Proceso de Administración de Seguridad	ESTÁNDAR Tipo: Estándar de proceso

Familia: Administración de servicios
Tema: Administración de Seguridad, violaciones, incidentes
Estándar: Proceso de Administración de Seguridad

Dirección General del Sistema Estatal de Informática
Secretaría de Finanzas
Gobierno del estado de México

Año: **2014**
Revisión programada: Anual
Última actualización: 2014-08-29
Última revisión: 2014-08-29

Autor(es)/Revisor(es)

Fecha	Autor/Revisor	Versión	Descripción
2013-02-03	Proveedor externo	1.0	Creación de la primer versión del documento, siendo draft, ya que no está revisada por Directores y
2013-10-08	Proveedor externo	2.0	Draft. Correcciones con base en revisión del Área de Calidad.
2013-10-08	Proveedor externo	1.0	Versión 1.0 para la DGSEI
2015-04-30	Ernesto González G.	1.0	Se cargo el estándar en la plataforma SAEGEM

Exposición de motivos

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)

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.

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

Referencias normativas

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

Términos y 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.

Cláusulas

No. Cláusula	Descripción de la cláusula	Nombre documento	Liga
1	El proceso de administración de la seguridad esta descrito en el documento denominado: "Proceso de Administración de Seguridad". Remítase a dicho documento para referencia y detalle del estándar.	PRO_PCAO_10_Proceso de Administración de Seguridad_1.1.doc	
2	El proceso de Administración de Seguridad de la Información se audita, en términos de calidad, al menos cada seis meses.		
3	El único responsable de realizar cambios al proceso de Administración de Seguridad de la Información es el Administrador de la Seguridad de la Información.		
4	La política de seguridad es confidencial y propiedad de la DGSEI.		
5	La política de seguridad deberá publicarse cada seis meses, revisándola cada tres meses.		
6	La política de seguridad deberá comunicarse a todo el personal de la DGSEI a través de campañas de concientización		

Bibliografía

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

Contacto

Dueño del estándar: Dirección de Gobierno Electrónico de la DGSEI

Correo: gobierno.electronico@edomex.gob.mx

Departamento de Nuevas Tecnologías y Estándares TIC

Correo: estandares.dgsei@edomex.gob.mx