificación de los datos según los criterios de “confidencialidad / integridad / disponibilidad”. Esta clasificación, si existe, debería extenderse añadiendo criterios tales como “atractivo para el cibercrimen” o “atractivo para la ciberguerra.”

La otra dimensión de la información es el conjunto existente de elementos informativos sobre la ciberseguridad en sí misma

Servicios, Infraestructura y Aplicaciones

El catalizador de Servicios, Infraestructura y Aplicaciones identifica las capacidades de servicio, atributos y metas de la gestión de la seguridad de la información, como se describe en COBIT 5 para Seguridad de la Información:

- Arquitectura de seguridad
- Concienciación en seguridad
- Desarrollo seguro
- Evaluaciones de seguridad
- Sistemas asegurados y configurados de forma adecuada
- Acceso y derechos de acceso de los usuarios de acuerdo a los requisitos del negocio
- Protección adecuada ante software malicioso, ataques externos e intentos de intrusión
- Respuesta adecuada ante incidentes
- Pruebas de seguridad
- Servicio de supervisión y alerta para los eventos relacionados con la seguridad

Personas, Habilidades y Competencias

La gestión de la seguridad requiere un amplio conjunto de habilidades y competencias que se describen en COBIT 5 para Seguridad de la Información. La gestión de la ciberseguridad, aunque se ve a menudo como un subconjunto de la seguridad de la información en general, es una actividad muy especializada que requiere habilidades y experiencia adicionales

El concepto de empoderamiento del usuario final es una parte indispensable de la gestión de ciberseguridad. Cuando los usuarios finales no tienen suficientes habilidades o no tienen experiencia en términos de ataques / infracciones, es mucho más probable que la ciberdelincuencia y ciberguerra den lugar a importantes impactos y daños.

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

¡Gracias por su Atención!

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia