Proceso de Administración de Seguridad

1.Contenido

1. CONTENIDO 2
2. HISTORIAL DE VERSIONES 3
3. INTRODUCCIÓN 4
4. OBJETIVO DEL PROCESO 6
5. ALCANCE 7
6. REFERENCIAS 8
7. RESPONSABILIDADES 9
8. DEFINICIONES 10
9. INSUMOS 12
10. RESULTADOS 13
11. INTERACCIÓN CON OTROS PROCESOS 14
12. POLÍTICAS 15
13. DIAGRAMA 16
14. MEDICIÓN 28

2. Historial de versiones

Fecha	Versión	Descripción
03/02/2013	1.0 Draft	Creación de la primer versión del documento, siendo draft, ya que no está revisada por Directores y Jefes de Departamento
08/10/2013	2.0 Draft	Correcciones con base en revisión del Área de Calidad.
08/10/2013	1.0	Versión 1.0 para la DGSEI

3. Introducción

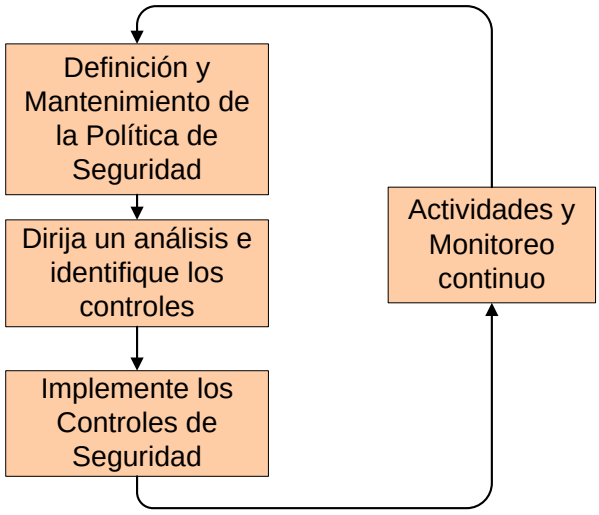
Administración de la Seguridad de la Información (ISM) es el proceso de manejar un nivel definido de seguridad, incluyendo manejar la reacción a las violaciones e incidentes de seguridad cuando ocurren. El proceso ISM en sí mismo necesita considerarse dentro del marco de trabajo global del gobierno corporativo de la organización y como tal deberá ser gobernado por una política de seguridad corporativa que documente la decisión de la organización de gastar tiempo y dinero en la seguridad de la información y servicios, y proporcione Administración con indicaciones y lineamientos. ISM deberá asegurarse que la Política de Seguridad se revisa y se actualiza regularmente para asegurar que refleje las necesidades del negocio. La estructura organizacional en términos de roles y responsabilidades de seguridad deberá también establecerse y mantenerse.

ISM se refiere acerca de proteger los activos clave de la organización. Para hacer esto se tienen que identificar esos activos. Una vez que los activos han sido identificados, se debe conducir un análisis para obtener un entendimiento de la importancia de cada activo y los impactos potenciales de negocio a través de la pérdida de confidencialidad, integridad o disponibilidad del activo. El resultado de este análisis permite clasificar los activos con una codificación adecuada de seguridad. Se debe conducir un Análisis de Riesgo para identificar las amenazas potenciales para cada activo, todo control actual que esté colocado para salvaguardar el activo y los niveles de riesgo que existen. Usando esta información y tomando en cuenta las clasificaciones de activo, se deberá producir un Plan de Seguridad. Este plan detalla los controles que justifican su costo y que se requieren para proteger los activos, y deberán ser acordados con la Gestor senior.

Administración de la Seguridad de la Información entonces maneja y coordina la implementación y prueba de controles de seguridad y el desarrollo de procedimientos para su operación y mantenimiento. Esto incluye el desarrollo de procedimientos, en conjunción con Administración de Incidente, para el manejo de incidentes de seguridad. Una vez que los controles se han implementado ISM cubre las actividades continuas requeridas para mantener la estructura de control de seguridad. Esto incluye actividades tales como evaluar RFCs por impacto potencial, coordinar pruebas regulares, promocionar conciencia de seguridad, entrenar a practicantes, manejar incidentes de seguridad y asegurar la eficiencia y efectividad del proceso.

El presente documento tiene como objetivo presentar el diseño del proceso de Administración de Seguridad de la DGSEI, el cual está alineado a las mejores prácticas de ISO 20000-1:2011.

El siguiente diagrama ilustra las macro actividades del proceso de Administración de Seguridad de la DGSEI:



Estructura de Seguridad

Esta estructura usualmente consiste en lo siguiente:

- Una Política de Seguridad de la Información (ISP)
- Un Sistema de Gestión de la Seguridad de la Información (ISMS)

- Una estrategia de seguridad que está vinculada y soporta los objetivos, estrategias y planes del negocio.
- Una estructura efectiva de seguridad organizacional
- La Gestión continua de riesgos de seguridad

Política de Seguridad de la Información (ISP)

Ésta deberá ser la fuerza impulsora detrás de todas las actividades de seguridad, la que deberá ser soportada cuando sea necesario por un sub conjunto de políticas de seguridad. El ISP deberá tener el soporte de Gestor Senior de ambos negocio y TI, y deberá incluir lo siguiente (entre otros):

- Uso y mal uso de la política de activos TI
- Políticas sobre controles de acceso y password
- Políticas sobre email, internet y virus
- Política de acceso remoto
- Etc.

Todas las políticas deberán estar ampliamente disponibles a todas esas personas que les afecten, incluyendo clientes, usuarios y terceros. Cuando sea relevante, los requerimientos para adherir a las políticas adecuadas deberán incluirse en acuerdos tales como SLAs, SLRs, y contratos de terceros. Una vez desarrollados y firmados por Gestión, necesitarán revisarse cuando sea necesario – normalmente con base anual como mínimo.

Sistema de Gestión de Seguridad de la Información (ISMS)

El ISMS representa la estructura generada para designar e implementar los procesos y controles de seguridad requeridos, junto con la Gestión continua, mantenimiento y reforzamiento de esos procesos y controles.

El ISMS tiene cinco elementos clave que son:

- **Control** – ej. Tal como establecer la estructura de Gestión y establecer una estructura de organización que soporte la operación de Gestión de Seguridad de la Información
- **Plan** – ej. Recabar requerimientos de todas las partes interesadas (tales como el negocio y la Gestión de Nivel de Servicio) y luego idear y recomendar las medidas de seguridad más adecuadas que se deberán poner en el lugar
- **Implementar** – ej. Generar las herramientas y controles que sustentan el ISP
- **Evaluación** – ej. Revisar la conformidad contra el ISP y ejecutar auditorías regulares de los sistemas técnicos de seguridad de TI
- **Mantener** – ej. Utilizando el ciclo Planear-Hacer-Verificar-Actuar para mejorar continuamente según acuerdos de seguridad detallados en SLAs (por ejemplo), así como mejorar la implementación de los controles y medidas de seguridad existentes
- **Gobierno de Seguridad** – ej. Revisar áreas clave tales como alineación estratégica, valor de entrega y Gestión de riesgo.

4. Objetivo del proceso

Alinear seguridad TI con seguridad de negocio y asegurar de que esa información de seguridad es manejada efectivamente en todos los servicios y actividades de Administración de Servicio.

Los objetivos específicos del proceso de Administración de Seguridad de la DGSEI son:

- Ganar una comprensión de las políticas y planes de seguridad de negocio
- Tener una conciencia de la operación de negocio existente y sus requerimientos de seguridad
- En coordinación con SLM entender los requerimientos de seguridad que están detallados dentro de los Acuerdos de Nivel de Servicio (SLAs)
- Entender riesgos de negocio y TI y lo que se está haciendo para manejar estos riesgos (como revisar el Registro de Riesgos y mantener una conciencia de cualquier actualización)

5. Alcance

El proceso de Administración de Seguridad, aplica a todo el personal involucrado en la generación de información, así como las áreas responsables de la administración de la misma de la Dirección General del Sistema Estatal de Informática.

Para la implementación del proceso de Administración de Seguridad, el alcance inicial para la habilitación serán los servicios:

- Trámites y servicios
- Sitios web
- Conectividad voz, datos e internet
- Plataforma tecnológica

6. Referencias

La información utilizada para este documento proviene de las siguientes fuentes de información:

- Libros de ITIL® v3, en específico Diseño del Servicio (Service Design)
- Norma ISO/IEC 20000-1:2011
- Información proporcionada por la UDPCC

7. Responsabilidades

El **Administrador de Seguridad** deberá

- Desarrollar y mantener la Política general de Seguridad así como todas aquellas políticas que formen parte del proceso.
- Evaluar a los Seguridad
- Desarrollar y documentar procedimientos para operar y mantener controles de Seguridad, de monitoreo, para incumplimientos de Seguridad y manejo de incidentes de Seguridad.
- Promocionar educación y conciencia de la Seguridad.
- Efectuar regularmente auditorías a los controles de Seguridad y sus procedimientos.
- Evaluar los requerimientos de control de cambio en cuanto a aspectos de Seguridad.
- Asistir a las reuniones del Comité de Control de Cambios cuando sea apropiado.
- Participar en toda revisión de la Seguridad que surja de un incumplimiento de la Seguridad.
- Desarrollar, establecer y mantener políticas y procedimientos para promover la Seguridad y el funcionamiento ininterrumpido de los sistemas de aplicaciones basadas en la informática.

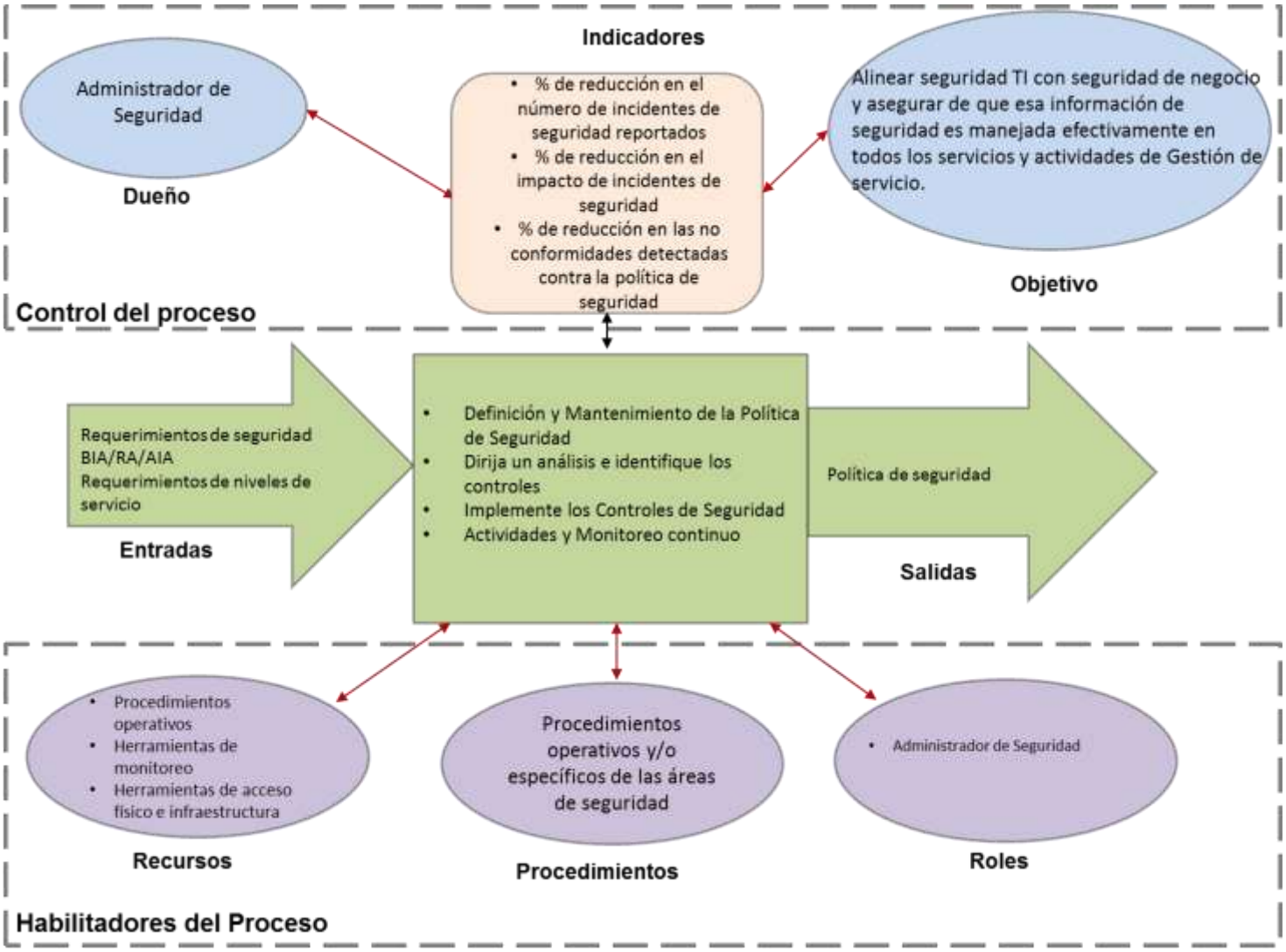
Las responsabilidades del **Administrador de Incidentes**, quien participa en el proceso de Administración de Seguridad de la Información, son descritas en el documento del proceso de Administración de Incidentes.

El rol **Todos los procesos** se refiere que a cualquier rol dentro de la Administración de Servicios de ISO 20000 de la DGEI puede participar en realizar el requerimiento de seguridad, o bien, dar aviso de las violaciones de seguridad que se pueden dar en la organización.

8. Definiciones

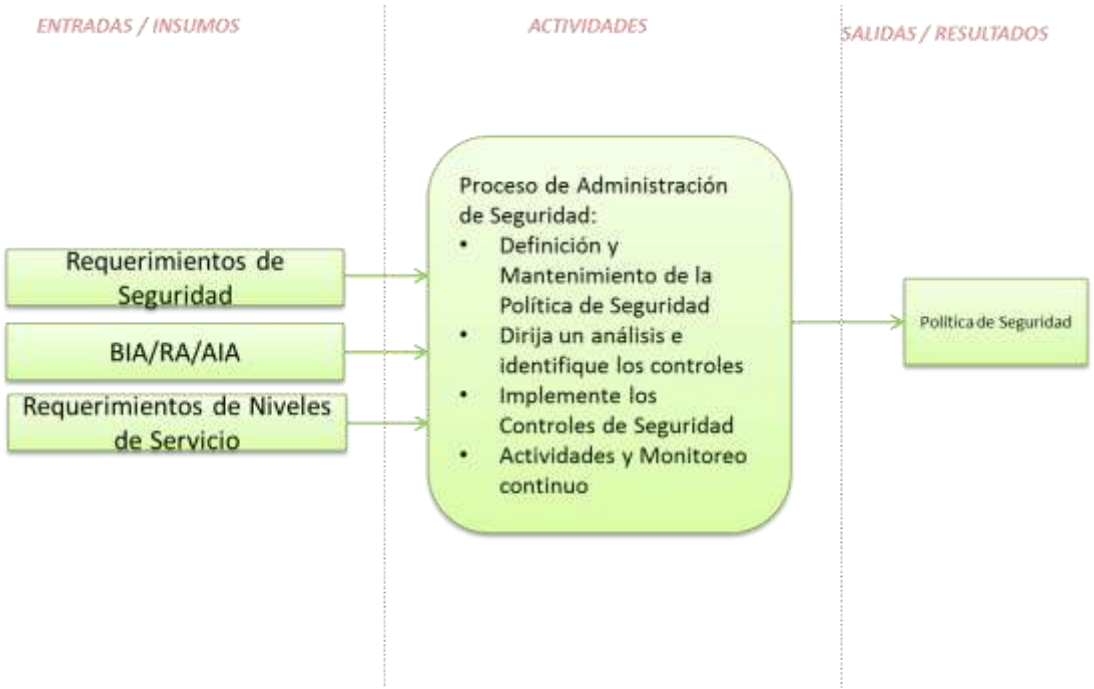
- **Análisis de Riesgos:** Los pasos iniciales de la administración de riesgos: analizar el valor de los activos del negocio, identificando amenazas a esos activos y evaluando la vulnerabilidad de las amenazas identificadas para cada activo. La evaluación del riesgo puede ser cuantitativo (basado en información numérica) o cualitativa.
- **BIA:** actividad de la gestión de la continuidad del negocio que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, otros procesos de negocio, servicios TI, etc. BIA define los requerimientos de recuperación para los servicios de TI. Dichos requerimientos incluyen objetivos de tiempos de recuperación, objetivos del punto de recuperación y los objetivos mínimos de nivel de servicio para cada servicio de TI.
- **ISM:** Por sus siglas en inglés Information Security Management (Administración de Seguridad de la Información). Proceso que asegura Confidencialidad, Integridad y Disponibilidad de los Activos de una Organización, de la información, de los datos y de los Servicios de TI. La Gestión de la seguridad de la información usualmente forma parte de un abordaje Organizacional de la Gestión de la seguridad que tiene un alcance mayor que el del Proveedor de Servicios de TI, y comprende la manipulación de los papeles, el acceso al edificio, las llamadas telefónicas, etc., en toda la Organización.
- **ISMS:** Por sus siglas en inglés Information Security Management System (Sistema de Administración de Seguridad de la Información). El marco de las Políticas, los Procesos, las Normas, Directrices y herramientas que garantizan que una Organización pueda alcanzar sus Objetivos de Gestión de la seguridad de la información.
- **ISP:** Por sus siglas en inglés Information Security Policy (Política de Seguridad de la Información). Política que rige la concepción de la Organización sobre la Gestión de la Seguridad de la Información.
- **RFC:** Por sus siglas en inglés Request For Change (Solicitud de Cambio). Propuesta formal para que se realice un Cambio. Un RFC incluye detalles del Cambio propuesto, y puede ser registrada en papel o en soporte electrónico.
- **SACM:** Por sus siglas en inglés Service Asset and Configuration Management (Administración de Activos del Servicio y Configuración). Proceso responsable por la Administración de la Configuración y la Administración de Activos.
- **SLA:** Por sus siglas en inglés Service Level Agreement (Acuerdo de Nivel de Servicio). Acuerdo entre un Proveedor de Servicios de TI y un Cliente. El SLA describe el Servicio de TI, documenta las Metas de Niveles de Servicio y especifica las responsabilidades del Proveedor de Servicios de TI y del Cliente. Un único SLA puede cubrir varios Servicios de TI o múltiples Clientes.
- **SLM:** Por sus siglas en inglés Service Level Management (Administración de Niveles de Servicio). Proceso encargado de la negociación de las Metas de Niveles de Servicio y de asegurar que se cumplan estas. La SLM es responsable de asegurar que todos los Procesos de Administración del Servicio de TI, los Acuerdos de Nivel Operacional, y los Contratos de Apoyo, sean correctos para las Metas de Niveles de Servicio acordadas. La SLM monitoriza e informa sobre los Niveles de Servicio, y mantiene revisiones regulares con los Clientes.
- **SLR:** Por sus siglas en inglés Service Level Requerimient (Requerimiento de Nivel de Servicio). Requisito del cliente para un aspecto de un Servicio de TI. Las SLRs se basan en Objetivos del Negocio y se usan para negociar Metas de Niveles de Servicios acordadas.

9. Diagrama de tortuga



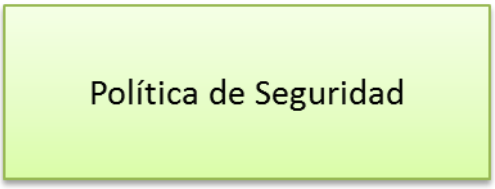
10.Insumos

La siguiente imagen muestra el resumen del proceso de Administración de Seguridad, definiendo con detalle las entradas y salidas del mismo.



11.Resultados

Las salidas o resultados del proceso de Administración de Seguridad de la DGSEI son las siguientes:



12.Interacción con otros procesos

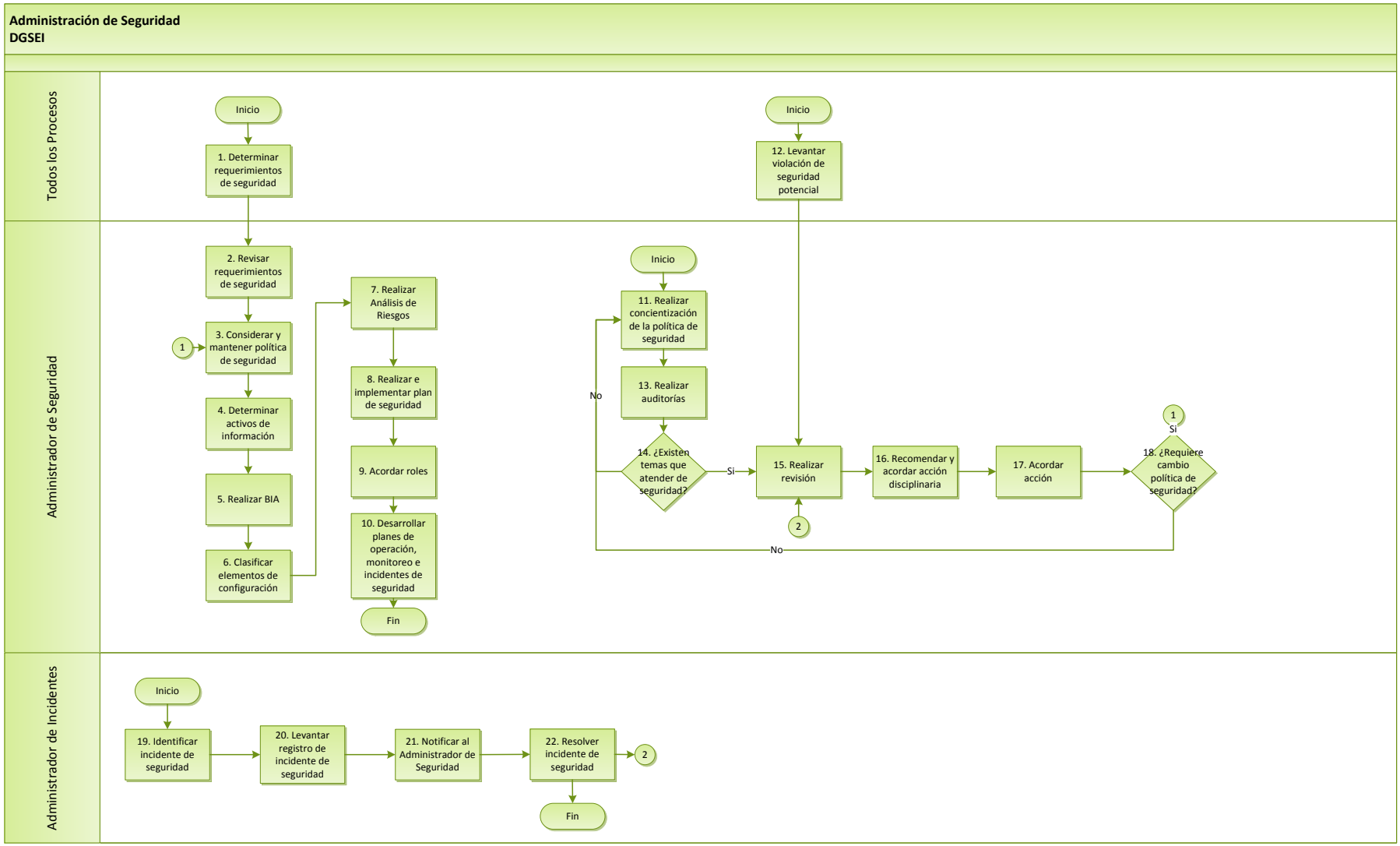
El siguiente diagrama muestra las principales relaciones del proceso de Administración de Seguridad con otros procesos de la Administración de Servicios ISO 20000.

13.Políticas

Las políticas se definen para normar al proceso de la Administración de Seguridad. Éstas están basadas en las necesidades de la organización y las mejores prácticas, quedando a validación y mejora permanente por parte del dueño y administrador del proceso.

- El proceso de Administración de Seguridad de la Información se audita, en términos de calidad, al menos cada seis meses.
- El único responsable de realizar cambios al proceso de Administración de Seguridad de la Información es el Administrador de la Seguridad de la Información.
- La política de seguridad es confidencial y propiedad de la DGSEI.
- La política de seguridad deberá publicarse cada seis meses, revisándola cada tres meses.
- La política de seguridad deberá comunicarse a todo el personal de la DGSEI a través de campañas de concientización.

14.Diagrama


Administración de Seguridad
DGSEI
Todos los Procesos
Administrador de Seguridad
Administrador de Incidentes
Inicio
1. Determinar requerimientos de seguridad
2. Revisar requerimientos de seguridad
3. Considerar y mantener política de seguridad
4. Determinar activos de información
5. Realizar BIA
6. Clasificar elementos de configuración
7. Realizar Análisis de Riesgos
8. Realizar e implementar plan de seguridad
9. Acordar roles
10. Desarrollar planes de operación, monitoreo e incidentes de seguridad
Fin
1
Inicio
12. Levantar violación de seguridad potencial
Inicio
11. Realizar concientización de la política de seguridad
13. Realizar auditorías
14. ¿Existen temas que atender de seguridad?
No
Si
15. Realizar revisión
2
16. Recomendar y acordar acción disciplinaria
17. Acordar acción
1
Si
18. ¿Requiere cambio política de seguridad?
No
Inicio
19. Identificar incidente de seguridad
20. Levantar registro de incidente de seguridad
21. Notificar al Administrador de Seguridad
22. Resolver incidente de seguridad
2
Fin

15.Método de trabajo

No.	Actividad	Descripción	Entrada	Salida	Responsable
1	Determinar requerimientos de seguridad	Los requerimientos de Seguridad pueden ser por una variedad de razones tales como: el desarrollo de servicios nuevos, cambios a la legislación externa, la aparición de nuevas amenazas a las que se enfrentan nuevos clientes o proveedores nuevos, cambios a acuerdos existentes tales como SLAs, etc. Cualquier proceso debe identificar un nuevo requerimiento, pero se debe pasar este requerimiento a Administración de Seguridad de la Información. Habrá interfases clave aquí con Administración de Niveles de Servicio y Administración de Proveedores, pero también con representantes del negocio. Uno de los documentos clave que determinará requerimientos nuevos o revisados será la Política de Seguridad del Negocio y es vital que el Administrador de Seguridad de la Información permanezca al pendiente de los contenidos de ésta y toda revisión que se proponga o implemente. Continuar en la actividad número 2	Requerimiento de seguridad	• Requerimiento de seguridad	• Todos los procesos
2	Revisar requerimientos de seguridad	Revisar los requerimientos de seguridad identificados en la actividad anterior. Al identificarse nuevos requerimientos de Seguridad, Administración de Seguridad de la Información de TI es responsable de levantarlos y de analizarlos para verificar cómo atenderlos y su impacto en la Política	• Requerimiento de seguridad	• Requerimiento de seguridad revisado	• Administrador de Seguridad

		de Seguridad. Continuar en la actividad número 3.			
3	Considerar y mantener la política de seguridad	La Política de Información de Seguridad debe reflejar las necesidades de la DGSEI y las amenazas a las que están sujetos. La política deberá ser revisada regularmente a la luz de nuevos o cambios de requerimientos, o cualquier asunto nuevo de Seguridad que surja, para asegurar que todavía cubre todos los temas necesarios y continúa cubriendo las necesidades de la organización. Cuando sea necesario, la Política deberá actualizarse y reeditarse para asegurar que permanece vigente. Continuar en la actividad número 4.	• Política de seguridad • Requerimiento de seguridad	• Política de seguridad actualizada	• Administrador de Seguridad
4	Determinar activos de información	Para proteger los activos TI de la organización que sean clave para la entrega de los servicios, es necesario primero identificar cuáles son. Los activos de TI que Administración de Seguridad de la Información de TI toma en cuenta, no son necesariamente los mismos Elementos de Configuración que se tienen registrados en la CMDB (Administración de Configuraciones), ya que pueden existir elementos de carácter confidencial que por necesidades de la DGSEI, no podrán registrarse en dicho repositorio. Continuar en la actividad número 5	• Elementos de configuración • Información que se genera	• Lista de activos	• Administrador de Seguridad
5	Realizar BIA	Una vez que estos activos han sido identificados, es necesario entender su importancia y el impacto potencial que su pérdida o corrupción tienen para la DGSEI.	• Cuestionarios de BIA	• BIA	• Administrador de Seguridad

		Esta información deberá recabarse con un enfoque hacia el Negocio como parte de un ejercicio de Análisis de Impacto al Negocio. Continuar en la actividad número 6.			
6	Clasificar elementos de configuración	Cuando la importancia de los activos identificados ha sido comprendida, se deberá asignar a cada activo una clave de clasificación de Seguridad, para indicar al personal, el nivel de Seguridad con que ese activo deberá tratarse. La clasificación ayudará a justificar el costo de medidas de seguridad para proteger dicho activo. Los registros de Elementos de Configuración (CI) deben estar actualizados para reflejar la clasificación de Seguridad, cuando éstos se encuentren registrados dentro de la CMDB. Continuar en la actividad número 7.	• Lista de elementos de configuración	• Clasificación de elementos de configuración	• Administrador de Seguridad
7	Realizar análisis de riesgos	Se debe conducir un Análisis de Riesgo de Seguridad para identificar las amenazas, vulnerabilidades y riesgos asociados a cada activo. Las amenazas deberán incluir seguridad física, seguridad lógica y seguridad de respaldos de datos. Las amenazas de ambas fuentes interna y externa deberán incluirse. Se deberá considerar la posibilidad e impacto potencial de cada riesgo. Los resultados del Análisis de Riesgo deben documentarse y, donde sea posible, se debe recomendar cualquier control de Seguridad relevante. Continuar en la actividad número 8.	• Reportes de revisiones de controles	• RA	• Administrador de Seguridad
8	Realizar e	Donde se identifiquen riesgos,	• Política de	• Política de	• Administrador de

	implementar plan de seguridad	Administración de Seguridad de la Información debe considerar posibles controles que se podrían implementar. Todo control de Seguridad deberá justificar su costo contra impactos potenciales identificados durante el Análisis de Impacto al Negocio. Los controles de Seguridad identificados deberán formar parte de un Plan de Seguridad. El Plan de Seguridad deberá contener dos secciones principales: 1. Controles a implementar en función del análisis de riesgos y las necesidades del negocio 2. Las mejoras al proceso o herramientas relacionadas a seguridad, que deberán implementarse como parte de un plan anual de mejora. Los controles de Seguridad nuevos o modificados identificados dentro del Plan de Seguridad necesitan implementarse y probarse para asegurar su efectividad. Administración de Seguridad de la Información de TI es responsable de implementarlos de acuerdo con el proceso de Administración de Cambios. Continuar en la actividad número 9.	seguridad	seguridad implementada	Seguridad
9	Acordar roles	Determinar los roles que están involucrados en otros procesos que deberán apoyar al proceso de Administración de Seguridad Continuar en la actividad número 10.	• Organigrama SEI	• Roles acordados	• Administrador de Seguridad
10	Desarrollar planes de operación, monitoreo e	Los procedimientos deben desarrollarse y documentarse a fin de cubrir tareas operacionales que deben completarse	• Experiencia de especialistas técnicos	• Procedimientos operativos, monitoreo e	• Administrador de Seguridad

incidentes de seguridad	regularmente (tal como limpiar los “log files” y hacer respaldos) y tareas de mantenimiento (tales como aplicar parches, hacer cambios de configuración y actualizar software). Muchos controles de Seguridad requieren de algún mecanismo de monitoreo. Esto incluye monitoreo con herramientas de seguridad como sistemas de Detección de Intrusos y Registros de Firewall, como también monitorear las herramientas mismas para asegurar que están corriendo y funcionando como se requiere. Los procedimientos deben desarrollarse y documentarse cubriendo cómo y cuándo se llevará a cabo este monitoreo, y quién deberá ser alertado si surgen asuntos. Administración de Seguridad de la Información de TI deberá trabajar en conjunción con Administración de Incidentes para identificar y documentar procedimientos para responder a varios tipos de Incidentes de Seguridad. Los procedimientos variarán por los diferentes tipos de Incidentes; por ejemplo, la respuesta a un brote de virus puede involucrar diferentes medidas al de una sospecha de ataque de ‘Negación de Servicio’ en la página web corporativa. Es importante que los procedimientos para el manejo de Incidentes de Seguridad consideren preservar toda evidencia posible incluyendo el Incidente. Se podrá necesitar que se mantenga rastro para la auditoría de los eventos y acciones con el	• Manuales técnicos	incidentes de seguridad

		fin de ayudar a cualquier juicio en el futuro. Continuar en la actividad número 11.			
11	Realizar concientización de la política de seguridad	Deberá haber un programa continuo de entrenamiento en Seguridad para todo el personal. Este entrenamiento cubrirá la Política de Seguridad, sus responsabilidades con respecto a Seguridad, asuntos clave de Seguridad y cómo reportar violaciones potenciales o reales de Seguridad. Para principiantes en la organización, este entrenamiento deberá formar parte de su proceso de inducción. El entrenamiento deberá complementarse con un programa de conciencia de Seguridad con la intención de recordar los asuntos clave al personal, y promocionar una cultura de Seguridad. Continuar en la actividad número 13.	• Política de seguridad	• Concientización	• Administrador de Seguridad
12	Levantar violación de seguridad potencial	Es responsabilidad de todos los miembros de la DGSEI y dueños de procesos, reportar debilidades potenciales de seguridad al Administrador de Seguridad de la Información tan pronto como se detecten. Durante la operación diaria de cualquier proceso se puede reconocer que existen fallas potenciales en los procedimientos de seguridad o que se pasen por alto. Esto debe informarse a Administración de Seguridad de la Información tan pronto como sea posible. Continuar en la actividad número 15.	• Violación de seguridad	• Violación de seguridad	• Todos los procesos
13	Realizar auditorías	Deberá existir un programa continuo de auditoría y revisión de actividades dirigido a	• Política de seguridad	• Auditoría	• Administrador de Seguridad

		asegurar que los controles estén trabajando efectivamente y que los procedimientos de Seguridad se siguen. El programa deberá involucrar ambas, auditoría interna y auditoría independiente, produciendo reportes y, donde sea adecuado, haciendo recomendaciones para mejorar. Las auditorías y revisiones también deberán cubrir a terceros, especialmente cuando ellos tienen acceso a la infraestructura de la organización de TI. Continuar en la actividad número 14.			
14	¿Existen temas que atender de seguridad?	Como resultado de las auditorías se determina si existen problemáticas en la seguridad. En caso de que si existan problemas de seguridad, ir a la actividad número 15, en caso contrario ir a la actividad número 11.	• Resultado de auditoría	• Si o No	• Administrador de Seguridad
15	Realizar revisión	Todo asunto de seguridad, actual o potencial, identificado deberá registrarse, investigarse, revisarse para entender la naturaleza, causa y amenaza potencial que representan los asuntos. Cuánto más significativo el Incidente o asunto, más profunda deberá ser la investigación y revisión. Las estadísticas deberán guardarse respecto al número de Incidentes de Seguridad de varios tipos que se hayan detectado. Continuar en la actividad número 16.	• Política de seguridad • Reportes de auditorías	• Revisión de temas de seguridad	• Administrador de Seguridad
16	Recomendar y acordar acción disciplinaria	Las acciones que apoyen a resolver la problemática de seguridad deberán ser acordadas con el Director General del SEI, así como la Delegación Administrativa	• Política de seguridad • Reportes de auditorías	• Acción disciplinaria	• Administrador de Seguridad

		Continuar en la actividad número 17.	• Revisión de temas de seguridad		
17	Acordar acción	Acordar las acciones propuestas y revisadas con la Dirección General del SEI y Delegación Administrativa Continuar en la actividad número 14.	• Acción disciplinaria	• Acción disciplinaria acordada	• Administrador de Seguridad
18	¿Requiere cambio política de seguridad?	Determinar si la política de Seguridad requiere cambios. En caso de que si requiera cambios, ir a la actividad número 3; en caso contrario, ir a la actividad número 11.	• Política de seguridad • Acción disciplinaria	• Si o no	• Administrador de Seguridad
19	Identificar incidente de seguridad	Administración de Incidentes es responsable de detectar y reaccionar ante Incidentes de Seguridad siguiendo el proceso normal de Administración de Incidentes y todo procedimiento específico adicional de Seguridad que haya sido acordado con Administración de Seguridad de la Información. Continuar en la actividad número 20.	• Incidente de seguridad	• Incidente de seguridad identificado	• Administrador de incidentes
20	Levantar registro de seguridad	Todo Incidente de Seguridad deberá registrarse siguiendo el procedimiento normal de Administración de Incidentes. Continuar en la actividad número 21.	• Incidente de seguridad identificado	• Registro de incidente	• Administrador de incidentes
21	Notificar al Administrador de Seguridad	Administración de Incidentes deberá notificar a Administración de Seguridad de la Información que el Incidente de Seguridad está en progreso o se ha llevado a cabo, para que Seguridad de la Información pueda utilizar herramientas especializadas de seguridad y habilidades para asistir a la investigación y resolución	• Registro de incidente	• Notificación	• Administrador de incidentes

		del Incidente. Continuar en la actividad número 22.			
22	Resolver incidente de seguridad	Administración de Incidentes es responsable de manejar Incidentes de Seguridad a través de su ciclo de vida, de la misma manera que otros Incidentes. Fin de actividades	• Registro de incidente	• Incidente de seguridad resuelto	• Administrador de incidentes

16.Matriz RACI

Una tarea muy importante es realizar un mapeo de los roles y las responsabilidades, así como su intervención en cada una de las actividades del proceso, para conocer quién toma parte en cada actividad y con qué nivel de participación. Este mapeo se lleva a cabo con una matriz llamada RACI, donde cada letra que forma su nombre es el nivel de responsabilidad específico en la actividad.

A continuación se muestra la nomenclatura a utilizar dentro de la tabla RACI definida para el proceso de Administración de Seguridad.

	RESPONSABILIDAD	DESCRIPCIÓN
R	Responsible	Responsable de ejecutar la actividad.
A	Accountable	Encargado del cumplimiento y la calidad en la ejecución de la actividad.
C	Consulted	Aporta conocimiento y/o información para que el responsable ejecute la actividad.
I	Informed	Rol que debe ser informado una vez que la actividad ha finalizado,

A continuación se muestra la tabla RACI definida para el proceso de Administración de Seguridad. Dicha tabla está conformada por los siguientes rubros:

- **No:** Número correspondiente a la secuencia de actividades del diagrama de flujo del proceso de Administración de Seguridad.
- **Actividad:** Nombre de la actividad del diagrama de flujo del proceso de Administración de Seguridad.
- **Roles:** Nombre de los roles participantes en el proceso de Administración de Seguridad.

No.	Actividad	Todos los procesos	Administrador de Seguridad	Administrador de Incidentes
1	Determinar requerimientos de seguridad	R	A/R	
2	Revisar requerimientos de seguridad		A/R	
3	Considerar y mantener la política de seguridad		A/R	
4	Determinar activos de información		A/R	

5	Realizar BIA		A/R	
6	Clasificar elementos de configuración		A/R	
7	Realizar análisis de riesgos		A/R	
8	Realizar e implementar plan de seguridad		A/R	
9	Acordar roles		A/R	
10	Desarrollar planes de operación, monitoreo e incidentes de seguridad		A/R	
11	Realizar concientización de la política de seguridad		A/R	
12	Levantar violación de seguridad potencial	R	A/R	
13	Realizar auditorías		A/R	
14	¿Existen temas que atender de seguridad?		A/R	
15	Realizar revisión		A/R	
16	Recomendar y acordar acción disciplinaria		A/R	
17	Acordar acción		A/R	
18	¿Requiere cambio política de seguridad ¿		A/R	
19	Identificar incidente de seguridad			R
20	Levantar registro de seguridad			R
21	Notificar al Administrador de Seguridad		I	R
22	Resolver incidente de seguridad		I	R

17.Medición

Los indicadores tienen como objetivo proveer de datos estadísticos sobre el comportamiento del proceso o calidad del producto generado por la Administración de Seguridad; a través de dichas mediciones se busca la optimización y mejora continua del proceso.

A continuación se muestra una tabla con los indicadores definidos para el proceso. Dicha tabla está conformada por los siguientes rubros:

- **Código:** Identificador asignado al indicador, para hacer referencia a este en reportes.
- **Indicador:** Nombre de la métrica
- **Descripción:** Propósito del indicador
- **Fórmula:** Ecuación o regla que relaciona objetos matemáticos o cantidades.
- **Unidad:** Unidad de medición que se obtiene al generar el indicador
- **Frecuencia:** Lapso de tiempo específico para generar el indicador
- **Responsable:** Rol responsable de generar el indicador

Código	Indicador	Descripción	Fórmula	Unidad	Frecuencia	Responsable
	% de reducción en el número de incidentes de seguridad reportados	Validar que el número de incidentes de seguridad baja debido a cumplimiento de la política de seguridad de la información.	((Total de incidentes – Número de Incidentes de Seguridad)/Total de incidentes) * 100%	%	Mensual	Administrador de Seguridad de la Información
	% de reducción en el impacto de incidentes de seguridad	Identificar que el impacto de los incidentes de seguridad baje gracias al cumplimiento de los lineamientos de seguridad.	((Total de incidentes seguridad de impacto alto– Número de Incidentes de Seguridad de impacto medio y bajo)/Total de incidentes de seguridad de impacto alto) *	%	Mensual	Administrador de Seguridad de la Información

			100%			
	% de reducción en las no conformidades detectadas contra la política de seguridad	Validar la eficiencia del proceso de Administración de Seguridad de la Información y cumplimiento de las políticas.	((Total de incidentes – Número de Incidentes de Seguridad)/Total de incidentes) * 100%	%	Mensual	Administrador de Seguridad de la Información

--- Fin del Documento --