METODOLOGIA PARA UNA PLANIFICACION EFICAZ

Nogueron,L.,Russo, A.
Gerencia TIC – División Seguridad Informática
Gerencia de Calidad-Departamento CAC
CNEA – Centro Atómico Constituyentes
Contactos: drusso@cnea.gov.ar, lnogueron@cnea.gov.ar

Objetivos:

Presentar una metodología que facilite el desarrollo de las tareas de planificación de los sectores que permita integrar en forma coherente y consistente la planificación estratégica, los objetivos generales y particulares, procesos, tareas e indicadores.

Desarrollo

I-Introducción:

La planificación es, tal vez, la tarea más importante en cuanto condiciona el hacer y el actuar. En los tiempos que corren es inaceptable manejar el concepto de trabajar sin una planificación con sus objetivos, metas y estrategias a seguir. A su vez es importante definir los actores más importantes de cada etapa ya que esto permite identificar responsabilidades.

Cuando no hay planificación, el comportamiento es de forma reactiva, es decir, se van tomando decisiones a medida que los problemas o necesidades van apareciendo. Cuando se es proactivo, se actúa únicamente en la medida en que hay cosas que resolver. En realidad, si no hay ningún imprevisto o ningún problema acuciante, se seguirá haciendo todo de acuerdo a las rutinas, sin cambiar nada. El problema es que, al actuar de ésta forma, se está dejando que la organización vaya sin rumbo. Se estarán solucionando los problemas más apremiantes, sin tener una idea clara de hacia dónde se quiere ir.

De nada sirve la planificación, si no se tiene un control adecuado. El control permite determinar en qué etapa se encuentra el proyecto respecto del plan, e iniciar acciones correspondientes si hay una discrepancia significativa.

Por último, el trabajo se completa con un estudio de caso donde se aplicó la metodología con el fin de generar un Plan de Seguridad de la Información que cumpla con todos los requerimientos de la Política de Seguridad de la Información Modelo de la ONTI Res 01/15 , siendo ésta última de cumplimiento obligatorio por parte de los organismos del estado.

II- Metodología a aplicar:

1- P-D-C-A : Planificar- Hacer-Controlar-Actuar.

2- Gestión de Riesgos: Priorización de Controles a Implementar.

3- Diagrama Espina de Pescado (Visión gráfica de los requerimientos a implementar)

4- GANTT. (Administración del tiempo y las tareas).

Conclusiones:

- Alineamiento con Plan Estratégico TIC CNEA
- Mejora Continua
- Cumplimiento de la planificación propuesta
- Obtención de Métricas y Asignación de Recursos
- Aportes a la Comunidad a nivel Institucional.
- Trabajo Multidisciplinario entre Gerencias de CNEA.

A METHODOLOGY FOR EFFICIENT PLANNING

Nogueron,L.,Russo, A.
Gerencia TIC – División Seguridad Informática
Gerencia de Calidad-Departamento CAC
CNEA – Centro Atómico Constituyentes
Contacts: drusso@cnea.gov.ar, lnogueron@cnea.gov.ar

Objectives

To present a methodology which simplifies the planning process by consistently and coherently integrating the strategic plan, general and particular objectives, internal processes, tasks and indicators.

Introduction

Planning is, perhaps, the most important task as it conditions the execution and implementation of projects, programs, etc. Nowadays it's unacceptable to work without previous planning of objectives, goals and strategies to follow in order to achieve them. At the same time it's imperative to define the key -actors- of each stage which allows the identification of responsibilities

When there's no planning, the behavior then becomes reactive, meaning that decisions are taken as problems or necessities arise. When one is proactive, one acts only as long as there are things to resolve. Actually, if there are not unexpected events nor any pressing matters, everything continues according to the planned routines without change. The problem is that by acting this way the organization moves forward without a set goal. Compelling problems are solved without having a clear idea of what one wants to achieve.

Planning is pointless without an adequate control process. This type of process allows detecting in which stage the project stands according to the plan, and initiating of the pertinent actions if there's significant divergence.

Lastly, this work is finished with a case study where this methodology was applied with the purpose of creating an Information Security Plan that complies with all the requirements set by ONTI ‘s security policy model “Política de Seguridad de la Información Modelo” (ONTI Res. 01/15) being mandatory for all the organisms of the Argentinian State.

Methodology

1. P-D-C-A Plan-Do-Check-Act
2. Risk Management: Prioritizing of Controls to Implement
3. Cause and Effect Diagram (Visual feedback of the requirements to implement)
4. GANTT. (Time and Tasks Administration).

Conclusions

-Alignment with CNEA's TIC Strategic Plan
-Continuous Improvement
-Plan Compliance
-Gathering of Metrics and Resource Allocation
-Institutional Contribution to the Community
-Multidisciplinary work among CNEA's sectors.

DESARROLLO

El objeto de una buena planificación básicamente es eliminar el comportamiento de forma reactiva que tienen las personas que van tomando decisiones a medida que los problemas o necesidades van apareciendo y se desvían de los objetivos previamente fijados o establecidos, generando un caos en su organización.

Básicamente, la mala o nula planificación en la mayoría de los casos proviene de una mala cultura de la organización que tiende a la improvisación conduce al uso inadecuado de recursos, degrada la calidad de productos y servicios prestados, se incrementan desperdicios y finalmente se elevan los costos de las actividades realizadas.

Entre los aspectos positivos de una buena planificación se encuentra que: disminuyen problemas potenciales, el personal conoce que se espera de ellos, se genera un óptimo uso de todos los recursos de la organización y de alguna forma se predice el futuro de la organización.

.

El objetivo de este trabajo es proponer una metodología de planificación simple, basadas en herramientas ya probadas y ordenadas de forma tal que nos permita planificar nuestras actividades de forma simple y eficaz.

Se requiere de un orden de objetivos a cumplir asociados un determinado tiempo, es decir, se necesita de un plan que refleje cual será la estrategia a seguir por el sector en el mediano plazo.

Cuando es necesario tomar decisiones bajo niveles de incertidumbre, se piensa en herramientas de gestión de riesgos o tipo FODA que permitan establecer un orden de prioridades en el tiempo de objetivos a cumplir.

Esta metodología fue aplicada en la Gerencia TIC – División Seguridad Informática con el objetivo de generar normas y políticas de seguridad de la información a nivel institucional tal lo plantea el Plan Estratégico de la CNEA y se tomará como caso de ejemplo.

ETAPA 1: CICLO P-D-C-A

El economista norteamericano Edward Deming propuso una sistemática para la implementación de procesos de Calidad Total.

Cualquiera que fuese el proceso, los pasos a seguir deben ser siempre los mismos y una vez cumplidos deben volver a aplicarse para hacer sostenible y en continuo crecimiento los logros buscados.

El ciclo de Deming (fig.1), conocido también como ciclo PHVA por las iniciales de planificar, hacer, verificar y actuar, debe seguirse continuamente para generar un círculo virtuoso que nos permita como organización desarrollarnos en el mediano y largo plazo.

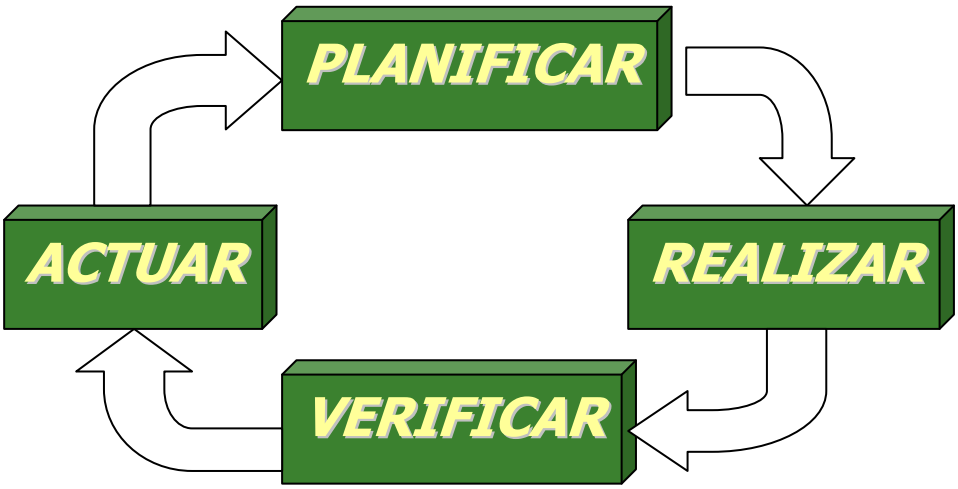


Figura 1

Otro aspecto importante de la planificación está definido por la pirámide de planificación que de alguna manera define los aspectos más importantes de la planificación en función de algunos interrogantes como ser:

¿Dónde estamos?
¿Hacia dónde vamos?
¿Hacia dónde queremos llegar?
¿Si contamos con todos los recursos?
etc.

La respuesta a los interrogantes planteados en la pirámide de planificación están dados función de su prioridad, ya que si no sabemos dónde vamos, está claro que no sabremos si llegamos

Pirámide de planificación (Figura 2)

La importancia de relacionar la planificación, con los procesos y el control (indicadores y métricas) se describen en el trabajo presentado en el año 2014 en el AATN *(Metodología para el diseño y análisis de indicadores de gestión)*

ETAPA 2: GESTIÓN DE RIESGOS

¿Qué es un Riesgos? :

- Un riesgo es un problema que todavía no llegó
- Es un problema esperando ocurrir
- Un problema es un riesgo que se manifestó
- Un problema es un riesgo al que le llegó la hora

Es parte de toda actividad y nunca puede ser eliminado por completo

¿Cómo definimos un Riesgo?

Los riesgos tratan sobre eventos posibles del futuro que se caracterizan por:

- Probabilidad de ocurrencia
- Impacto negativo si ocurren

La exposición al riesgo se mide: **Probabilidad de ocurrencia * Impacto negativo**

¿Qué es la Gestión de Riesgos?

- Involucra todas las tareas relacionadas con la identificación, la resolución y comunicación de los riesgos
- Se basa en tomar decisiones bajo niveles de incertidumbre
- No involucra decisiones futuras
- Incluye todas las decisiones presentes que tienen incidencia en el futuro

Paradigma de Gestión de Riesgos:

1 Identificación.

Se utilizan varias técnicas entre brainstorming, taxonomías, repaso de experiencia, etc. Deben documentarse.

Para enunciarlos se suele utilizar la representación de Glutch (Figura 3):

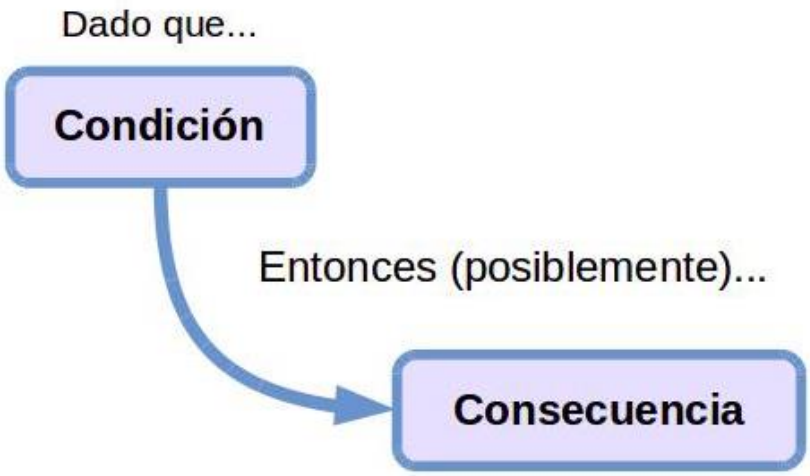


Figura 3

2 Análisis.

Convertir la información de riesgos que se identificó en información que permita tomar decisiones.

Cada riesgo debe estar lo suficientemente claro para permitir decidir acerca de él.

Esta actividad es la que les permite a la alta dirección concentrarse en los riesgos más críticos.

Para ello se debe:

- Estimar probabilidad e impacto.
- Estudiar causas y acciones correctivas.
- Identificar causas comunes.
- Identificar tiempos de ocurrencia.

3 Planificación.

La información de riesgos se transforma en decisiones y acciones.

La priorización se hace en función del grado de exposición y de la urgencia que demande la acción correctiva.

Un plan de acción puede tener la siguiente forma:

- **Evitar** el riesgo (por ejemplo, cambiando el diseño del producto final)
- Reducir la probabilidad de ocurrencia con planes de **mitigación**
- **Atacar el impacto** con planes de contingencia.
- **Aceptar el riesgo** sin tomar acciones, aceptando las consecuencias derivadas de su posible ocurrencia

4 Seguimiento.

Monitorear que las acciones que fueron definidas en el plan se ejecuten.

Aplicar las métricas sobre presupuesto, calendario y consideraciones técnicas.

Informar las desviaciones respecto de los objetivos.

Identificar nuevos riesgos permanentemente.

5 Control.

Realizar las correcciones de las desviaciones producidas sobre el proceso de riesgos.

6 Comunicación.

Proveer “feedback” sobre las actuales actividades sobre riesgos.

Para poder ser analizados y administrados, los riesgos deben ser comunicados a los niveles adecuados de la organización.

ETAPA 3: ESPINA DE PESCADO

Es una herramienta que ayuda a identificar, clasificar y poner de manifiesto posibles causas, tanto de problemas específicos como de características de calidad, funcionalidad, etc. e. Ilustra gráficamente las relaciones existentes entre un resultado dado (efectos) y los factores (causas) que influyen en ese resultado.

Con la ayuda de técnicas complementarias como la “tormenta de ideas” se pueden visualizar causas de diferentes grupos de problemas previamente establecidos.

El diagrama más usado es el denominado “5M” que define las 5 categorías o grupos de problemas previamente definidos siendo los mismos:

- Las **“maquinas”** (herramientas, aparatos, etc.)
- El **“método”** (la manera de trabajar, el modo de medir, etc.)
- Los **“materiales”** (la materia prima e insumos)
- La **“mano de obra”** (el personal calificado)
- El “**medio ambiente**” (infraestructura y procesos sustentables)

En realidad, no existe una cantidad o clasificación universal de las categorías de las causas, de manera que se debe definir en cada caso particular una solución, según lo ilustra la figura 3.

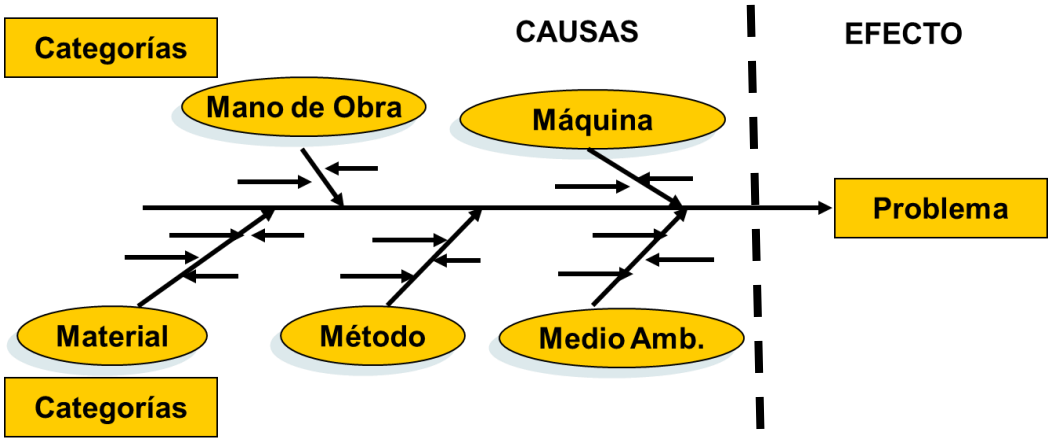


Figura 4

ETAPA 4: GRAFICA DE GANTT

La grafica de Gantt relaciona el estado en que se encuentra cada tarea/actividad a lo largo del tiempo y ello hace que se puedan ver dichas relaciones e interdependencias, resultando muy útil visualizar la relación entre tiempo y carga de trabajo

Dicho diagrama es una gráfica donde las barras que lo componen representan la longitud de una actividad o tarea que son dibujadas a escala.

El diagrama está compuesto por un eje vertical donde se establecen las actividades que constituyen el trabajo que se va a ejecutar, y un eje horizontal que muestra en un calendario la duración de cada una de ellas, como lo muestra la figura 4

La ventaja principal de la gráfica de Gantt es su simplicidad y que es muy fácil de entender y explicar y permite resolver el problema de la programación de actividades visualizando las fechas de inicio y finalización de cada tarea o actividad. Además el tamaño de la barra nos indica la longitud relativa del tiempo que llevara a terminar la tarea.

Otra ventaja importante es que permite el seguimiento de pequeños proyectos los cuales se integran a través de tareas o actividades que se realizan en forma consecutiva y ordenada e identificada los responsables de las mismas.

Su principal desventaja es que no muestra las tareas o actividades claves de un proyecto, ni sus prioridades.

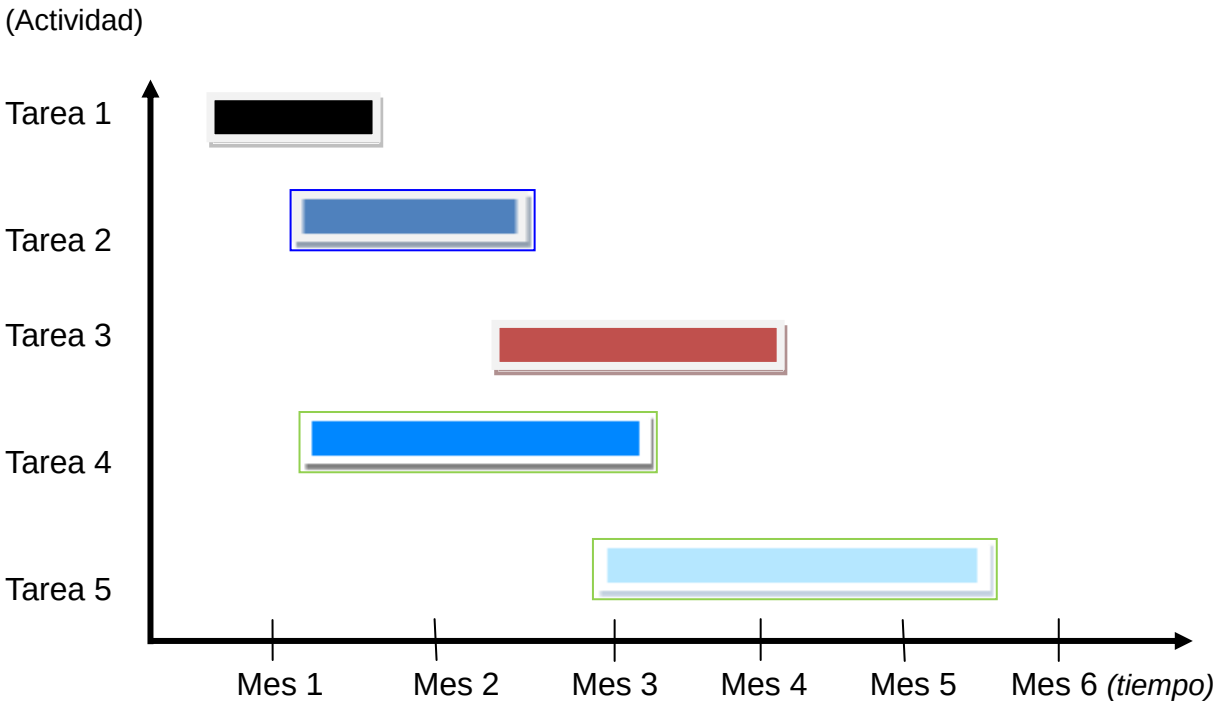


Figura 5

EJEMPLO CASO DE USO DIV SEGURIDAD INFORMATICA:

Para cumplir el Plan Estratégico y sus objetivos generales y particulares relativos a la Gerencia TIC, la División Seguridad Informática implementó esta metodología para crear un Plan de Seguridad de la Información. Dicho plan abarca todas las etapas que son propuestas por dicha metodología y permitió ordenar la generación de documentos, sus responsables, yel tiempo estipulado de generación y aprobación.

i. Gestión de Riesgos.

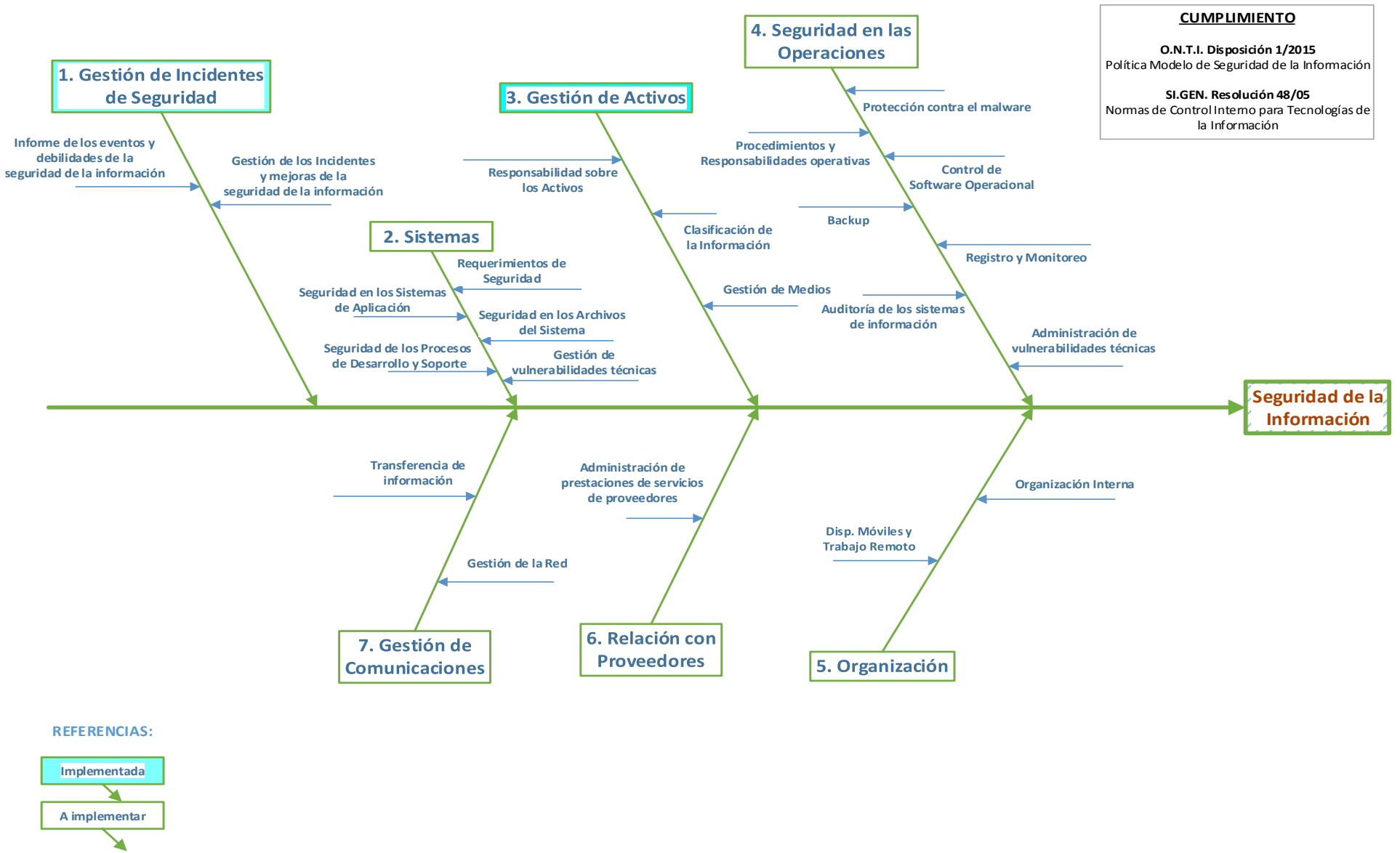
En base a la necesidad del cumplimento de las clausulas establecidas en la Disposición 1/2015 “Política Modelo de Seguridad de la Información” O.N.T.I. (resolución de cumplimiento obligatorio por todas las dependencias del Estado), se estableció, de acuerdo a un criterio de gestión de riesgos, un orden de criticidad (prioridad) reflejado en la siguiente tabla:

ID	Nombre	Riesgo Representativo	Probalidad	Impacto	Ocurrenci	Prioridad	Plan Estratégico
1	Gestion de Incidentes	Sistemas críticos comprometidos a través de la web institucional ya comprometida	80	ALTO	9	Prioridad 1	Procesos propio de la Gerencia TIC
2	Sistemas	Dado que no existen controles de los aplicativos publicados en internet pueden ser objeto de abusos	80	MEDIO	7	Prioridad 3	Desarrollo de Politicas, Normativos y Procedimientos
3	Gestion de Activos	Dado que no se elimina la información de manera segura antes de dar la baja definitiva de los medios de almacenamiento digital da una imagen institucional negativa	80	ALTO	8	Prioridad 2	Desarrollo de Politicas, Normativos y Procedimientos
4	Seguridad en las Operaciones	Dado que no se cuenta un sistema de registros (logs) centralizado de las transacciones de los sistemas criticos entonces no es posible investigar en forma eficiente e independiente los incidentes de SI	70	ALTO	8	Prioridad 4	Procesos propio de la Gerencia TIC
5	Organización	Dado que los usuarios de dispositivos moviles no cuentan con capacitación en seguridad informática, se dan muchos problemas de infeccion con malware	80	ALTO	3	Prioridad 7	Programa de concientización y capacitaciones
6	Relación con proveedores	Dado que no existen politicas/normativas especificas de contratacion de Desarrollo de Software por parte de terceros, dichos sistemas sufren continuamente de problemas de seguridad	80	ALTO	5	Prioridad 6	Desarrollo de Politicas, Normativos y Procedimientos
7	Gestion de Comunicaciones	Dado que no existen normativas sobre como debe realizarse el cableado estructurado de red , entonces los nuevos tendidos del mismo sufrirán interrupciones de servicios en caso de contingencias (ej. inundaciones)	80	ALTO	4	Prioridad 5	Desarrollo de Politicas, Normativos y Procedimientos
CALCULO RIESGO (PRIORIDAD) =		PROBABILIDAD (0-100) x IMPACTO (ALTO=3,MEDIO=2,BAJO=1) x #OCURRENCIAS (de 1 hasta 3 = 1 ;de 4 hasta 8= 2 ; mas de 8 = 3)					
	MINIMO = 1x1x0 = 0						
	MAXIMO = 3x3x100 = 900						

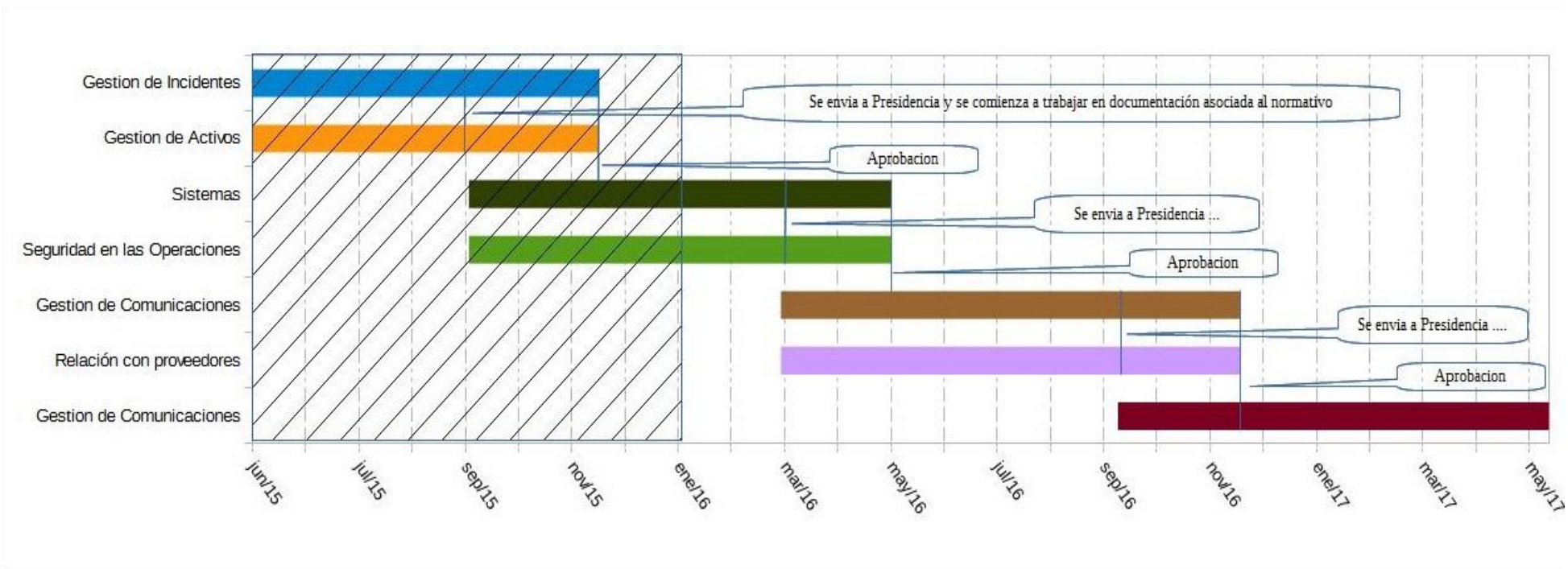
ii. Diagrama Espina de Pescado.

Mediante ésta herramienta se ilustra gráficamente las relaciones existentes entre las clausulas anteriormente seleccionadas a implementar de la Res. 1/2015 ONTI (i – Gestión de Riesgos) y el resultado esperado que es la seguridad de la información.

En el gráfico también se indica las clausulas ya implementadas en el corriente año “1- Gestión de Incidentes de Seguridad” y “3 – Gestión de Activos”.


CUMPLIMIENTO
O.N.T.I. Disposición 1/2015
Política Modelo de Seguridad de la Información
SI.GEN. Resolución 48/05
Normas de Control Interno para Tecnologías de la Información
1. Gestión de Incidentes de Seguridad
Informe de los eventos y debilidades de la seguridad de la información
Gestión de los Incidentes y mejoras de la seguridad de la información
2. Sistemas
Requerimientos de Seguridad
Seguridad en los Sistemas de Aplicación
Seguridad en los Archivos del Sistema
Seguridad de los Procesos de Desarrollo y Soporte
Gestión de vulnerabilidades técnicas
3. Gestión de Activos
Responsabilidad sobre los Activos
Clasificación de la Información
4. Seguridad en las Operaciones
Protección contra el malware
Procedimientos y Responsabilidades operativas
Control de Software Operacional
Backup
Registro y Monitoreo
Gestión de Medios
Auditoría de los sistemas de información
Administración de vulnerabilidades técnicas
Seguridad de la Información
Transferencia de información
Gestión de la Red
7. Gestión de Comunicaciones
Administración de prestaciones de servicios de proveedores
6. Relación con Proveedores
Organización Interna
Disp. Móviles y Trabajo Remoto
5. Organización
REFERENCIAS:
Implementada
A implementar

iii. GANTT



Inicio	días	Fin
1/06/15	195	12/12/15
1/06/15	195	12/12/15
1/10/15	238	25/05/16
1/10/15	238	25/05/16
25/03/16	259	8/12/16
25/03/16	259	8/12/16
1/10/16	244	1/06/17

En el diagrama de GANTT se identifican las clausulas ya aprobadas (sector sombreado) que permitieron estimar el tiempo de aprobación de las nuevas clausulas planificadas. También se indica en el tiempo las tareas/actividades a implementar como ser el desarrollo de documentación asociada (procedimientos operativos, formularios, etc.) al documento normativo a la espera de la aprobación.

iv. Métricas e Indicadores

Objetivo General 2: Elaborar e implementar un plan integral de las TIC´s en CNEA, aplicando las normativas específicas establecidas para la Administración Pública Nacional	
Objetivo Específico 2.4:	Fijar las normativas y los procedimientos

Nombre:	Capacidades para la gestión de los incidentes de seguridad de la información	**Código:**	
Responsable:	**Lucas Noguerón**		
Subresponsable:	Pablo Milmanda		
Objetivo asociado:	O. Esp. 2.4	**Tiempo de medición:**	Anual
Formula del Indicador	Cantidad de documentos generados * ——————————— Cantidad de documentos proyectados		
Línea de Base	6		
Valor Objetivo	8		
Fuente del dato	Resolución Presidencial.	**Responsable de Fuente de dato**	Lucas Nogueron.

Conclusiones:

- ***Alineamiento con Plan Estratégico TIC CNEA***

La estrategia de mitigación (tratamiento de los riesgos) debe ser coherente con los objetivos estratégicos de las áreas afectadas.

- ***Mejora Continua***

Asegura que los procesos implementados no se comporten como un sistema estanco en el tiempo, si no que a través del mismo evolucionen, para ser sostenibles y en permanente crecimiento alcanzando los objetivos establecidos.

- Cumplimiento de la planificación propuesta

Las clausulas “Gestion de Incidentes de Seguridad” y “Gestión de Activos” de la Disposición 1/2015 ONTI cumplidas satisfactoriamente dentro del período establecido previamente en el GANTT (en celeste)

- ***Obtención de Métricas y Asignación de Recursos***

Se establece una herramienta para la futura obtención de métricas en función de los procesos planificados.

- Aportes a la Comunidad a nivel Institucional.

Se establece una metodología para cumplir con la Disposición 01/2015 ONTI que establece que todos los Organismos del Estado deben generar sus propias Políticas de Seguridad de la Información y que a su vez puede ser reproducida por otros organismos con características similares.

- Trabajo Multidisciplinario entre Gerencias de CNEA.

Esta metodología se desarrolló en conjunto la Gerencia de Gestión de la Calidad y la Gerencia Tecnología de la Información y de las Comunicaciones.

Bibliografía:

Lazarsfeld, P. (1966), "De los conceptos a los índices empíricos", en Boudon y Lazarsfeld, Metodología de las Ciencias Sociales, Vol. I y II, Barcelona, Ed. Laia.

José Tana. (2014) “Manual de Sistemas de Gestión” Segunda Edicion, C.A.B.A, Ed. CEIT.

Norma ISO 9000:2005“Sistemas de gestión de la calidad – Fundamentos y vocabulario”