Revista de
Tecnología e Innovación
en Educación Superior

PRINCIPALES ELEMENTOS PARA EL DISEÑO DE LA GOBERNANZA INSTITUCIONAL/ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

https://doi.org/10.22201/dgtic.26832968e.2019.2.2

Xóchitl Díaz Pillado
https://www.ties.unam.mx/

Fecha de recepción: 3 de septiembre de 2019 • Fecha de publicación: octubre de 2019

Octubre de 2019 | número de revista 2 • ISSN 2683-2968

Acervos Digitales, Dirección General de Cómputo y de Tecnologías de Información y Comunicación, UNAM

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

PRINCIPALES ELEMENTOS PARA EL DISEÑO DE LA GOBERNANZA INSTITUCIONAL/ ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Resumen

El presente artículo tiene como objetivo brindar un panorama general de los principales elementos para el diseño de la Gobernanza Organizacional de Seguridad de la Información (SI). Para ello, en la introducción se aborda como punto de partida, los Servicios Críticos Institucionales, que deberán ser considerados en primera instancia, por ser los que constituyen la misión y visión de la organización. También se efectúa la diferencia entre *SI y Seguridad Informática*.
El breve contexto menciona distintas acciones que al respecto se han llevado a cabo internacionalmente y en México, tanto el sector público como privado.
Las consideraciones generales para el diseño de la gobernanza institucional/organizacional de SI, plantean cuestiones relativas a Arquitectura de Negocio, Arquitectura Tecnológica Empresarial, Grupo Estratégico de SI, Servicios Críticos Institucionales, Infraestructura Crítica, Gestión de Riesgos e Incidentes, entre otros.
En las Áreas de Oportunidad, se enuncian las principales para las IES, como: SGSI, SGCN, cumplimiento legal y regulatorio, oferta educativa en SI y ciberseguridad para todos los niveles y áreas del conocimiento, vinculación y fomento a la cultura de SI.
Finalmente la conclusión plantea la corresponsabilidad que atañe a toda la organización que requerirá a su vez mayor colaboración interinstitucional.

Palabras clave:

Seguridad de la información, gobernanza, continuidad del negocio, servicios críticos institucionales – infraestructura crítica.

ORGANIZATIONAL SECURITY INFORMATION GOVERNANCE DESIGN: KEY ELEMENTS

Abstract

This paper aims to show a general scope of the key elements to design the Organizational Information Security Governance. To do so, in the introduction we can see why the organization critical services must be taken into account first of all. That is because those services are essential to accomplish the organization's mission and vision: its core. In this section, we contrast Information Security and Information Technology Security concepts.
As a brief context, we can find different Information Security international actions taken in one hand, and in México on the other hand, in both public and private sectors.
In order to achieve the Organizational IS Governance Design, in the general considerations section we talk about Business Architecture, Technological Business Architecture, Information Security Committee, Organizational Critical Services, Critical Infrastructure, Risk and Incident Management, etc.
In the main areas of opportunity section we have listed several of which might be of importance to the purposes of the Universities, such as: ISMS, BCMS, Law and Regulatory Enforcement, IS and Cybersecurity Academic Programs for every level and field of knowledge, IS and Cybersecurity Research and Development, IS and Cybersecurity Collaboration agreements and IS awareness.
Finally, in the conclusion section we strongly recommend that the Information Security can no longer be considered as a single area's responsibility, but as a shared commitment across the whole organization with inter-agency coordination and collaboration.

Keywords:

Information Security, governance, business continuity, critical organizational services, critical infrastructure.

TiES Revista de Tecnología e Innovación en Educación Superior

Principales elementos para el diseño de la Gobernanza Institucional/Organizacional de Seguridad de la Información
Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

PRINCIPALES ELEMENTOS PARA EL DISEÑO DE LA GOBERNANZA INSTITUCIONAL/ ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Introducción

MANTENER LA CONTINUIDAD DE LA OPERACIÓN DE SUS SERVICIOS ESENCIALES REDUNDA EN EL MAYOR INTERÉS Y BENEFICIO DE TODA INSTITUCIÓN, así como también en beneficio no sólo de sus clientes o usuarios, ya sean internos o externos, sino de todas las partes interesadas a distintos niveles. Pero, ¿cómo saber bien a bien cuáles son esos servicios esenciales?, ¿qué hacer para identificarlos? Como punto de partida deben ser considerados los que constituyan la razón de ser de la organización; es decir, aquellos que sean cruciales para cumplir su misión y proyectarla hacia su visión. Acto seguido, efectuar los siguientes cuestionamientos: de presentarse una degradación o interrupción en la prestación de dichos servicios (incidentes), ¿cuáles serían las consecuencias y cuál sería su gravedad?, ¿cuáles causas (vulnerabilidades, riesgos) podrían originar tal interrupción? Y ante ello, ¿qué implicaciones legales, regulatorias, normativas, contractuales, financieras, laborales, sociales, de reputación o confiabilidad, etc., habría que enfrentar?, ¿cuáles serían los peores escenarios que podrían presentarse?, ¿quiénes podrían conocer mejor las repercusiones que esa situación representaría y tener el panorama completo del grado de impacto que ocasionaría?, ¿qué rol juegan las áreas técnicas? Para poder responder tales preguntas y así como para poder pensar en continuidad, primero hay que considerar seriamente la Seguridad de la Información (SI) a nivel organizacional.

Aún hoy en día, al escuchar "Seguridad de la Información," la mayoría de las personas lo siguen asociando únicamente a "Seguridad Informática," refiriéndose en muchos casos a ambas como sinónimos y por ende, circunscribiéndolas al ámbito de las Tecnologías de la Información y Comunicación, o más coloquialmente, "a la gente de TI" por una parte y a las investigaciones de los académicos por otra. Sin embargo, la SI tiene un sentido mucho más amplio, cuyo fin está orientado a preservar en la mayor medida posible la *confidencialidad, integridad y disponibilidad* (Tríada CID) de la información institucional, sin perder de vista por supuesto, la trazabilidad y el no repudio de la misma desde la perspectiva de la Arquitectura de Negocio (organización), mientras que la Seguridad Informática se avoca al aspecto técnico desde el enfoque de la Arquitectura Tecnológica Empresarial. En este orden de ideas, la segunda es sólo uno de los subconjuntos que conforman a la primera. Para ilustrar lo anterior, abordaremos someramente algunos detalles.

Breve contexto

EN EL ENTORNO TANTO INTERNACIONAL COMO NACIONAL, CADA VEZ MÁS ORGANIZACIONES PERTENECIENTES AL sector público como al privado, están llevando a cabo el diseño, implementación y certificación del Sistema de Gestión de SI (SGSI) acorde a los estándares que integran la familia ISO 27000 [1]– vigente

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

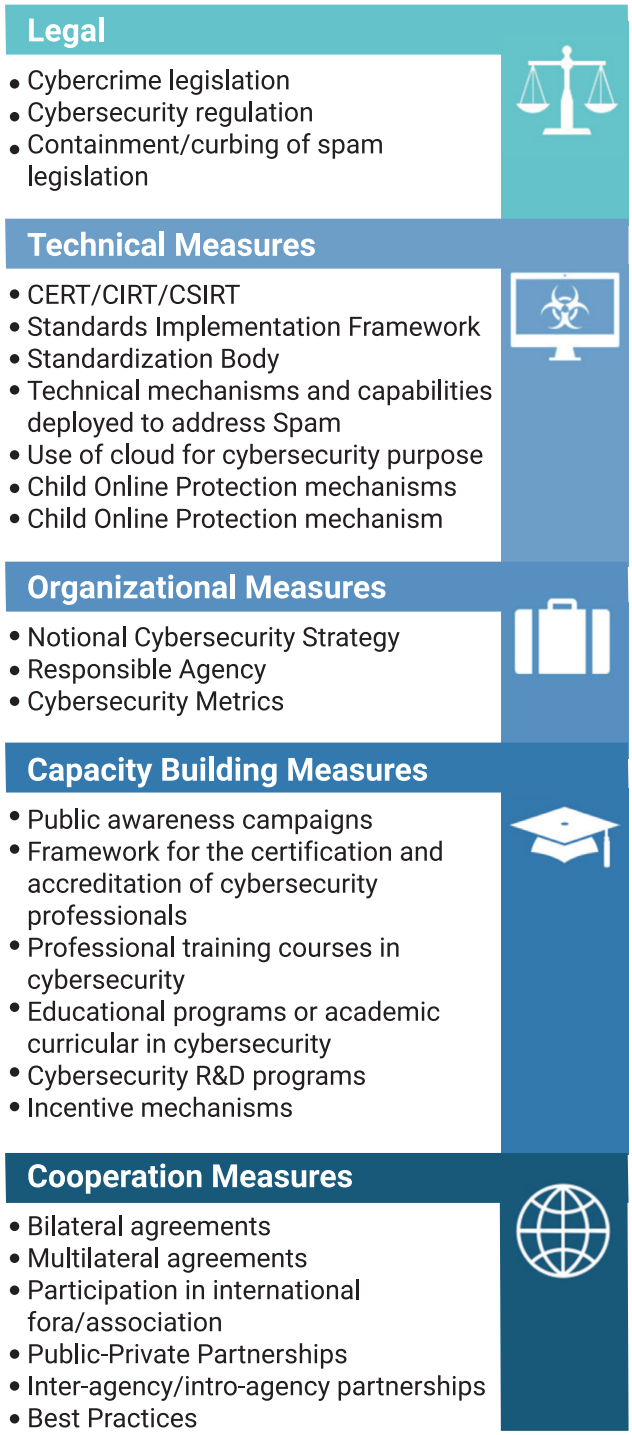


Figura 1.
" Pilares e indicadores," Global Cybersecurity Index 2018, [Fotografía]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf Consultado en agosto 29, 2019.]

(https://www.iso.org/isoiec-27001-information-security.html), e incluso obtienen la certificación del SGSI específicamente de conformidad a lo indicado en el estándar ISO/IEC 27001 Requerimientos del Sistema de Gestión de Seguridad de la Información [2] (SGSI) vigente.

Una vez que han obtenido la certificación de su SGSI, muchas empresas y/o instituciones dan el siguiente paso y se perfilan hacia la implementación de ISO 22317 Análisis de Impacto al Negocio [3] vigente, así como también a la implementación y certificación de ISO 22301 Requerimientos del Sistema de Gestión de Continuidad de Negocio [4] (SGCN) vigente.

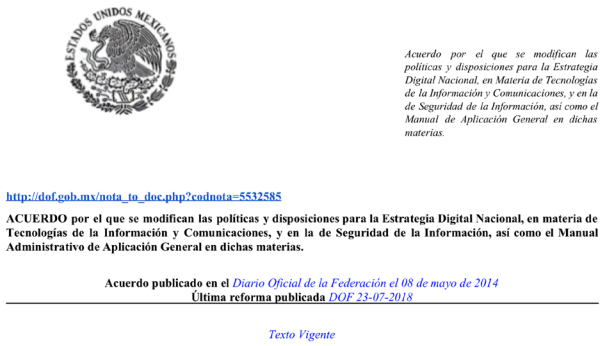
Así mismo, existen diversas organizaciones internacionales que incluso desde la perspectiva del ámbito de la ciberseguridad (considerado de forma tradicional altamente técnico), han realizado estudios de relevancia con un enfoque interdisciplinario integral. Tal es el caso de la Unión Internacional de Telecomunicaciones (*International Telecommunication Union, ITU*), la cual publicó el Índice Global de Ciberseguridad (*Global Cybersecurity Index, GCI*) [5] en 2014, 2017 y 2018. El GCI es una referencia confiable que mide el compromiso de los países respecto a la ciberseguridad a nivel global [6]. México se encuentra posicionado en el lugar 63 de 175 a nivel global y en el lugar 4 en el continente Americano. El índice está compuesto por cinco pilares de los cuales sólo uno se refiere al aspecto técnico, mientras que los cuatro restantes incluyen diversos ámbitos, entre los que se encuentran los legales, organizacionales, de construcción de capacidades y de cooperación (figura 1).

Por otra parte, en México durante la Administración Pública Federal 2013 – 2018, uno de los programas que estuvieron contenidos en su Plan Nacional de Desarrollo [7], fue el "Programa para un Gobierno Cercano y Moderno," que a su vez incluyó a la Estrategia Digital Nacional [8] de la cual se desprende el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, (MAAGTICSI), cuya modificación es vigente hasta la fecha de elaboración del presente texto. Fue publicada en el Diario Oficial de la Federación el 23 de julio de 2018 (figura 2).

Uno de los nueve procesos que conforman al MAAGTICSI es precisamente el Proceso de Administración de Seguridad de la Información (ASI).

Adicionalmente, del Programa Nacional de Seguridad Pública y del Programa para la Seguridad Nacional del

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/



Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual de Aplicación General en dichas materias.

http://dof.gob.mx/nota_to_doc.php?codnota=5532585

ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo publicado en el *Diario Oficial de la Federación el 08 de mayo de 2014*
Última reforma publicada *DOF 23-07-2018*

Texto Vigente

Figura 2.
"Estrategia Digital Nacional," 2018. [Fotografía]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/380408/MAAGTICSI_compilado__20182208.pdf [Consultado en agosto 29, 2019.]

mismo Plan, se desprendió también a su vez la Estrategia Nacional de Ciberseguridad [9] (figura 3).

En ambas Estrategias Nacionales referidas, se encuentran dispuestas entre varias cuestiones, las relativas a SI, enfoque basado en Gestión de Riesgos y Respuesta a Incidentes, a ser implementadas en las instancias de la Administración Pública Federal.

Visto el panorama descrito en la introducción y en el contexto, ¿cómo proceder?

Consideraciones generales para el diseño de la gobernanza institucional/organizacional de SI

ES MENESTER RESALTAR QUE EL ACTIVO DE INFORMACIÓN MÁS IMPORTANTE DE CUALQUIER ORGANIZACIÓN, son las personas que la integran, dado que son ellas las que poseen el conocimiento necesario, el *know how* para que aquellas operen. El tema de SI es sumamente amplio y en esta ocasión, trataremos la parte organizacional. De acuerdo con lo indicado por el estándar ISO 27001 vigente, los servicios esenciales, prioritarios y de mayor criticidad para el negocio son los que deberán ser asegurados en primera instancia, por lo que deberán ser incorporados desde el primer ciclo de implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)**. Este alcance, como la definición de la **Política Institucional de Seguridad de la Información**, deberán ser establecidos por el nivel estratégico empresarial/institucional. Esto tiene mucho sentido si consideramos que, después de todo, ¿quién mejor que la alta dirección para saber con precisión los efectos de la detención parcial o total, durante varios minutos, horas o días de las actividades neurálgicas de la institución?

Tener siempre presente la misión, la visión y los objetivos institucionales, ayudará a identificar de forma inicial, aquellos servicios que guardan alineación estratégica y por ende, los procesos de negocio que los integran. De ahí, se deberá definir cuáles son servicios esenciales y cuáles son servicios de apoyo. Con el fin de formalizar la determinación de los servicios prioritarios, marcos arquitectónicos como SOA [10] (*Service Oriented Architecture*), **TOGAF®** [11] (*The Open Group Architecture Framework*), estándares internacionales como los citados ISO/IEC 27001 vigente, ISO 22301 vigente, ISO 22317 Análisis de Impacto al Negocio – BIA, *Business Impact Analysis* –, herramientas como el enfoque de procesos, el análisis FODA, las 5 Fuerzas de Porter [12], y *Balanced Score Card* [13] son de mucha utilidad.

Es factible expresar la Arquitectura Empresarial (o de negocio), en términos sumamente simplificados en dos capas: la capa 1 involucra a los servicios institucionales/

Figura 3.
"Estrategia Nacional de Ciberseguridad," 2017. [Fotografía]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [Consultado en agosto 29, 2019.]

https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

organizacionales (críticos o no) y a los procesos de negocio que componen a los mismos. La capa 2 contiene lo relativo a la Arquitectura Tecnológica Empresarial, la cual soporta a su vez a la capa 1. En este sentido, la Arquitectura Empresarial contempla a la organización de forma holística. Ahora, observemos cómo se gestan las interacciones entre ambas capas. Partiendo prioritariamente de la determinación de los ya citados servicios críticos, se procede a identificar aquellos activos de información en los cuales dichos servicios "viven" o están instalados. Tales activos son por añadidura de igual forma críticos o esenciales. Precisando: un grupo de integrantes de la alta dirección, llamado por ejemplo, Grupo Estratégico de SI, **GESI** [14], son quienes determinan los servicios críticos y sus procesos de negocio (capa 1). Si esos servicios son proporcionados por aplicativos, sistemas, bases de datos etc., (software), que naturalmente se encontrarán hospedados en hardware, entonces tales activos de información se denominan infraestructuras críticas/ esenciales de información. Cabe mencionar que de forma general se puede distinguir entre dos tipos principales de infraestructura crítica: de cómputo (servidores, unidades de almacenamiento, etc.), y comunicaciones (elementos que componen las redes de datos y que proveen la conectividad con otras redes locales, externas y aquellos que proveen la conexión hacia Internet, como routers, switches, etc. y la cada vez más preponderante "nube"). En este orden de ideas, tanto el hardware como el software forman parte de la Arquitectura Tecnológica Empresarial (capa 2). Para que la capa 1 pueda operar sobre la capa 2, entran en acción distintos equipos multidisciplinarios (formados tanto por los responsables de los procesos de negocio como por especialistas técnicos) que dependerán del GESI, y que por tanto lo apoyarán para que de forma conjunta, identificar tales infraestructuras, que serán contempladas para realizar una Gestión de Riesgos con apego sugerido a ISO/IEC 27005 [15] vigente, lo que permitirá averiguar cuán vulnerable es y ante qué riesgos existe exposición a efecto de diseñar un Plan de Tratamiento de Riesgos, en el que se plasmen los controles de seguridad que sean aplicables. Los controles de seguridad deberán implementarse preferentemente con base en los ya incluidos en el Anexo "A" del estándar ISO/IEC 27001 vigente, con la intención de evitar en la mayor medida posible que esos riesgos se materialicen tanto en la operación del día a día como en las ventanas de mantenimiento y que en tal caso, llegaran a convertirse en Incidentes de SI, los cuales desde luego también implican llevar a cabo una correspondiente labor de gestión.

Es también menester resaltar que es de suma importancia mantener a la vista además de los activos/ infraestructura de información críticos tangibles, los activos de información intangibles, como el prestigio, la reputación y la confianza en la institución u organización, que por un incidente dado de SI, podrían verse seriamente afectados.

La Gestión de Riesgos es un proceso vivo que no se hace una vez al año. Si llegado el caso por no haber sido contemplados ciertos controles o bien porque el control o controles implementados no hayan sido del todo adecuados o hayan resultado insuficientes, es cuando pudiera materializarse algún o algunos riesgos afectando negativamente la SI y/o provocando el incumplimiento de lo establecido en la Política Institucional de SI. Es entonces cuando los riesgos dejan de serlo y se convierten en incidentes. Por lo tanto, será momento de iniciar la Gestión de Incidentes de SI, sugiriéndose pare ello el uso de ISO/IEC 27035-1 [16] vigente, Gestión de Incidentes de Seguridad de la Información – Parte 1: Principios de Gestión de Incidentes, ISO/IEC 27035-2 [17] vigente y Gestión de Incidentes de Seguridad de la Información – Parte 2: Guía de planeación y preparación para Respuesta a Incidentes. Así mismo, será recomendable considerar el estándar ISO/IEC 27031 [18] vigente, *Guidelines for information and communication technology readiness for business continuity* – un IRBC – lo que previamente se conocía como un Plan de Recuperación de Desastres – DRP, *Disaster Recovery Plan* – y que sí, en efecto, éste elemento a diferencia de los otros, es netamente técnico –. La Gestión de Incidentes entonces proporcionará información vital que retroalimentará a la Gestión de Riesgos y a los Controles de Seguridad (también llamados mecanismos de seguridad o salvaguardas), contribuyendo así a propiciar un ciclo de mejora continua.

Cabe aclarar que es de vital importancia realizar lo descrito mediante Gestión de Cambios o Cambios Administrados con un panorama global de acuerdo con las competencias respectivas tanto en capa 1 como en capa 2 (los riesgos e incidentes se presentan tanto en los procesos de negocio como en la parte técnica).

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

Áreas de oportunidad

LAS CIRCUNSTANCIAS PREVALECIENTES EN LA ACTUALIDAD Y LA CONSTANTE EXPANSIÓN DE NUESTRA COTIDIANIDAD en el llamado "ciberespacio," han dotado más que nunca de altos niveles de prioridad a la SI. Las actividades derivadas de esta hiperconectividad constituyen una tan vasta diversidad desde de las más sencillas situaciones individuales, hasta la complejidad que implica el desarrollo en el entorno mundial.

Conscientes o no aún de ello, ningún tipo de organización puede seguir manteniéndose ajena al hecho de cada vez un mayor número de países cuentan desde hace tiempo con implementaciones del SGSI, del SGCN, así como de Estrategias Nacionales de Ciberseguridad, prioridades todas en sus agendas nacionales al más alto nivel, que en consecuencia se propagan hacia todos los sectores.

Por tanto, habiendo expuesto el panorama abordado a lo largo de estas líneas, resulta inminente que las Instituciones de Educación Superior (IES) den prioridad dentro de sus Planes de Desarrollo Institucionales, a la inclusión de un eje o línea fundamental que se avoque a la SI Institucional, involucrando así proactivamente a su cúpula directiva en el diseño de estrategias que formalicen a cabalidad la importancia que ésta verdaderamente merece, con el fin de emprender acciones con un compromiso fehaciente para su implementación en toda la institución.

Hay que reconocer que en muchas acciones de gobernanza no se empieza con un lienzo en blanco, y en ese sentido el potencial con que ya cuentan las IES es enorme. Con el patrocinio y compromiso de la alta dirección se pueden capitalizar las iniciativas ya existentes en las mismas, para dejar de operar en silos y promover la interoperabilidad, con el fin de concatenar los esfuerzos aislados hasta el momento, de forma coordinada y articulada de manera que propicien la utilización de todos los recursos disponibles. Un ejemplo de ello son las matrices de riesgos desarrolladas con las metodologías propias de la institución y con apego a la normatividad que las rige. Todo esto puede verse enriquecido por las aportaciones, innovaciones y beneficios que generan algunas de las investigaciones de la academia relacionadas y que aplicadas en conjunto con la gobernanza y las buenas prácticas, creen una sinergia que de igual forma nutran a la mejora continua.

Así mismo y de acuerdo a su misión y visión, las IES pueden diseñar planes y programas de estudio que contengan asignaturas referentes a la SI que incidan no sólo en carreras afines a las TIC, sino en todas las áreas del conocimiento, mismas que de acuerdo a sus competencias, se incorporarán a un "*cibermercado*" laboral al que deberán incursionar de facto con un bagaje mínimo indispensable en la materia y que asciende vertiginosamente.

Con base en los planteamientos hasta aquí realizados, a continuación se enuncian una serie de rubros en las que seguramente las IES, tienen una vastedad de áreas de oportunidad:

- Acciones para iniciar con la implementación de un SGSI:
  - Realizar con alineación estratégica, la determinación de los Servicios Institucionales Críticos, Procesos de Negocio e Infraestructura Crítica.
  - Identificar los activos de información tangibles/intangibles con base en los Servicios Críticos Institucionales.
  - Establecer la Política Institucional de Seguridad de la Información, así como su alcance con base en los Servicios Críticos Institucionales determinados.
  - Designar, por parte del Titular de la Institución, al Responsable de la SI Institucional en el nivel jerárquico estratégico (*Chief Information Security Officer, CISO*).
  - Establecer por parte del Titular de la Institución en conjunto con el RSII, al Grupo (comité, equipo) Estratégico de SI Institucional que será coordinado por el RSII. Sus integrantes deberán pertenecer al nivel jerárquico estratégico y las áreas institucionales críticas.
  - Efectuar el aseguramiento de las islas locales (en unidades académicas y/o administrativas) de Infraestructura Crítica y de Desarrollo de Servicios Críticos Institucionales que se encuentren fuera de la cobertura de redundancia eléctrica y alta disponibilidad que ofrecen los Centros de Datos Institucionales.
  - Establecer Centros de Datos alternos al Centro de Datos Institucional.
  - Implementar medidas de seguridad física y lógica de la infraestructura crítica.

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

- Implementar repositorios seguros de configuraciones de la Infraestructura Crítica Institucional.
- Establecer marcos de referencia – *Frameworks* – Institucionales para el desarrollo seguro de sistemas, aplicaciones, etc.
- Efectuar la Gestión de Riesgos de SI.
  - Capitalizar las iniciativas y proyectos institucionales ya existentes, como las Matrices de Riesgos Institucionales.
- Efectuar la Gestión de Incidentes de SI IRBC (antes DRP), Planes de Comunicación y Escalamiento.
  - Crear *CERT's* o *CSIRT's* académicos institucionales.
- Efectuar la Gestión del Conocimiento en Ciberseguridad recabado por la institución.
- Efectuar la Gestión del Talento en Ciberseguridad formado por la institución.
- Realizar Acuerdos de Confidencialidad de SI en concordancia con las funciones y responsabilidades de directivos, responsables y comunidad en general de la institución, así como de sus distintas partes interesadas.
- Establecer, en conjunto con las áreas críticas institucionales y el área de capital humano, los procesos y procedimientos para la incorporación/separación segura del empleo.
- Realizar auditorías periódicas de SI.
- Tomar en consideración los estudios realizados para universidades (por ejemplo, el elaborado por la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), en el Estado Actual de las Tecnologías de la Información y las Comunicaciones en las Instituciones de Educación Superior / Estudio 2018 [19], cuyo capítulo cinco es relativo a SI).

– Acciones para iniciar con la implementación de un SGCN:
  - Establecer medidas para preservar en el mayor grado posible la seguridad de las personas que conforman la institución.
  - Implementar planes para la Continuidad de los Servicios Institucionales Críticos.
  - Efectuar el Análisis de Impacto al Negocio, tomando primordialmente en consideración el correspondiente a los Servicios Críticos Institucionales.
  - Realizar simulacros de ataques y ciberataques por agentes internos y/o externos (*insiders/outsiders*) a la institución.
– Acciones generales para el cumplimiento legal y regulatorio:
  - Observar leyes y reglamentos aplicables según el caso, relativos a SI (por ejemplo en cuanto a Protección de Datos Personales, clasificación y resguardo de información, preservación de documentos electrónicos, etc.)
  - Observar la Normatividad Institucional establecida con relación a la SI en caso de contar con alguna (por ejemplo en materia de gestión de riesgos, etc.)
– Acciones generales que podrían ser incorporadas en la oferta educativa a nivel Medio Superior, Superior, Posgrado e Investigación en SI y Ciberseguridad:
  - Integrar formación en SI y Ciberseguridad en planes y programas de estudios a nivel Medio Superior, Superior y Posgrado en todas las áreas de conocimiento (Médico Biológicas, Sociales Administrativas, Físico-Matemáticas, Ingenierías, etc.), acorde a dichas áreas.
  - Difundir la oferta en formación en SI y Ciberseguridad de las distintas universidades.
  - Conformar y difundir (en caso pertinente) un padrón de investigadores y proyectos de investigación en SI y Ciberseguridad.
– Acciones generales para la vinculación Academia – Investigación – Industria:
  - Generar mecanismos de vinculación, convenios de colaboración, etc., nacionales e internacionales con universidades y organismos público-privados en SI y Ciberseguridad.
– Acciones generales para establecer Programas de Fomento a la Cultura de SI
  - Crear programas de sensibilización y concientización a la comunidad en general para fomentar la cultura de la SI y Ciberseguridad Institucional.
  - Generar capacidades y formación: Cursos/Diplomados y capacitación especializada en Seguridad de la Información y Ciberseguridad.

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

¿Por dónde comenzar?

AQUÍ LOS PRIMEROS PASOS RECOMENDADOS PARA INICIAR CON EL ESTABLECIMIENTO DE LA GOBERNANZA Institucional de SI con perspectiva incremental:

Paso	Responsable	Descripción
1. Designación del Responsable de SI Institucional (RSII), *Chief Information Security Officer* (CISO) y establecimiento del Grupo Estratégico de SI.	Titular de la Institución	El RSII y los miembros del GESI deberán pertenecer al nivel jerárquico estratégico y las áreas institucionales críticas. El RSII coordinará al GESI.
2. Determinación de los Servicios Críticos Institucionales.	GESI	El RSII deberá presentarlos al Titular de la Institución para su consideración y en su caso para la aprobación del titular.
3. Definición de la Política Institucional de Seguridad de la Información y su alcance.	GESI	Con base en los Servicios Críticos Institucionales aprobados, definir la Política y presentarla al área jurídica institucional y al Titular de la Institución para su consideración y en su caso aprobación. Una vez autorizada, la Política deberá ser publicada y difundida a toda la comunidad y partes interesadas.
4. Establecimiento y coordinación de un equipo de trabajo de apoyo para el GESI.	GESI	El equipo de trabajo con base en los Servicios Críticos Institucionales, deberá determinar los procesos de negocio que los integran así como la Infraestructura Crítica que los soportan u hospedan. Tomar en consideración las interdependencias correspondientes de ambos rubros e implementar un Repositorio Seguro de Configuraciones para dichas infraestructuras. Cabe resaltar que el citado equipo deberá ser multidisciplinario, y que sus miembros deberán ser especialistas de los procesos de negocio, así como especialistas técnicos.
5. Gestión de Riesgos e Incidentes de SI	Equipo de trabajo de apoyo	Con base en los Servicios Críticos Institucionales, sus procesos de negocio y su Infraestructura Crítica, realizar ambas gestiones.
6. Evaluación y mejora continua.	GESI	Implementar un programa de evaluación para realizar la retroalimentación y mejora continua de los cinco pasos anteriores.

Tabla 1.
Seis primeros pasos recomendados para iniciar una implementación de un SGSI.
Fuente: elaboración propia.

Xóchitl Díaz Pillado
https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

Es así como en el presente documento brevemente se han abordado las áreas de oportunidad más neurálgicas. Sin lugar a dudas, existen muchas más en el amplísimo campo de acción de las IES, las cuales dependerán de las particularidades, concepción, grado de concientización, necesidades, nivel de madurez, etc., que cada una de ellas guardan con respecto a la SI y la ciberseguridad como una estrategia holística institucional.

Conclusión

NO ES SOSTENIBLE CONTINUAR DELEGANDO LA SI INSTITUCIONAL SOLAMENTE A LAS ÁREAS TÉCNICAS Y OPERATIVAS. Es un trabajo conjunto que nace de la perspectiva estratégica y que permea a todas las áreas y niveles de la organización. Siendo una corresponsabilidad que trasciende los confines de la misma al incorporarse en un frente común, mediante su participación a través de la suma de sus capacidades y talentos, en estrategias e iniciativas de colaboración interinstitucional en la que las alianzas público-privadas serán cruciales.

https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

BIBLIOGRAFÍA

[1] International Organization for Standardization, "ISO/IEC 27001 Information security management" *International Organization for Standardization*, 2019. [En línea]. Disponible en: https://www.iso.org/isoiec-27001-information-security.html. [Consultado en septiembre 22, 2019].

[2] International Organization for Standardization, "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements" *International Organization for Standardization*, 2013. [En línea]. Disponible en: https://www.iso.org/standard/50054.html. [Consultado en septiembre 22, 2019].

[3] International Organization for Standardization, "ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)" *International Organization for Standardization*, 2015. [En línea]. Disponible en: https://www.iso.org/standard/54534.html. [Consultado en septiembre 22, 2019].

[4] International Organization for Standardization, "ISO 22301:2012 Societal security — Business continuity management systems — Requirements" *International Organization for Standardization*, 2012. [En línea]. Disponible en: https://www.iso.org/standard/50038.html. [Consultado en septiembre 22, 2019].

[5] International Telecommunication Union, "Global Cibersecurity Index" *International Telecommunication Union*, 2019. [En línea]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. [Consultado en agosto 29, 2019].

[6] International Telecommunication Union, "Global Cibersecurity Index" *International Telecommunication Union*, 2019. [En línea]. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. [Consultado en agosto 29, 2019].

[7] Gobierno de los Estados Unidos Mexicanos, "Plan Nacional de Desarrollo 2013-2018" *Diario Oficial de la Federación,* 2013. [En línea]. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5299465&fecha=20/05/2013. [Consultado en agosto 29, 2019].

[8] Gobierno de los Estados Unidos Mexicanos, "ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias" *Diario Oficial de la Federación*, 2018. [En línea]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/380408/MAAGTICSI_compilado__20182208.pdf. [Consultado en agosto 29, 2019].

[9] Gobierno de los Estados Unidos Mexicanos, "Estrategia Nacional de Ciberseguridad" *Gobierno de los Estados Unidos Mexicanos*, 2017. [En línea]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf. [Consultado en agosto 29, 2019].

[10] W.R. Schulte, "Five Principles of SOA in Business and IT". Gartner, 2006.

[11] The Open Group. "The TOGAF® Standard" *The Open Group*, 2019. [En línea]. Disponible en: https://www.opengroup.org/togaf. [Consultado en agosto 29, 2019].

https://doi.org/10.22201/dgtic.26832968e.2019.2.2
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

[12] S. Michaux, and A. C. Cadiat, *Porter's Five Forces: Understand competitive forces and stay ahead of the competition (Management & Marketing Book 1)*, 50minutes.com, 2015. [E-book] Disponible en: Amazon Kindle Edition.

[13] R. Kaplan, and D. Norton, "Balance Score Card". Harvard Business Review, 1992.

[14] Gobierno de los Estados Unidos Mexicanos, "ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias" *Diario Oficial de la Federación*, 2018. [En línea]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/380408/MAAGTICSI_compilado__20182208.pdf. [Consultado en agosto 29, 2019].

[15] International Organization for Standardization, "ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management" *International Organization for Standardization*, 2018. [En línea]. Disponible en: https://www.iso.org/standard/75281.html. [Consultado en agosto 29, 2019].

[16] International Organization for Standardization, "ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management" *International Organization for Standardization*, 2016. [En línea]. Disponible en: https://www.iso.org/standard/60803.html. [Consultado en agosto 29, 2019].

[17] International Organization for Standardization, "ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response" *International Organization for Standardization*, 2016. [En línea]. Disponible en: https://www.iso.org/standard/62071.html. [Consultado en agosto 29, 2019].

[18] International Organization for Standardization, "ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity" *International Organization for Standardization*, 2011. [En línea]. Disponible en: https://www.iso.org/standard/44374.html. [Consultado en agosto 29, 2019].

[19] Asociación Nacional de Universidades e Instituciones de Educación Superior, *Estado Actual de las Tecnologías de la Información y las Comunicaciones en las Instituciones de Educación Superior / Estudio 2017*. México: ANUIES, 2017.

Cómo se cita:

X, Díaz Pillado, "Principales elementos para el diseño de la Gobernanza Institucional/Organizacional de Seguridad de la Información," *TIES, Revista de Tecnología e Innovación en Educación Superior*, n.o. 2, octubre, 2019. [En línea]. Disponible en: https://www.ties.unam.mx/ [Consultado en octubre, 2019].