CURSO: GOBERNANZA Y GESTIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

Unidad 3: Gestión y evaluación de la seguridad de la información

Patricia Prandini y Raúl Saroka
DOCENTES

Índice

- Clasificación de la información
- Métricas de seguridad de la información
- Modelos de madurez

CLASIFICACIÓN DE LA INFORMACIÓN

Visión general

- La información es un recurso clave para las organizaciones, desde el momento en que se crea hasta que es destruida.
- La tecnología juega hoy un papel fundamental y es utilizada en todos los niveles, tanto operativos como para la gestión y el gobierno.
- La tecnología habilita funciones del negocio, incluyendo las propias de TI.

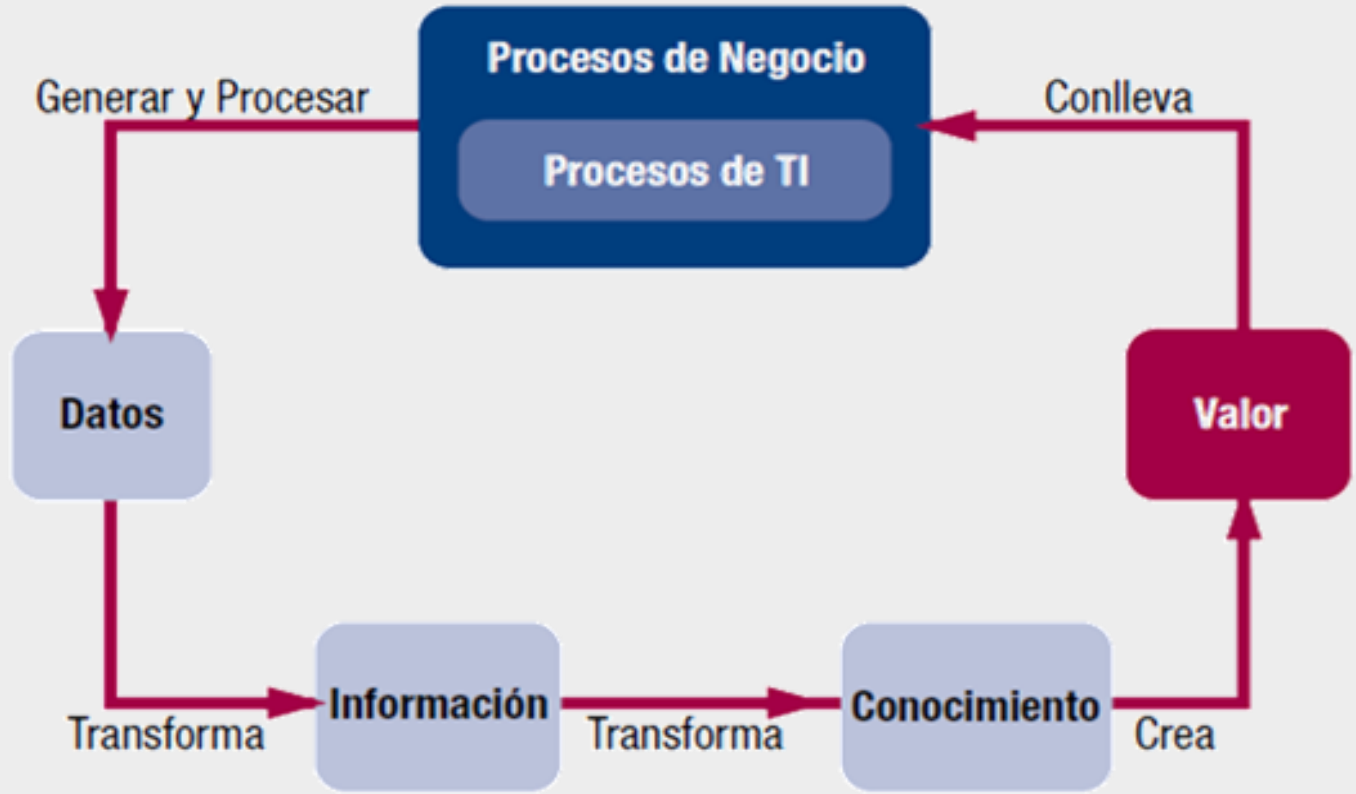
La información contribuye al logro de los objetivos de la organización.

Información

- Incluye toda la información relevante para la organización, no sólo la que es objeto de tratamiento electrónico.
- Puede ser estructurada o desestructurada, formalizada o informal.
- Se analiza con independencia del formato y del soporte utilizado.
- Los procesos de negocio generan y procesan datos, transformándolos en información y conocimiento, generando valor para la organización.

Ciclo de vida de la Información

Figura 35—Metadatos de COBIT 5 - Ciclo de la Información



Elemento que es o representa un hecho (texto, número, texto, gráfico, sonido, video, etc.)

Utilidad o aptitud de las cosas para satisfacer las necesidades o entregar bienestar

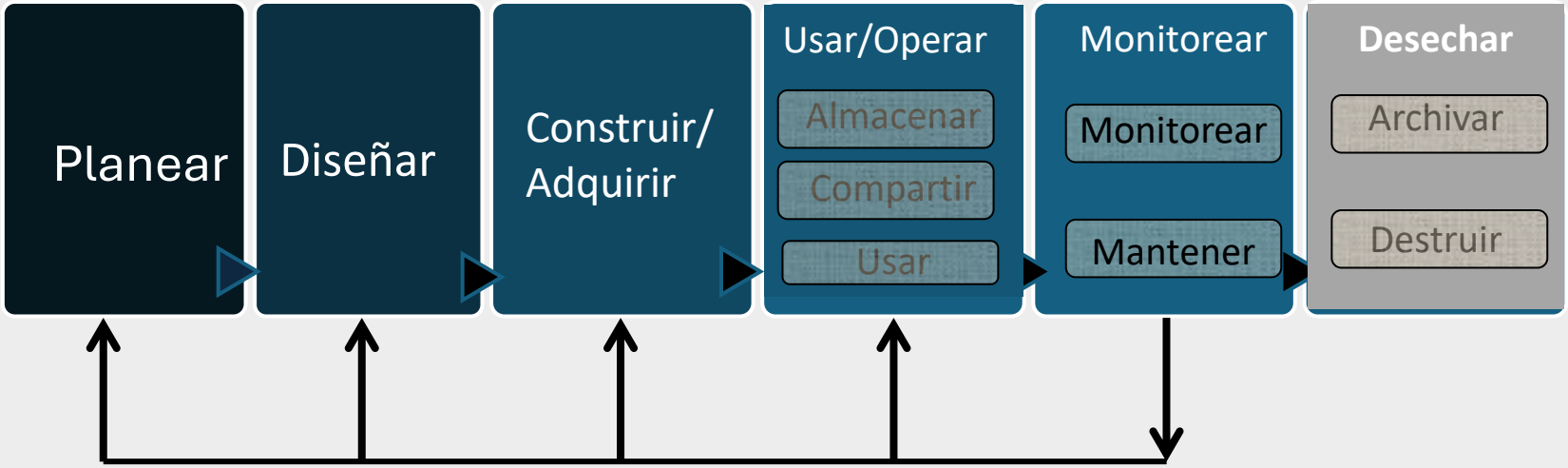
Dato en un contexto determinado, lo que implica darle un significado

Piezas de información que al ser tomadas en conjunto proporcionan valor

Fuente: COBIT 5

Ciclo de vida de la Información

Debe considerarse el ciclo de vida completo de la información, ya que se requieren diferentes enfoques según la fase.



¿En qué etapa se clasifica la información?

Fuente: COBIT FOR INFORMATION SECURITY – Figura 23

Ciclo de vida de la Información

Fase	Descripción	Ejemplos de Actividades
Planear	Consiste en la preparación para la creación, adquisición y uso del recurso de información	▪ Comprender el uso de la información en el proceso de negocio ▪ Determinar el valor del activo de información y **su clasificación** ▪ Identificar objetivos ▪ Planear la arquitectura
Diseñar	Comprende la especificación del formato de la información y la forma en que será procesada	▪ Desarrollo de estándares y definiciones
Construir /Adquirir	Abarca la adquisición de la información	▪ Creación de los registros de datos ▪ Adquisición de datos ▪ Incorporación (“loading”) de archivos externos

Ciclo de vida de la Información

Fase	Descripción	Ejemplos de Actividades
Usar/ Operar	Incluye: Almacenar: retener la información en formato electrónico, papel, memoria humana, etc.	▪ Resguardar la información en soporte electrónico, papel, etc.
	Compartir: permitir que la información se encuentre disponible para su uso a través de algún método de distribución	▪ Desarrollar procesos que impliquen hacer llegar la información a lugares donde pueda ser accedida y utilizada. (Puede haber superposiciones con la etapa de almacenamiento, p.e. BD)
	Usar: utilizar la información para cumplir los objetivos	▪ Usar la información en situaciones de todo tipo (decisiones gerenciales, procesos automáticos, etc.)

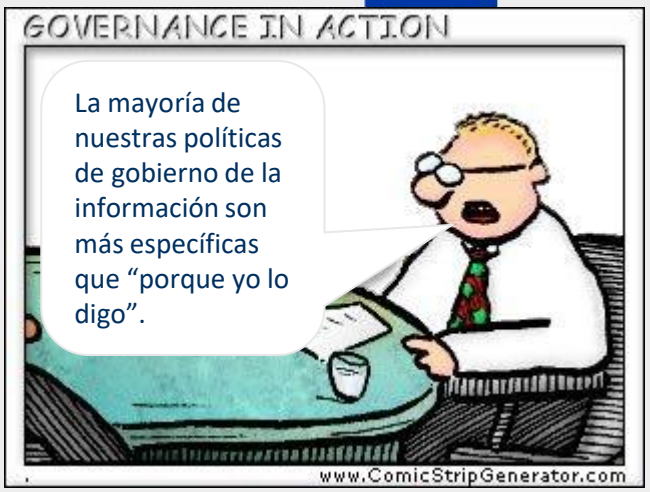
Ciclo de vida de la Información

Fase	Descripción	Ejemplos de Actividades
Monitorear	Abarca el aseguramiento de que el recurso continúa trabajando correctamente	▪ Actualizar la información ▪ Realizar otras actividades de gestión de información (remoción de duplicados, mejora, combinación, etc.)
Desechar	Comprende la transferencia o retención por un período determinado, la destrucción o el archivo, según sea requerido	▪ Retener la información ▪ Archivar la información ▪ Destruir la información

Información

Las organizaciones cuentan con:

- Políticas (normas) respecto del uso y clasificación de la información.
- Asignación de roles y responsabilidades



<u>Propietario/dueño del dato (data owner)</u>

- Quien toma decisiones sobre su tratamiento durante el ciclo de vida, o sea, desde su recolección, hasta su almacenamiento y/o destrucción.
- Además, establece las condiciones de calidad y seguridad de la información y participa en la evaluación de riesgos del negocio analizando aquellos a los que está expuesto el dato.

Información

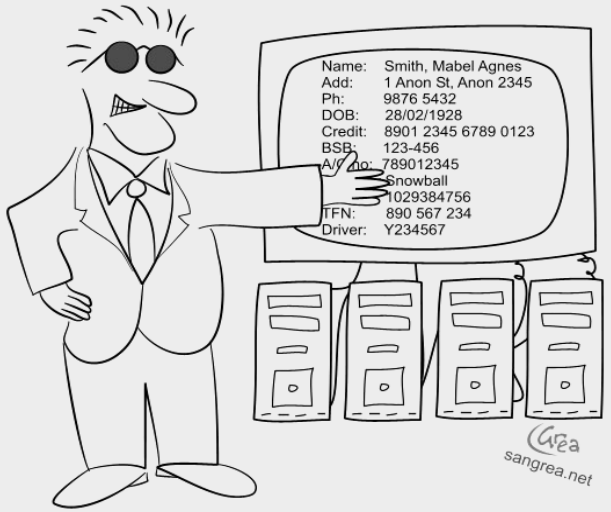
Consideraciones para los dueños de datos:

- **Requerimientos legales** (por ejemplo, Ley de Protección de Datos Personales)
- **Disponibilidad** para la continuidad del negocio, especialmente, la información crítica.
- **Integridad**
- **Difusión**
- **Concientización**
- **Accesos**
  - ¿Quién tiene derechos de acceso y a qué?
  - ¿Cuál es el nivel de acceso a ser otorgado?
  - ¿Qué aprobaciones son necesarias para otorgar accesos?

Información

Custodio de la información (data custodian) Responsable de implementar tecnológicamente las reglas del negocio respecto de seguridad, calidad, almacenamiento, transporte, transferencia y destrucción.

Por lo tanto, los custodios de la información no son responsables de tomar decisiones respecto de su criticidad o tratamiento.



¡Hola! ¿Quiere comprar datos? Están apenas usados. Su último dueño fue una viejita que los usaba para hacer compras

Clasificación de la Información

Es la organización sistemática de la información en categorías, con el objeto de gestionarla de manera predefinida.

Debe ser:

- Sistemática: método consistente
- Categorías: agrupamientos alrededor de los cuales se organiza la información

(Adaptada del Internet Security Forum)

Clasificación de la información

En el contexto de la seguridad de la información, se basa en su nivel de criticidad y en el impacto para la entidad de su exposición, alteración o destrucción no autorizada.

(Adaptada de Carnegie Melon University)

Es la decisión conciente de asignar un nivel de criticidad a los datos cuando son creados, almacenados o transmitidos.

Clasificación de la información

¿Por qué es importante clasificar la información?

- Uso malicioso
- Volumen creciente
- Nuevas regulaciones

Si bien las necesidades son obvias, no es así respecto a las soluciones, dada la complejidad de la información, la sofisticación de la tecnología y la creciente disponibilidad de soluciones.

Fuente: SANS Institute

Clasificación de la información

- Facilita el cumplimiento de **requerimientos regulatorios**, minimizando el riego de sanciones monetarias y/o penales.
- Permite **ahorrar esfuerzos y costos**, garantizando que solo los roles adecuados intervengan en los procesos.
- Provee una **ventaja competitiva**, ya que ejemplifica para el resto de la organización y para otras partes, la voluntad de proteger los datos.
- **Mejora los resultados de las auditorías**, debido a que muestra a los auditores la existencia de un análisis serio y organizado y brinda a los empleados una serie de objetivos a ser cumplidos.

Fuente: SANS Institute

Clasificación de la información

Algunas consideraciones:

- Es un punto de partida para la ejecución de otras acciones.
- Solo se pueden construir políticas y procedimientos sólidos y costo-efectivos a partir de un adecuado programa de clasificación.
- La **consistencia** en la aplicación de un programa de clasificación es clave: lo que para una persona es muy crítico para otra puede ser sólo crítico. Tener en cuenta las complejidades de varias partes involucradas.

Clasificación de la información

- Cada organización fija sus niveles (no hay un único estándar).
- La clasificación se vincula con el nivel de protección requerido.
- Demasiados niveles son poco prácticos y pueden confundir.
- Pocos niveles dan una escasa percepción del valor para la organización y de las instancias de su utilización.
- No debe haber superposición entre los niveles de clasificación.

Clasificación de la información

- Cada nivel debe asociarse a criterios claros y predefinidos.
- Los niveles deben utilizarse también para los sistemas y otros activos utilizados para gestionar la información.
- Los usuarios involucrados deben conocer los niveles y criterios de clasificación, a través de políticas y procedimientos específicos.
- La clasificación no es una asignación estática, varía en el tiempo.

Clasificación de la información

- Al analizar el impacto, la agregación de información puede tener implicancias en su clasificación, ya que los sistemas electrónicos facilitan estos procesos al punto que agregar o copiar una base puede demandar prácticamente el mismo esfuerzo que hacerlo con un solo registro.
- Por ejemplo, al analizar una filtración de datos personales, es importante conocer la cantidad de registros involucrada. Las consecuencias no serán las mismas si el acceso no autorizado fue a un solo registro o a toda la base.

Clasificación de la información

- El esquema elegido debe ser **fácil de comprender, utilizar y mantener**.
- La mayoría de los sistemas de clasificación se focalizan en la **confidencialidad**. Sin embargo, este enfoque es limitado y se debe ampliar a otros aspectos como la **integridad y la disponibilidad**.

Clasificación de la información

ISO/IEC 27001/2022 – Anexo A

5.12 - La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la **confidencialidad, la integridad, la disponibilidad** y los requisitos pertinentes de las partes interesadas.

5.13 - Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el **etiquetado de la información de acuerdo con el esquema de clasificación de la información** adoptado por la organización.

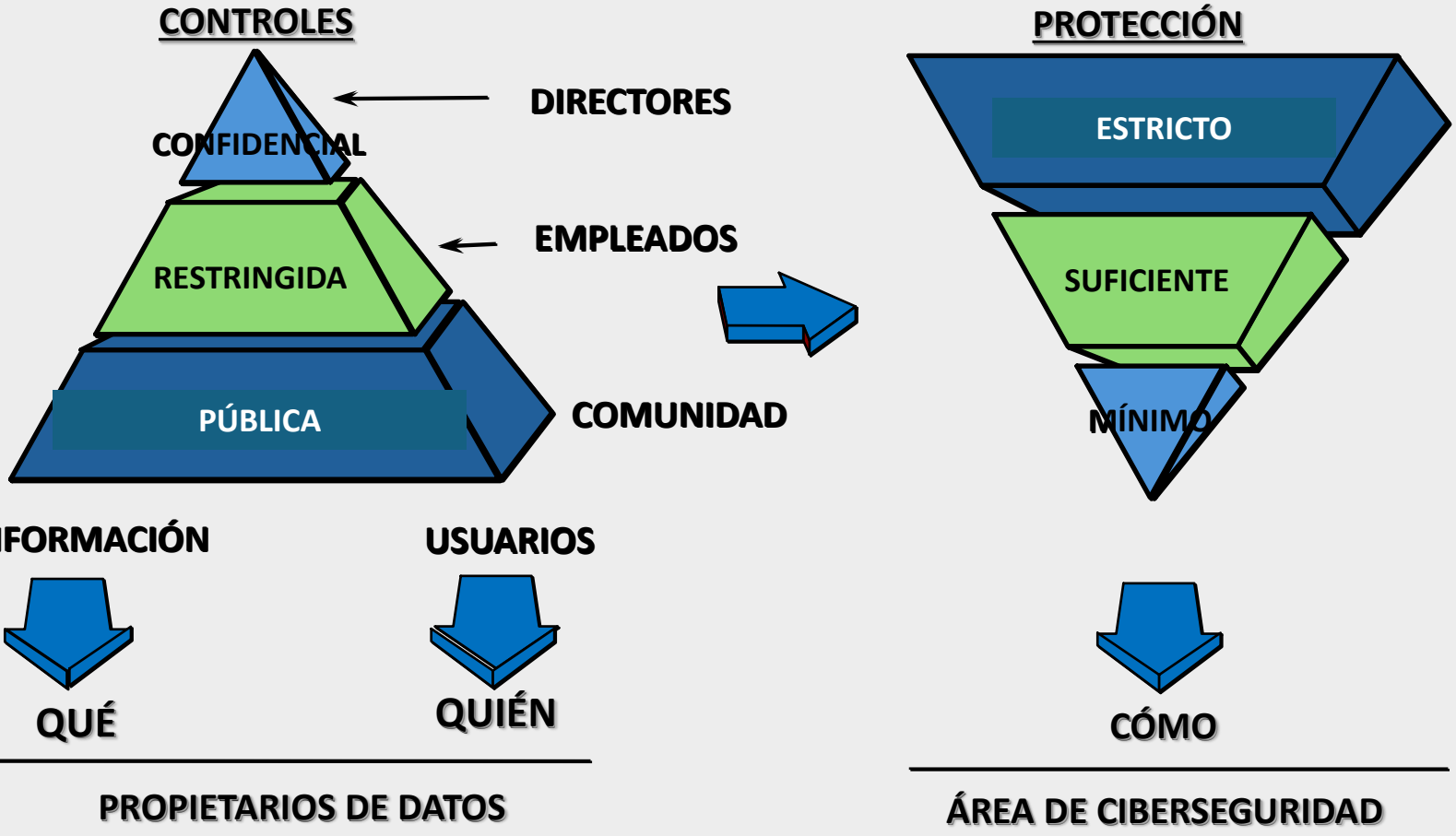
Clasificación de la información

ISO/IEC 27001/2022 – Anexo A (cont.)

6.1 - Los **controles de verificación de antecedentes de todos los candidatos** para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y **serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.**

7.10 - **Los medios de almacenamiento deben gestionarse** a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación **de acuerdo con el esquema de clasificación** y los requisitos de manipulación de la organización.

Protección de la Información



Clasificación de la Información

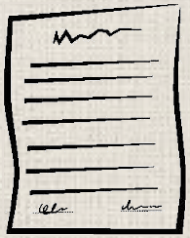
Desafíos de la clasificación de la información

Distintos tipos de información

Clasificación de la Información

Distintos estados en el ciclo de vida

Creación



Proceso

Almacenamiento

Transmisión

Destrucción

Distintos formatos

Política de Clasificación de información

- La clasificación de información forma parte de un conjunto de políticas asociadas a la gestión de activos de la organización.
- Una política de clasificación de la información puede contener como mínimo:
  - Objetivos
  - Alcance
  - Responsabilidades
  - Esquema y criterios de clasificación
  - Metodología de clasificación
  - Glosario
  - Ejemplos que faciliten el proceso de clasificación

Gestión de la clasificación de información

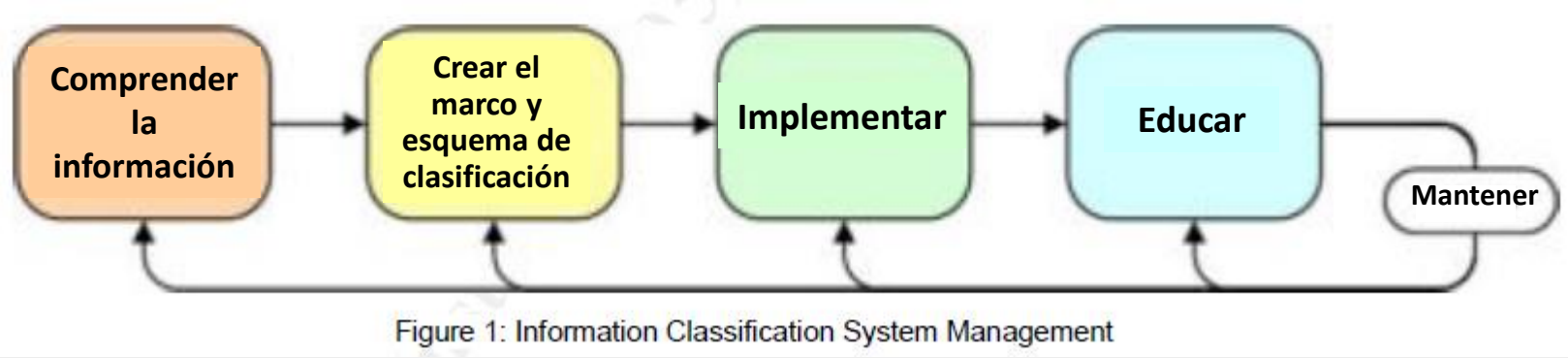


Figure 1: Information Classification System Management

Clasificación – Acceso, creación, manejo, almacenamiento , envío y recepción (transmisión, transferencia) de información clasificada

Políticas, documentos de catalogación de seguridad, clasificación de datos existentes

Procedimientos para la comunicación de los resultados de la clasificación, tales como rotulado, inventario, concientización, cláusulas en acuerdos y procedimientos de seguridad, etc.

Entrenamiento formal, campañas de concientización, inducción al ingresante

Fuente: SANS Institute

Conclusiones (1/2)

- La pérdida de datos por múltiples vectores es una realidad.
- La clasificación de la información es un proceso continuo e iterativo.
- Deben implementarse estándares y procedimientos para asegurar que cada nueva pieza de información crítica sea clasificada.
- La clasificación de la información debe realizarse los más temprano posible respecto al momento de creación del dato.

Conclusiones (2/2)

- El esquema elegido debe ser fácil de comprender, utilizar y mantener y especialmente, aplicado en forma consistente en toda la organización.

- El usuario debe participar en el proceso desde su rol.

- Sin una adecuada clasificación, las decisiones para proteger la información se tomarán cada día de manera discrecional por administradores, propietarios y usuarios.

- Un adecuado programa de clasificación permite asegurar que las decisiones se toman en base a los objetivos de protección de la información de la organización.

MÉTRICAS DE SEGURIDAD DE LA INFORMACIÓN

Métricas de Seguridad

¿La seguridad de la información PUEDE medirse?

¿La seguridad de la información DEBE medirse?

Veamos un caso probable….

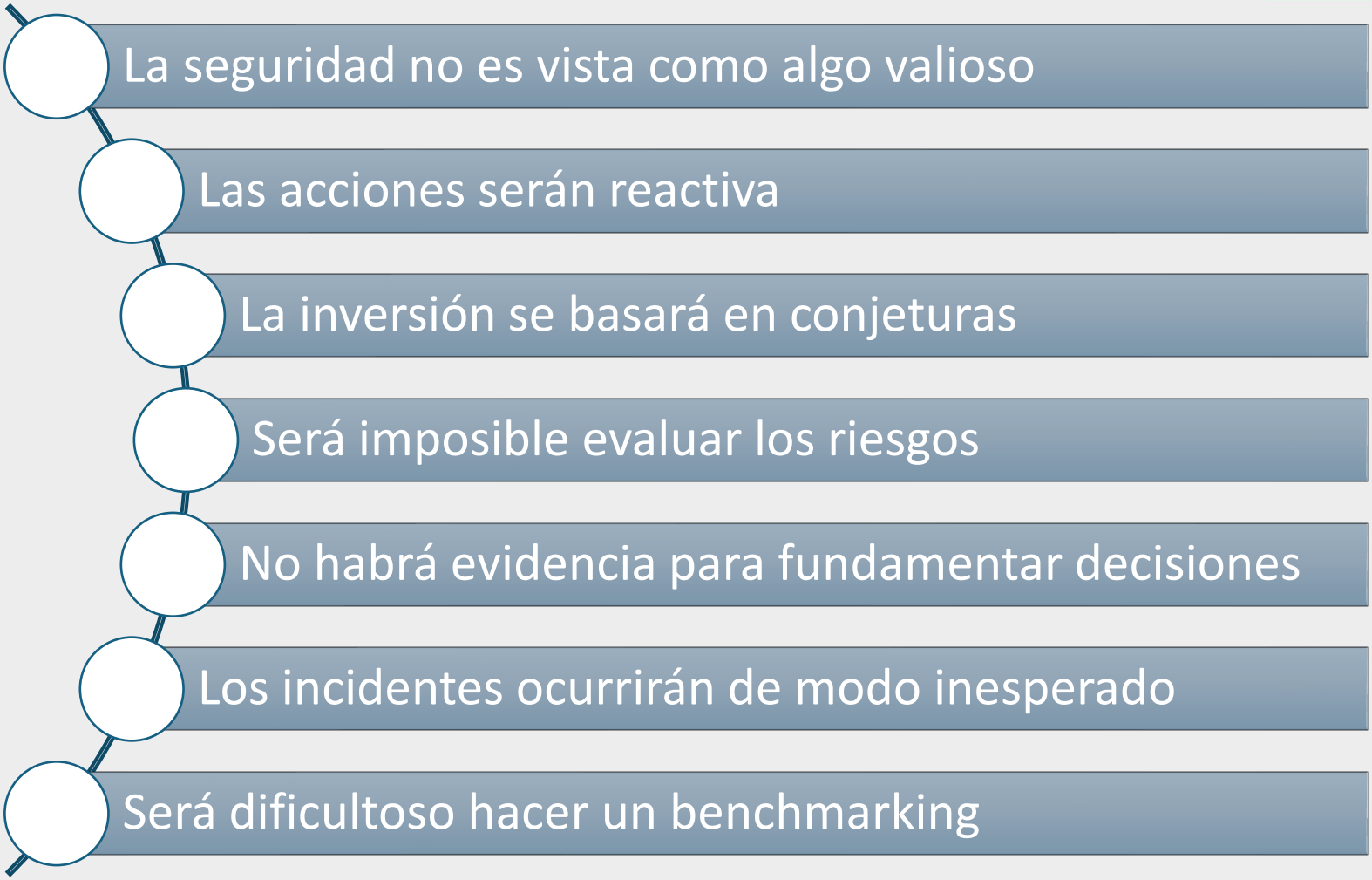
Métricas de Seguridad

ACTUALIZACIÓN INFORMÁTICA
CPAP

Algunas razones por las que un CISO debe contar con métricas

- Mejorar sistemáticamente la seguridad de la información
- Responder a las preguntas de la Dirección
- Atender cuestiones tácticas y operativas
- Asegurar el cumplimiento normativo y responder a auditorías
- Implementar mejores controles
- Disminuir pérdidas y respaldar el negocio permitiendo decisiones racionales

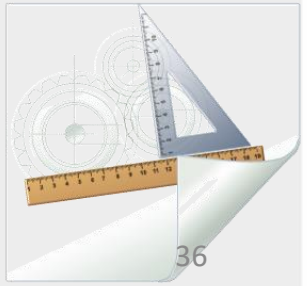
Problemas de no medir



Definiciones

- ✓ **Medición:** Valor tomado en un determinado momento en el tiempo. Surge del cálculo y es solo un dato.

- ✓ **Métrica:** Es un valor calculado en base a la comparación de dos o más mediciones obtenidas a lo largo del tiempo, contra un determinado parámetro previamente definido. Surge del análisis y es una interpretación en base a datos.



¿Por qué usarlas? (1/2)

- Son **una herramienta fundamental** para EVALUAR el Sistema de Gestión de Seguridad de la Información, ya que permiten determinar su:
  - Grado de efectividad
  - Eficiencia
  - Nivel de Implementación
  - Madurez

- Permiten demostrar **la efectividad de un programa, de algunos de sus componentes, de un producto o de un proceso** vinculado a la seguridad, así como **la habilidad del área** para realizar su tarea

¿Por qué usarlas? (2/2)

- Permiten **analizar el riesgo** a asumir por ejecutar una acción determinada
- Proveen una **guía para determinar prioridades**
- Pueden ser usadas para **aumentar la concientización**
- Permiten a los responsables de seguridad de la información **responder a las siguientes preguntas:**

¿Estamos hoy más seguros?

¿Estamos lo suficientemente seguros?

¿Cómo estamos en comparación con otras organizaciones?

Características

Las métricas deben:

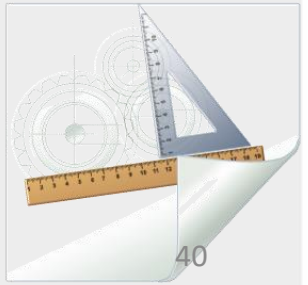
- ✓ Indicar **el grado en que se cumplen los objetivos de seguridad**, p.e. confidencialidad
- ✓ **Llevar a la acción** para mejorar el programa de seguridad de la organización
- ✓ **Desarrollarse en función del receptor** (gobierno o gestión)

- ✓ **Específicas**
- ✓ **Medibles**
- ✓ **Alcanzables**
- ✓ **Repetibles**
- ✓ **Actuales**

SMART

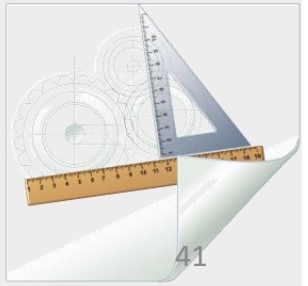
Ejemplos de métricas - 1

- Cantidad de personas que completaron y aprobaron un entrenamiento sobre seguridad
- Proporción de cuentas de usuario inactivas deshabilitadas de acuerdo con políticas
- Cantidad de incidentes de seguridad reportados por clientes, usuarios, empleados, etc.
- Cantidad de observaciones críticas de auditoría
- Cantidad y tipo de llamados a la mesa de ayuda relativos a seguridad de la información



Ejemplos de métricas - 2

- Proporción de sesiones bloqueadas por el firewall
- Intentos de acceso a sitios web de listas negras
- Cantidad de intentos de ataque repelidos
- Indicador de respuesta a las actividades de concientización (por ejemplo, cantidad de mensajes de correo o llamadas)
- Cantidad de personal asignado al área de seguridad
- Costo de las brechas de seguridad



Principales Dificultades

- Falta de Parámetros de Referencia
- Diferencia de intereses (Técnicos / Directivos)
- Barrera de comunicación
- Inmadurez de la disciplina y falta de terminología

Principales Dificultades y Soluciones

- Falta de Parámetros de Referencia
  - Participar a distintas áreas en la definición de los baseline
- Diferencia de intereses (Técnicos / Directivos)
  - Diferenciar las métricas Operativas de las Tácticas y Estratégicas
- Barrera de comunicación
  - Buscar la mejor manera de comunicar las métricas y analizar el grado de interés de los receptores en cada una
- Inmadurez de la disciplina y falta de terminología
  - Identificar experiencias y profundizar en el tema

Requisitos mínimos de las métricas

Para cada métrica, se debe especificar:

- **Propósito y alcance**
- **Fuente del dato** (logs de firewalls/sistemas, mesas de ayuda, informes de auditoría, reportes de usuarios, productos de recolección automática, etc.)
- **Frecuencia de recolección**
- **Cálculo**
- **Responsable** del dato, incluyendo precisión, compilación y generación

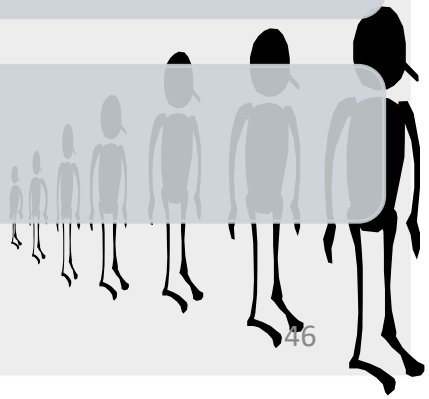
¿A quiénes van dirigidas?

- Es fundamental pensar en la audiencia
- Responden a preguntas a todos los niveles:

OPERATIVO	• ¿Qué incidentes de seguridad se presentan con mayor frecuencia en la organización?
TÁCTICO	• ¿Cuán efectivas son las herramientas de seguridad implementadas?
ESTRATÉGICO	• ¿Cuál es el grado de madurez de la organización en términos de seguridad?

¿A quiénes van dirigidas?

Externos	• Propietarios - transparencia • Reguladores y autoridades – cumplimiento y transparencia • Clientes y sociedad en general – transparencia
Directivos	• Razones estratégicas • Gobierno de las TI y de la seguridad • Transparencia
Mandos medios	• Gestión de la seguridad • Mejora de procesos
Operaciones	• Aspectos técnicos
Pares	• Benchmarking • Buenas prácticas



Conclusión

- Las métricas son una **herramienta para la toma de decisiones** y una **práctica esencial de la gestión y el gobierno** de la seguridad de la información
- Deben proporcionar **información cuantificable**
- Deben permitir el logro de **mejoras** en la seguridad (y poder demostrarlo)
- Los datos que las soportan deben ser **sencillos de obtener**

Es importante empezar por un programa de implementación de métricas sencillo, que produzca rápidos resultados, económico y sobre la base de información existente

MODELOS DE MADUREZ

Buenas prácticas y modelos de madurez

- Las **buenas prácticas** son iniciativas que funcionan en forma efectiva y eficiente en un determinado contexto y dado un contexto similar, se espera que funcionen del mismo modo.

- La implementación de un marco de buenas prácticas asegura que una organización cubra todos los aspectos relevantes que pueden afectar positiva o negativamente la protección de la información.

- Las buenas prácticas permitan el establecimiento de una estructura efectiva de gobernanza de la seguridad de la información.

Modelo de Madurez

Un **MODELO DE MADUREZ** es un conjunto estructurado de elementos que permiten determinar el **NIVEL DE MADUREZ** de una organización en un aspecto determinado, como por ejemplo, la **SEGURIDAD DE SU INFORMACIÓN**

El **USO DE NIVELES DE "MADUREZ"** refiere a la adopción y uso de **BUENAS PRÁCTICAS DE SEGURIDAD** para la protección de la confidencialidad, integridad y disponibilidad de la información en la organización.

Modelos de Madurez

- Establecen un lenguaje común, que facilita la comunicación
- Proporcionan una hoja de ruta e indican el progreso
- Determinan el orden en que se deben aplicar los controles de seguridad
- Determinan los recursos necesarios para el programa de seguridad
- Permiten la generación de medidas de seguridad válidas y reproducibles
- Facilitan la comparación con pares
- Pueden habilitar el cumplimiento de requisitos regulatorios

Modelos de Madurez

Al seleccionar el modelo de madurez a utilizar, se debe tener en cuenta, entre otros aspectos:

- El tamaño y tipo de organización
- El sector industrial
- La madurez actual de la organización
- Los requisitos regulatorios aplicables

Niveles de Madurez

- Los niveles proporcionan información y contexto sobre la manera en que una organización gestiona el riesgo de ciberseguridad y su proceso para gestionarlo.

- Los niveles describen qué tan bien integradas están las decisiones de riesgo ante ciberincidentes y el grado en que se comparte y recibe información sobre ciberseguridad de fuentes externas.

- En general, estos niveles reflejan una progresión desde respuestas informales y reactivas hasta enfoques ágiles y basados en riesgos.

Modelos de Madurez

ACTUALIZACIÓN INFORMÁTICA

CPAP

Nivel	ISO 27001	NIST Cybersecurity Framework	CIS Critical Security Controls
Nivel 1: Inicial	La organización no ha implementado un sistema de gestión de la seguridad de la información (SGSI).	La organización tiene una comprensión básica de los riesgos de ciberseguridad, pero no ha implementado ningún control formal para mitigarlos.	La organización no ha implementado ninguno de los controles de seguridad CIS.
Nivel 2: Implementado	La organización ha implementado un SGSI, pero no lo ha integrado completamente en sus operaciones.	La organización ha implementado controles básicos para mitigar los riesgos de ciberseguridad, pero no los ha integrado completamente en sus operaciones.	La organización ha implementado los controles de seguridad CIS, pero no los ha integrado completamente en sus operaciones.
Nivel 3: Gestionado	La organización ha integrado el SGSI en sus operaciones y lo gestiona de forma proactiva.	La organización ha integrado los controles de ciberseguridad en sus operaciones y los gestiona de forma proactiva.	La organización ha integrado los controles de seguridad CIS en sus operaciones y los gestiona de forma proactiva.
Nivel 4: Optimizado	La organización mejora continuamente su SGSI en función de las lecciones aprendidas y las oportunidades de mejora.	La organización mejora continuamente sus controles de ciberseguridad en función de las lecciones aprendidas y las oportunidades de mejora.	La organización mejora continuamente sus controles de seguridad CIS en función de las lecciones aprendidas y las oportunidades de mejora.

Fuente: **Modelos y Niveles de Madurez en Ciberseguridad -** https://fysinformatica.com/new2/modelos-y-niveles-de-madurez-en-ciberseguridad/

Ejemplo de niveles de madurez

- **Nivel 0:** acciones vinculadas a seguridad de la información y ciberseguridad son **casi o totalmente inexistentes**. La organización no ha reconocido aún la necesidad de realizar esfuerzos en ciberseguridad. Este nivel no es incluido en la tabla del modelo de madurez.

- **Nivel 1: algunas iniciativas sobre ciberseguridad**, aunque los esfuerzos se realizan en forma aislada. Se realizan implementaciones con enfoques ad-hoc y existe alta dependencia del personal que lleva a cabo las tareas que habitualmente no se encuentran documentadas y una actitud reactiva ante incidentes de seguridad.

Fuente: AGESIC - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/estructura-del-marco-ciberseguridad/modelo-madurez

Ejemplo de niveles de madurez

- **Nivel 2: ciertos lineamientos** o pautas para la ejecución de las tareas, pero aún existe **dependencia del conocimiento individual.** Se ha avanzado en el desarrollo de los procesos y existe cierta documentación para realizar las tareas.

- **Nivel 3: formalización y documentación de políticas y procedimientos, así como implementaciones de alta complejidad y/o automatizaciones que centralizan y permiten iniciativas de gobernanza**. Las políticas y procedimientos son difundidos, facilitan la gestión y posibilitan establecer controles y métricas. Los esfuerzos en ciberseguridad se enfocan en los procesos, las personas y la tecnología.

Fuente: AGESIC - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/estructura-del-marco-ciberseguridad/modelo-madurez

Ejemplo de niveles de madurez

- **Nivel 4:** el **Responsable de la Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del Sistema de Gestión de Seguridad de la Información (SGSI)** realizando o coordinando actividades de control interno para verificar cumplimientos y desvíos. Se desarrollan las lecciones aprendidas que, junto con los controles determinan acciones para la mejora continua. Las partes interesadas son informadas periódicamente, lo cual permite alinear los esfuerzos, estrategias y tecnologías de ciberseguridad con los objetivos y estrategias de la organización.

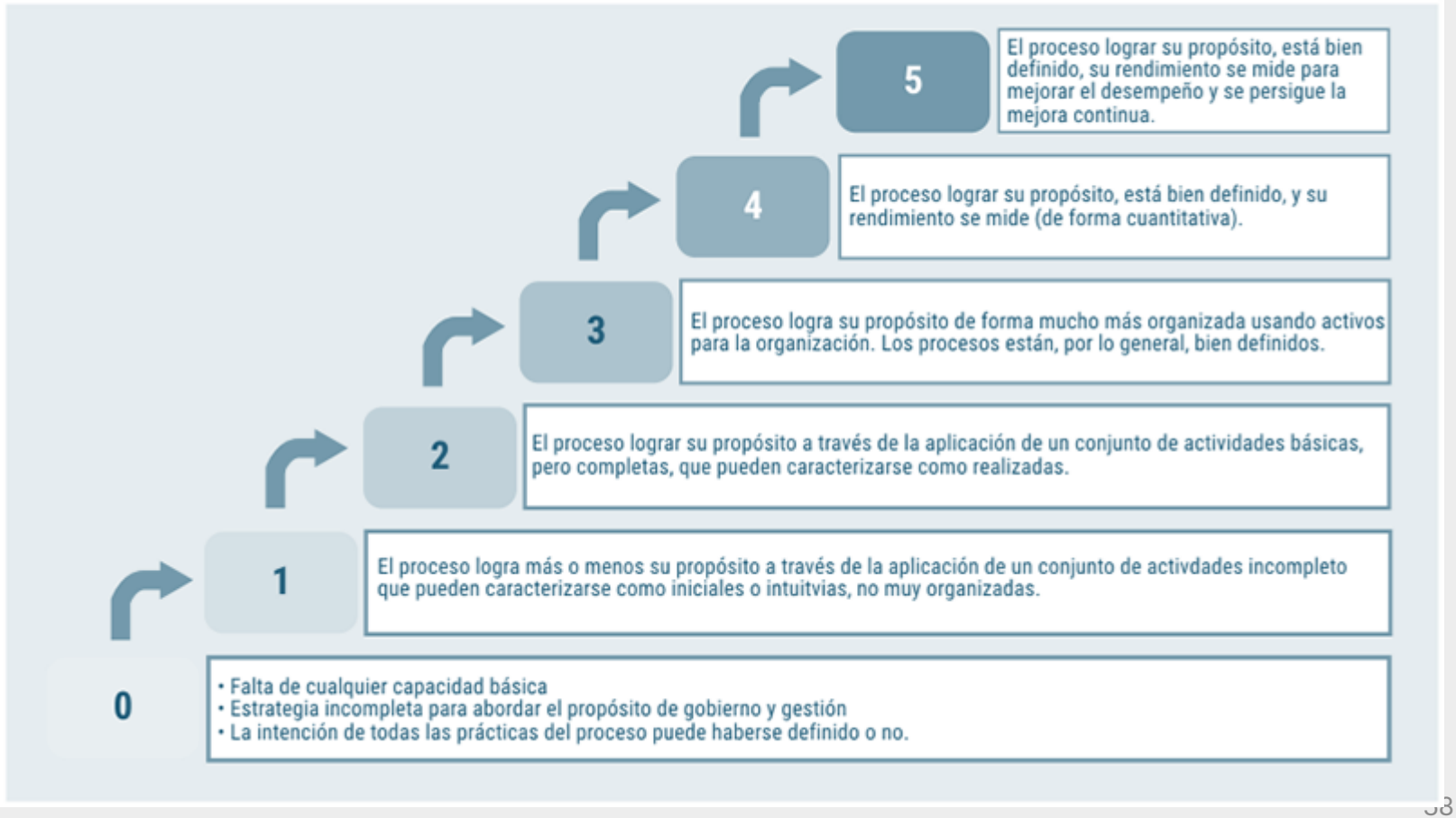
Fuente: AGESIC - https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/estructura-del-marco-ciberseguridad/modelo-madurez

Ejemplo de niveles de madurez

ACTUALIZACIÓN INFORMÁTICA
CPAP

COBIT 2019- Modelo de evaluación de Procesos

Figura 2—Niveles de capacidad para procesos



Ejemplo de niveles de madurez

Nivel	Descripción
Inicial	No existe un programa de seguridad formal. Las medidas de seguridad son reactivas y ad hoc.
Repetible	Se han establecido procesos y procedimientos básicos de seguridad. La organización puede repetir acciones de seguridad de manera consistente.
Definido	Se ha documentado un programa de seguridad formal. Los roles y responsabilidades están claramente definidos.
Medido	Se han establecido métricas para medir la efectividad de las medidas de seguridad.
Gestionado	Se utilizan los datos de las métricas para tomar decisiones informadas y mejorar continuamente el programa de seguridad.
Optimizado	La organización es proactiva en la identificación y mitigación de riesgos. La seguridad está integrada en todos los procesos de negocio.

Evaluación del Modelo de Madurez

- Se trata de un análisis profundo de las defensas cibernéticas de una organización, su grado de preparación y su habilidad para enfrentar ataques.

- La evaluación busca determinar el nivel de desempeño de los controles, procedimientos y regulaciones de ciberseguridad y ayudar a las entidades a identificar puntos de falla y mejora.

- Las entidades pueden priorizar sus activos y esfuerzos para mejorar su postura de seguridad si comprenden bien su nivel de madurez tecnológica actual.

Beneficios de los modelos de madurez

- ✓ Permiten una **visión integral y sistémica** del estado de la seguridad de la información en la organización
- ✓ Habilitan la **comparación** de la situación en el tiempo y respecto a las mejores prácticas y a otras organizaciones
- ✓ Son **base para la identificación y priorización** de las inversiones
- ✓ Sustentan el **plan estratégico y los planes operativos**
- ✓ Permiten establecer y consensuar **nuevos requerimientos** entre las áreas de la organización
- ✓ Dan pie a la **evaluación del éxito** en nuevos proyectos y de la **efectividad** de lo realizado en proyectos terminados o en avance

CURSO: GOBERNANZA Y GESTIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

Unidad 3: Gestión y evaluación de la seguridad de la información

Patricia Prandini y Raúl Saroka
DOCENTES