Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencias de la Administración

Concientización y cultura de la seguridad de la información en una Institución Gubernamental

T e s i s

Que para optar por el grado de:

Maestra en Informática Administrativa

Presenta:
Tania Yadira Hernández Molina

Tutor:
Dr. José Luis Solleiro Rebolledo
Facultad de Contaduría y Administración

Ciudad de México, febrero de 2019

Índice

Introducción

Debido a la creciente digitalización de los negocios por medio del uso de dispositivos tecnológicos se ha incrementado la inversión que las organizaciones hacen en seguridad de la información lógica y física.

Por tal motivo, los requerimientos de seguridad son cada vez mayores debido a que se busca que los recursos informáticos de una organización estén disponibles y que no se encuentren afectados por personas o situaciones maliciosas. Estas personas pueden ser o no parte de la organización y buscan tener acceso a información confidencial para modificar, sustraer o borrar datos; lo que puede ocasionar una afectación en las actividades de la organización y generar pérdidas económicas.

Por lo anterior, resulta transcendental establecer políticas de seguridad que permitan implementar una serie de solucione tecnológicas, así como el desarrollo de un plan de acción que ayude a actuar de forma rápida y eficaz en el manejo de incidentes, recuperación de la información y la disminución del impacto. Asimismo, resulta valioso la aplicación de mejores prácticas orientadas a crear una cultura de seguridad adecuada sobre el aseguramiento de la información, al igual que la implementación de diversas normas y estándares que se requieres para lograrlo.

El presente estudio de caso aborda uno de los aspectos que menos pueden controlarse en seguridad de la información: las personas. De acuerdo con (Excelsior, 2018), los empleados en entrenamiento, exempleados y proveedores de servicio de tecnología son los principales responsables de llevar a cabo algún tipo de fraude en las compañías. Por tal motivo, conocer el nivel de concientización y cultura en seguridad de la información es relevante para la creación de estrategias orientadas a mejorar la cultura organizacional.

Este caso de estudio está dirigido al sector gubernamental en México y en específico a la Auditoría Superior de la Federación por ser quien, por sus actividades, maneja información reservada misma que es susceptible a ser robada

o sufrir alteraciones, en temas de corrupción o pérdidas económicas. Expresar cuál es el objetivo

Resumen Capitular

Capítulo 1. Este capítulo está enfocado en conocer los conceptos básicos sobre la seguridad de la información y la seguridad informática, así como el panorama general en el mundo, las principales instituciones internacionales en la materia, los países líderes y las tendencias de ciberseguridad.

Capítulo 2. La seguridad de la información en instituciones gubernamentales, está orientado en ampliar el estudio de la seguridad de la información en las instituciones gubernamentales en México, la legislación mexicana y las distintas medidas estratégicas que el país implementa, así como la evaluación de estas.

Capítulo 3. El papel de las normas y mejores prácticas en la seguridad de la información; el análisis se enfocará en la revisión de la serie de normas ISO 27000 y la serie de publicaciones 800-50 del Instituto Nacional de Estándares y Tecnología de la agencia federal del Departamento de Comercio de los Estados Unidos, desde el punto de vista de la concientización de la seguridad de la información y las mejores prácticas relacionadas.

Capítulo 4. Caso de estudio: Auditoría Superior de la Federación, se presenta la justificación, problemática y metodología con la que se llevará a cabo la recolección de datos, con la finalidad de conocer la concientización y la cultura en seguridad de la información que tengan los empleados de la ASF, asimismo, se presenta el panorama general de actuación y el impacto que tiene la seguridad en la fiscalización en México.

Capítulo 5. Este capítulo está dedicado al análisis de los datos que se obtuvieron por medio de los diferentes métodos de recolección de datos, de esta manera se pretende llegar a responder las hipótesis, ya que, se tendrá un amplio conocimiento de la situación de la seguridad de la información en la ASF y por consecuencia se toma como base para hacer recomendaciones.

Capítulo 1. Acercamiento a la Seguridad de la información

1.1 Antecedentes

La seguridad en las organizaciones fue contemplada desde principios del siglo pasado, en estos inicios, la seguridad se limitaba a salvaguardar los activos físicos, instalaciones, la seguridad del personal y resguardarse contra el robo, fuego, inundaciones y todo tipo de disturbios sociales que pusieran en peligro las operaciones del negocio.

En ese tiempo la seguridad de la información aún no era considerada, principalmente porque no se tenían todos los sistemas informáticos que hoy en día existen y que contribuyen directamente a la gestión de los negocios.

Las Tecnologías de la Información y Comunicación han facilitado en gran medida la optimización de recursos, por medio de la vinculación de las diferentes áreas funcionales de las organizaciones, lo que ocasiona un correcto aprovechamiento de sus recursos materiales, financieros y humanos.

Antes de comenzar con el estudio de los esquemas de seguridad en la información que tienen las instituciones de gobierno, es significativo definir qué es la información y su importancia para, posteriormente, comprender la relevancia de su seguridad.

Hoy día estamos rodeados de información y los sistemas tecnológicos nos facilitan mucho más el acceso a ella. (Chiavenato, 2006, pág. 95) nos aporta una definición de información en donde menciona que es: “un conjunto de datos con un significado concreto, real y utilizable”. Otro concepto importante es la gestión del conocimiento (Mandado, 2003, pág. 59) menciona que: “es el proceso sistemático de crear, mantener y alimentar una organización con conocimientos, de manera que se les saque el mayor partido para crear valor añadido y crear una ventaja competitiva”.

Con lo anterior observamos que el conjunto de datos, gracias a su análisis, adquiere un significado para un individuo, organización o sociedad, estos datos, al

darles sentido, se convierten en información y, a su vez, al emplearse para alguna actividad específica, esta información se convierte en conocimiento que puede ayudar directamente a la toma de decisiones. Es aquí cuando las tecnologías de la información adquieren importancia, ya que, facilitan la gestión de la información y el conocimiento que posee una organización, seleccionándola y estructurándola para aumentar su valor. Toda empresa que tenga información oportuna y de calidad tanto externa como interna tendrá un mayor nivel de competitividad y oportunidades de desarrollo, he aquí la relevancia de mantenerla segura.

Incluso actualmente se pueden observar muchos ejemplos de servicios críticos que son soportados en su práctica por sistemas y redes informáticas como los servicios de producción y suministro eléctrico, medios de transporte, servicios de salud, abastecimiento de agua, gas etcétera. Mantener la operación de estos servicios, el resguardo de los sistemas y datos que se manejan es el día a día de una sociedad moderna.

1.2 Seguridad de la información

Una vez que hemos hablado acerca de la información y su importancia, podemos comenzar por describir los conceptos de seguridad de la información y seguridad informática, los cuales son utilizados con bastante frecuencia y se encuentran sumamente ligados. Por esta razón resulta importante conocer sus diferencias.

Comencemos con el concepto de seguridad de la información, el cual es definido por la norma ISO 27002 como la preservación de la confidencialidad, la integridad y la disponibilidad de la información. (medidas conocidas por su acrónimo “CIA” en inglés: “Confidentiality, Integrity, Availability”).

. Estos conceptos comprenden lo siguiente:

- Confidencialidad: está relacionado con la privacidad de los datos, es decir, no revelar los datos a personal no autorizado.

- Integridad: es el aseguramiento de que los datos no hayan sido manipulados.
- Disponibilidad: se refiere a que la información se encuentre accesible en todo momento al personal autorizado.

Figura 1.1. Seguridad de la Información según la norma ISO/IEC 17799

Figura 1, Triángulo de la seguridad de la información. Fuente: (Vieites A. G., 2014, pág. 17)

De igual manera Jeimmy J. Cano (año), define a la seguridad de la información como**:** "la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información". Es decir, este concepto está vinculado directamente con la parte estratégica y marco referencial que debe seguir una empresa para asegurar su información.

1.3 Seguridad informática

Por otra parte, a continuación se recopilaron definiciones de seguridad informática que aportan distintos autores, por ejemplo (Santos, 2014, pág. 19) menciona que: "La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así

como su modificación, sólo sea posible para las personas que se encuentren acreditadas y dentro de los límites de su autorización". Asimismo (Vieites A. G., 2014, pág. 16) define la Seguridad Informática como "cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema". A su vez, la norma ISO 7498 define la Seguridad Informática como "una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización".

Los principales objetivos de la seguridad informática se pueden resumir en los siguientes enunciados:

- Garantizar la adecuada utilización de los recursos y aplicaciones del sistema.
- Limitar las pérdidas de información y conseguir una adecuada recuperación del sistema en caso de un incidente de seguridad.
- Minimizar y gestionar riesgos de seguridad en la información.
- Cumplir con el marco legal.

Existen cuatro planos de actuación de la seguridad informática, los objetivos antes mencionados están contemplados dentro de ellos.

Figura 2, Planos de actuación de la seguridad informática. Fuente: elaboración propia con base en los planos de actuación de la seguridad informática, (Vieites A. G., 2014, pág. 19).

La figura 2 ilustra todos los sistemas informáticos tanto de hardware y software utilizados para la gestión de la información; asimismo, la sensibilización y formación del personal directivo, gerencial y operativo; también, las políticas, normas y procedimientos establecidas; así como, el cumplimiento de la legislación aplicable.

Por lo tanto, mientras que la seguridad de la información se encarga de establecer el plan y marco regulatorio para mantener la confidencialidad, integridad y disponibilidad de la información, la seguridad informática es el medio por el cual se van a cumplir estos objetivos, es decir, la seguridad informática aporta el nivel técnico y operacional para implementar las políticas de seguridad y el análisis de riesgos. A continuación, se muestra un esquema para facilitar su comprensión:

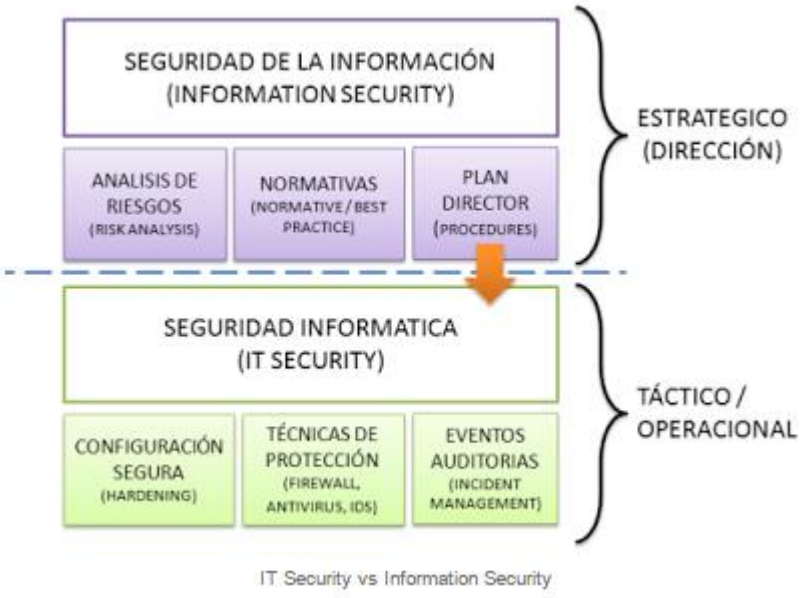

Figura 3, Diferencia entre seguridad informática y seguridad de la información. Fuente: (Seguridad para todos, 2011)

Con el esquema de la figura 3, se puede visualizar la estrecha relación que existe entre la seguridad de la información y la seguridad informática, podemos concluir, que son complementos que buscan la ejecución de buenas prácticas de la gestión corporativa, siendo responsabilidad de la alta dirección el poner los recursos y medios necesarios para la implantación de un adecuado sistema de Gestión de la Seguridad de la Información en la organización.

1.4 Amenazas informáticas

Una vez que hemos hablado sobre la seguridad informática, es importante conocer los tipos de amenazas que existen en contra de los sistemas informáticos y, sobre todo, que ponen en peligro la información y conocimiento que posee una empresa o institución gubernamental.

Comenzaremos con definir qué es una amenaza, de acuerdo con EC-Council Certified Security Specialist una amenaza es: “cualquier circunstancia o evento que

tiene el potencial de causar daño a un sistema o red", estas amenazas pueden causar destrucción de los datos o implicar invasión a la privacidad de la información.

Los sistemas informáticos están expuestos a sufrir diferentes tipos de amenazas, las cuales se pueden clasificar en tres grupos:

- Amenazas naturales
  Se trata de cualquier daño que puedan sufrir los sistemas informáticos causados por inundaciones, incendios, tormentas etc. que no sean provocadas con fines maliciosos.
- Amenazas por agentes internos
  Errores, por parte de empleados, en la utilización de herramientas, descuidos o malas intenciones por parte de ellos.
- Amenazas por agentes externos
  Virus informáticos, ataques de una organización criminal, sabotajes, intrusos en la red, robos, estafas etc.

Otro concepto que es importante definir es el de vulnerabilidad, de acuerdo con EC-Council Certified Security Specialist una vulnerabilidad es: "una debilidad o error de implementación que puede causar un evento inesperado, indeseable y que pone en riesgo la seguridad del sistema". Las vulnerabilidades pueden presentarse de manera física o lógica, teniendo por origen errores de ubicación, instalación configuración y mantenimiento de los equipos.

Hay aspectos organizativos que pueden influir en la existencia de vulnerabilidades en los sistemas, tales como: procedimientos mal definidos, no actualizados o ausencia de políticas de seguridad. Esto provoca que el factor humano sea el origen de muchos de estos problemas, desde el nivel directivo por la falta de implementación de políticas, hasta el nivel operativo por descuidos o incluso acciones mal intencionadas.

La diferencia entre amenaza y vulnerabilidad radica en que no todas las amenazas pueden convertirse en ataques, es decir, que se convierta en un incidente de seguridad; éste es cualquier evento que tenga como resultado la interrupción de los servicios suministrados por el sistema informático, con posibles pérdidas físicas de activos o financieras. Un incidente de seguridad es la materialización de una amenaza. Mientras tanto, la vulnerabilidad está más orientada a la omisión o errores, físicos o lógicos, en los sistemas informáticos.

Una vez que la amenaza se ha convertido en un incidente de seguridad, el concepto de impacto está muy relacionado, el cual, está definido como: “la medición y valoración del daño que podría producir a la organización un incidente de seguridad” (Vieites A. G., 2014, pág. 62). Medir el nivel de impacto resulta complejo, ya que se tendrá que tomar en cuenta los daños tangibles e intangibles, sobre todo en la cuantificación de la información que se haya dañado o que haya sido sustraída. Esta medición puede ser clasificada con niveles de impacto bajo, moderado o alto, los cuales indicarán el nivel de compromiso que tuvieron los sistemas informáticos frente al incidente y las repercusiones que se tuvieron.

Conocer el nivel de riesgo que tienen los sistemas informáticos también es importante para las empresas. El riesgo es definido como: “la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización” (Vieites A. G., 2014, pág. 63). Este conocimiento, del nivel de riesgo, dependerá del análisis de las vulnerabilidades del sistema, las amenazas y el impacto que puedan tener frente a los activos tangibles e intangibles que posee la empresa.

La medición del impacto de un incidente de seguridad tiene que ver directamente con el Plan de Seguridad de la empresa, ya que, el objetivo de la seguridad de la información es garantizar la continuidad del negocio y prevenir o minimizar el posible daño el impacto de los incidentes. Por esta razón, en lo fundamental las métricas en seguridad de la información están ligadas a la gestión

de riesgos ya que, en esencia, las decisiones de seguridad son decisiones de gestión de riesgos. Las métricas van a aportar luz en los tres niveles de decisión de la empresa: operativo, táctico y estratégico. Un ejemplo de esto es lo siguiente:

En el nivel estratégico los elementos a evaluar son: la administración de riesgos y el cumplimiento de objetivos de negocio. Particularmente en la identificación de activos a proteger, planes de actualización y seguimiento, mapas de riesgo y controles, entre otros.

En el nivel táctico los elementos a evaluar son: el perímetro, las aplicaciones y servicios. Particularmente en la medición de la efectividad del antivirus, la efectividad del Antispam, efectividad del monitoreo, entre otros.

En el nivel operativo los elementos a evaluar son: confidencialidad, integridad y disponibilidad de la información. Particularmente en accesos no autorizados, suplantación de IP o datos, contraseñas débiles, entre otros.

Las métricas nos ayudan a cuantificar un incidente de seguridad, para ello, nos podemos apoyar en Normas Internacionales como la ISO 27002 y la ISO 27004, esta última detalla las características de las métricas. Así como, las publicaciones especiales SP 800 del Instituto Nacional de Estándares y Tecnología donde se presentan los documentos de interés general relativos a la seguridad de la información y evaluación de riesgos.

Una vez descritos los anteriores conceptos, podemos comenzar con plantear los diferentes tipos de amenazas informáticas que pueden ir en contra de los sistemas informáticos de una empresa, y más aún, en contra de la estabilidad del negocio.

Amenazas informáticas:

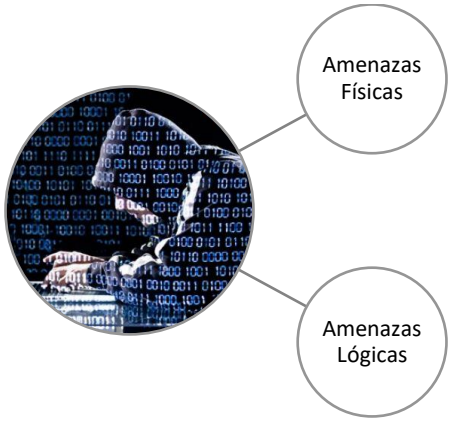

Figura 4. Tipos de amenazas cibernéticas. Fuente: elaboración propia con base en (Santos, 2014, pág. 32)

Amenazas físicas

Las amenazas físicas pueden definirse como aquellas que producen un daño o error en el hardware y pueden manifestarse en cualquier momento, provocando daños en: discos duros, procesadores, errores de funcionamiento de la memoria, entorpeciendo así la información aportada por estos. También se consideran amenazas físicas las catástrofes naturales y las hechas por el hombre de manera consciente. Algunos ejemplos de amenazas físicas son:

Empleados o exempleados

Existen diversos agentes que son causantes de los ataques informáticos, entre ellos, se encuentra el personal que labora en la misma empresa. Se tiene estimado que el 69% de las empresas ha experimentado un robo o intento de robo de datos por parte de sus empleados, de acuerdo con el estudio The State of Cybersecurity and Digital Trust 2016 elaborado por HFS para Accenture. Cabe mencionar que los empleados o incluso los exempleados son las personas con mayor conocimiento del negocio y de la importancia de la información que se maneja en ella, por lo que estos se convierten en sujetos potenciales de robo.

Hackers

Un hacker es una persona experta en programación que se dedica a ser intruso en sistemas informáticos para probar sus conocimientos como pasatiempo. Últimamente este término ha sido utilizado para referirse a personas que tienen propósitos maliciosos. El movimiento hacker surge en los años 1950 y 1960 en los Estados Unidos, con la aparición de las primeras computadoras.

Crackers (blackhats)

Es el término más preciso para referirse a personas dedicadas a atacar sistemas informáticos con el fin de obtener beneficios de forma ilegal, motivados por intereses económicos, políticos, etcétera. Los crackers pueden ayudarse de un *sniffer* que es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado equipo de cómputo. También pueden ser los responsables del envío masivo de miles de mensajes de correo electrónico, ocasionando que se colapsen los servidores y los buzones de correo de los usuarios. Esto con la finalidad de monitorear la información que ayuden a sus actos ilícitos.

Piratas informáticos

Los piratas informáticos son personas que se especializan en la reproducción, apropiación y distribución de software o contenidos digitales, con fines lucrativos y a gran escala, infringiendo la legislación de la propiedad intelectual.

Ingeniería social

La ingeniería social hace referencia a la manipulación de personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo. Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador.

Amenazas Lógicas

Las amenazas lógicas son principalmente software malicioso, también conocido como programa maligno (malware), que son creados con malas intenciones para dañar sistemas informáticos y obtener algún beneficio. Existen errores de programación denominados *bugs* y a los programas utilizados para aprovechar las vulnerabilidades de los sistemas y atacarlos se les denomina *exploits*.

Herramientas de seguridad

Las herramientas de seguridad pueden ser utilizadas por los administradores de red y seguridad de las empresas, para detectar vulnerabilidades y solucionar fallos en sus sistemas, sin embargo, estas herramientas también pueden ser utilizadas por los crackers que buscan información para atacar dichos sistemas. Algunas de esas herramientas son: NESSUS, SAINT o SATAN, que pasan de ser útiles a peligrosas.

Virus

Un virus es una secuencia de código que se inserta en un archivo ejecutable, de tal forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas. Los virus pueden causar daños a la información que almacena los sistemas informáticos y por lo tanto repercutir en la operación del negocio.

Gusano

Es un programa que se ejecuta por sí mismo a través de redes, el cual puede portar virus dañando los sistemas. Además, tiene un gran potencial de daño. Como en el caso de 1988, donde causo pérdidas millonarias al infectar y detener más de seis mil máquinas, este suceso se clasificó como el mayor incidente en su época.

Caballos de Troya

Los troyanos son instrucciones escondidas en un programa, aparentemente inofensivo, que funciona correctamente, ejecutando las tareas que el usuario espera

de él, sin embargo, realmente se están ejecutando tareas ocultas sin el conocimiento del usuario y que son potencialmente dañinas para los equipos.

Programas conejo o bacterias

Son programas que no tienen utilidad, se reproducen hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco duro), produciendo una negación del servicio.

Phishing

El phishing conocido como suplantación de identidad, es un modelo de abuso informático que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea.

Las amenazas anteriormente descritas son solo algunas de la gran diversidad que existe. Ahora bien, es crucial que en toda empresa privada o institución gubernamental se cuente con medidas específicas para disminuir estas amenazas potenciales, para esto, es necesario que se realice un análisis de las posibles pérdidas y la probabilidad de ocurrencia. Con el resultado del estudio se podrán crear políticas de seguridad y procedimientos para la realización de distintas tareas que sean preventivas y correctivas, orientadas a garantizar la protección de los sistemas y la red.

Algunas medidas podrían ser:

- Implementación de dispositivos como firewall que protejan la red empresarial

- Empleo de contraseñas para un mayor control de acceso a los sistemas
- Cifrado de datos en las comunicaciones
- Uso de software de seguridad (antimalware)
- Uso de software con licencia
- Realización de respaldos de seguridad
- Uso de hardware adecuado

Dado que las amenazas se pueden dividir en amenazas lógicas y amenazas físicas, los expertos en seguridad informática deben establecer las mejores estrategias adecuadas al ambiente de su organización.

1.5 La seguridad de la información en el mundo

En la actualidad los avances tecnológicos son cada vez mayores, generando un sinfín de oportunidades de desarrollo en diferentes sectores, por esta razón, los negocios en todo el mundo están experimentando un profundo proceso de digitalización; a su vez, este proceso demanda inversión en seguridad de la información y soluciones de privacidad, debido a que, como se ha descrito anteriormente, el resguardo de la información que genera una empresa es de suma importancia. La seguridad de la información se ha convertido en un tema cada vez más relevante para las empresas privadas e instituciones gubernamentales a nivel internacional, pues contar con un modelo de seguridad facilita el crecimiento del negocio, crea valor en el mercado y genera confianza de los clientes y sociedad en general. Este auge, se debe también a que en los últimos años se ha experimentado constantes ataques a los sistemas informáticos con el objetivo de dañar la información, sustraerla e interrumpir la operatividad, entre otros propósitos negativos, ocasionando innumerables pérdidas económicas.

Ahora bien, existen algunos organismos internacionales que de manera directa o indirecta están orientados a temas de seguridad de la información, como lo son:

- La Unión Internacional de Telecomunicaciones (UIT) como organismo de la Organización de las Naciones Unidas (ONU), está encargado de la creación de políticas y recomendaciones en el sector de las telecomunicaciones en donde participan las agencias gubernamentales de los miembros, además, tiene la encomienda de coordinar los esfuerzos internacionales en materia de ciberseguridad. En su portal de internet "The Cybersecurity Gateway" proporciona recursos e información relacionados con la ciberseguridad y el cibercrimen, así como iniciativas nacionales e internacionales en la materia con la participación de organismos internacionales, los sectores privado y público, instituciones académicas y organizaciones de la sociedad civil.

- La Organización para la Cooperación y el Desarrollo Económico (OCDE). Este organismo tiene como mandato discutir políticas públicas, buscar soluciones a problemas comunes entre sus miembros, identificar mejores prácticas y coordinar las políticas domésticas e internacionales en distintos sectores, incluyendo el área de tecnologías de información y comunicación. Durante la reunión Ministerial "El Futuro de la Economía Internet" celebrada en la ciudad de Seúl, Corea en junio de 2008 se llevó a cabo una mesa redonda titulada: "Building Confidence" en donde se trataron algunos aspectos sobre ciberdelincuencia y el robo de identidad en los países miembros de la OCDE, estas reuniones tienen como objetivo alertar a los países sobre nuevas prácticas maliciosas y apoyarse en el combate.

- El Consejo de Europa elaboró en 2001 el Convenio sobre Ciberdelincuencia o bien conocido como Convenio Budapest, el cual, es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. Además, este convenio establece la necesidad de crear una red de puntos o autoridades de contacto disponibles las 24 horas, los 7

días de la semana con el objeto de facilitar la cooperación internacional para la identificación de los delitos cometidos en la red.

- La Organización Internacional de Policía Criminal (INTERPOL) es la organización internacional mundial de policía de la cual forman parte 192 países y cuya misión principal es facilitar la cooperación policial transfronteriza. INTERPOL trabaja muy de cerca con los organismos internacionales en el monitoreo de conductas ilícitas en internet y coadyuva con las autoridades ejecutoras de le legislación de cada país para ayudar a prevenir y combatir la delincuencia a nivel internacional. También, tiene como una de sus prioridades combatir los delitos financieros y aquellos que se derivan del uso de las nuevas tecnologías.

- La Organización de los Estados Americanos (OEA) es un organismo multilateral que busca servir de foro para el diálogo y la toma de decisiones, así como propiciar relaciones más fuertes entre los distintos pueblos y naciones del continente. Entre los objetivos de la OEA, podemos destacar el fortalecimiento y mantenimiento de la paz en la región, la consolidación del sistema democrático, y la promoción de los derechos humanos. Asimismo, la OEA está orientada a promover el desarrollo, tanto económico como social, del continente, y a favorecer el desarrollo sustentable en los países de la región. Cuenta con un grupo de expertos intergubernamental sobre delito cibernético cuya información se disemina a través de un portal titulado: “Portal Interamericano de Cooperación en Materia de Delito Cibernético.” El mandato principal de dicho grupo de expertos es hacer un diagnóstico de la actividad delictiva vinculada a las computadoras y la información en los Estados miembros; hacer un diagnóstico del estatus de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad; identificar las entidades nacionales e internacionales que tienen experiencia en la materia; e implementar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

- Foro de Cooperación Económica Asia-Pacifico (APEC), en este organismo se tiene conformado un grupo de trabajo denominado: Grupo de Trabajo sobre Seguridad Electrónica (APEC TEL e-Security Task Group) cuyo mandato incluye la elaboración de políticas y recomendaciones, así como la implementación y el monitoreo de proyectos para fomentar la cooperación internacional y regional con otros organismos en materia de seguridad y ciberdelincuencia. En el 2002, APEC lanzó su "Estrategia en materia de Ciberseguridad (APEC Cybersecurity Strategy)" que consiste en un paquete de medidas y recomendaciones para proteger a las empresas y consumidores del cibercrimen y reforzar la confianza en el consumidor al utilizar el internet y llevar a cabo transacciones de comercio electrónico.

En resumen, todos estos organismos creados a nivel internacional y por regiones comparten el objetivo de generar iniciativas que refuercen la seguridad de la información en la red y combatir los ciberdelitos.

Se reconoce que cada vez existe mayor dependencia del uso de redes, dispositivos y servicios de las tecnologías de la información y comunicación, debido a que muchos servicios básicos de la vida cotidiana se sustentan en tecnología, por lo tanto, el crecimiento de la ciberseguridad ha sido proporcional al auge tecnológico. Sin embargo, existe una brecha evidente entre los países, en cuanto al conocimiento y capacidades de desplegar las estrategias y programas adecuados para garantizar el uso adecuado de las tecnologías de la información y comunicación.

La Unión Internacional de Telecomunicaciones (UIT) en su informe "Global Cybersecurity Index 2017" (Union International Telecommunication, 2017, pág. 13) evaluó el nivel que tienen los países en cuanto a participación en ciberseguridad, el cual, se basó en cinco pilares:

1. Legal: Se basa en la existencia de instituciones y un marco jurídico que traten con la ciberseguridad y cibercrimen.

2. Técnico: Se basa en la existencia de instituciones técnicas y marcos orientados a tratar la ciberseguridad.
3. Organizacional: Se basa en la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a nivel nacional.
4. Desarrollo de capacidades: Se basa en la existencia de investigación y desarrollo, educación y programas de entrenamiento; profesionales certificados y agencias del sector público que fomentan la creación de capacidades.
5. Cooperación: se basa en la existencia de asociaciones, marcos de cooperación y redes de intercambio de información.

La evaluación fue aplicada a un total de 193 países, en la figura 5 se puede observar el posicionamiento que tiene México frente a los compromisos cibernéticos, siendo el color verde el nivel de compromiso más alto y el color rojo el nivel de compromiso más bajo, como se aprecia a continuación:

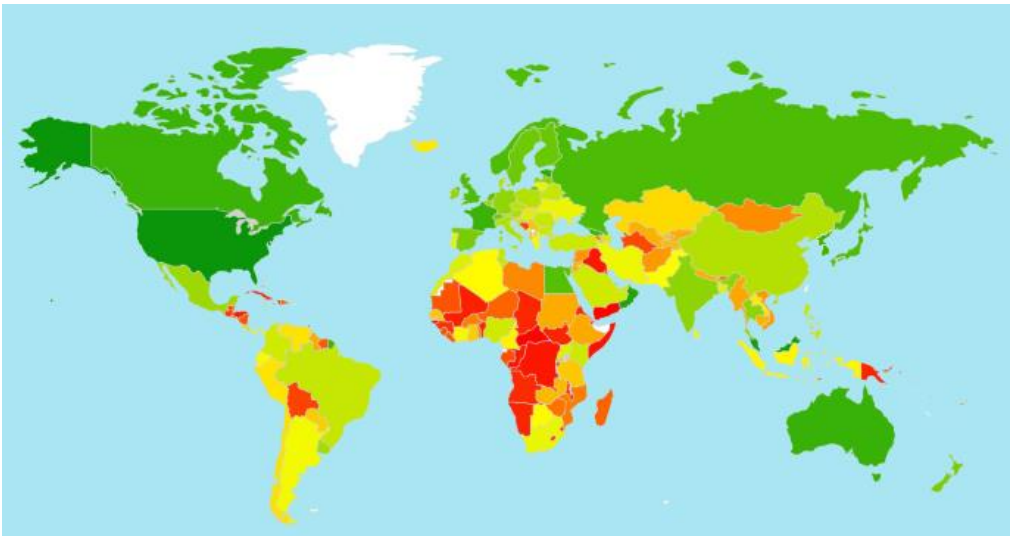

Figura 5. Mapa de ciberseguridad mundial. Fuente: (Union International Telecommunication, 2017, pág. 13)

La etapa de inicio corresponde a 96 países que comienzan a hacer compromisos de ciberseguridad, entre los que destacan: Afganistán, Cuba, El Salvador, Liberia, Mongolia, Somalia, Yemen, entre otros.

La etapa de maduración corresponde a 76 países, los cuales han desarrollado compromisos complejos y participan en programas e iniciativas de ciberseguridad, en esta etapa se encuentra México, al igual que: Argentita, Australia, Brasil, Israel, Nigeria, Portugal, Sudáfrica, entre otros.

Finalmente, en la etapa principal se encuentran 21 países, como se muestra en la tabla 1, que demuestran un alto compromiso en los cinco pilares (legal, técnico, organizacional, desarrollo de capacidades y cooperación), los cuales son:

Países líderes en ciberseguridad		
Australia	Corea	Rusia
Canadá	Malasia	Singapur
Egipto	Republica de Mauricio	España
Estonia	Países Bajos	Suecia
Finlandia	Nueva Zelanda	Suiza
Francia	Noruega	Reino Unido
Georgia	Omán	Estados Unidos
Japón		

Tabla 1, Países líderes en ciberseguridad. Fuente: (Union International Telecommunication, 2017, pág. 15)

Los esfuerzos que hacen los países en materia de ciberseguridad para cumplir con normas, programas, capacitación técnica, entre otros aspectos, pueden demandar no sólo recursos financieros, sino humanos, materiales y, sobre todo, un esfuerzo de la sociedad en general.

La búsqueda de mayor y mejor ciberseguridad radica en el equilibrio de los cinco pilares, siendo de suma importancia la generación de una estrategia que incluya a nivel nacional, el sector público, privado y la sociedad en general, haciéndolos más conscientes de la ciberseguridad en las telecomunicaciones.

Para este estudio se destaca la posición de México en la región de América, el cual ocupa el tercer lugar con una brecha considerable con respecto a los primeros lugares, que son ocupados por Estados Unidos y Canadá, como se muestra en la tabla 2.

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	0.91	1	0.96	0.92	1	0.73
Canada	0.81	0.94	0.93	0.71	0.82	0.70
Mexico	0.66	0.91	0.89	0.48	0.68	0.34

Tabla 2, Posicionamiento en Ciberseguridad en la Región de América. Fuente: (Union International Telecommunication, 2017, pág. 28)

Se observa en la tabla anterior, que los tres países destacan en los pilares legal y técnico, por ejemplo: Estados Unidos destaca con el centro de recursos para la ciberseguridad nacional, Canadá destaca por las características de protección de información personal y documentos electrónicos, y México destaca por la incorporación de aspectos de ciberseguridad a la legislación, cubriendo la criminalidad, la protección de datos, privacidad de datos y transacciones electrónicas. Sin embargo, México tiene una gran área de oportunidad en la generación de conciencia y cultura en seguridad de la información, ya que, presenta un puntaje bajo para el pilar de *desarrollo de capacidades,* el cual, contempla las prácticas para el aumento de recursos técnicos y humanos que combatan el delito cibernético. Esto incluye crear conciencia sobre la ciberseguridad entre el público, la existencia de estándares de seguridad cibernética y cuerpos de estándares, guías de mejores prácticas, iniciativas de educación e investigación y desarrollo.

Por otra parte, hay esfuerzos como los realizados por Dinamarca, Finlandia, Islandia, Noruega y Suecia, en los que se ayudan, a través de la colaboración Nórdica Nacional del Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team), donde incluyen ejercicios de cooperación técnica y ciberseguridad para evaluar y fortalecer la preparación cibernética, examinar procesos de respuesta a incidentes y mejorar el intercambio de información en la región. Siendo una muestra clara del creciente compromiso que los países están adquiriendo en materia de seguridad de la información. Sin embargo, a pesar de que en los últimos años a nivel mundial existe un mayor acceso

a internet y aumento en desarrollos tecnológicos, esto no implica que forzosamente mejore la ciberseguridad, principalmente en los países con economías en desarrollo.

1.6 La ciberseguridad y sus tendencias

Antes de comenzar, es importante destacar la diferencia entre seguridad de la información y ciberseguridad. El primer concepto tiene un alcance mayor ya que busca proteger la información en todo su ciclo; desde su generación, clasificación, representación, almacenaje, recuperación, distribución y uso. Es decir, se sustenta en metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos que soportan la idea de protección en las distintas facetas de la información de una manera integral. Por otro lado, la ciberseguridad se enfoca en cómo se va a proteger la información digital existente, dicho de otra manera, se orienta a las estrategias técnicas y tácticas de seguridad informática que se llevan a cabo con el fin del resguardo de la información.

La digitalización de los negocios ha marcado tendencia y aumenta la oportunidad de desarrollo de las empresas; sin embargo, en esta transición las empresas pueden hacerse vulnerables a los ataques cibernéticos lo que ocasiona que se encuentren en la mira los activos digitales críticos de las empresas.

Existen factores que han propiciado el aumento de la ciberseguridad, algunos de ellos son:

- Aumento de confianza en la tecnología, las empresas comienzan a apostarle a los negocios digitales.[1]
- Existe mucha información: legal, sociocultural, económica, geopolítica, entre otras, que necesita ser procesada por las empresas y, a su vez, resguardada de agentes internos o externos que quieran hacer mal uso de ella.
- Hay un incremento de las operaciones y transacciones digitales.

[1] Un negocio digital usa la tecnología para crear nuevo valor sobre los modelos de negocio, experiencias de clientes y capacidades internas que soportan el núcleo de las operaciones.

- Constantemente se crean nuevas amenazas a los sistemas cibernéticos pertenecientes a instituciones gubernamentales o privadas.

Ahora bien, la transformación que han experimentado las empresas por a la implementación de la tecnología digital en sus operaciones, ha propiciado un panorama favorable a la inversión en ciberseguridad.

En la encuesta *The Global State of Information Security* se refleja que el presupuesto que las empresas destinan a ciberseguridad casi se ha duplicado, pasando de 2.8 a 5.1 millones de dólares (PwC, 2017). Esto se debe en gran medida a que muchas organizaciones han comenzado a abandonar la idea de ver a la ciberseguridad como un gasto innecesario, por el contrario, se comienza a percibir como una solución que puede facilitar el crecimiento del negocio, crear ventajas en el mercado y construir confianza en la marca.

Cada vez más productos, dispositivos y servicios se conecten a internet, como parte de la estrategia que muchas empresas están adoptando, este hecho, aumenta el riesgo de tener vulnerabilidades o sufrir amenazas de ciberseguridad, por lo que la seguridad de la información se ha convertido en un factor crítico para los negocios. Las empresas comienzan a generar estrategias de seguridad adaptables a los riesgos y amenazas, por lo que se están orientando a la adopción de soluciones de análisis de datos y monitoreo en tiempo real, servicios de seguridad administrados y software de código abierto.

La encuesta realizada a directivos y responsables de TI de todo el mundo (Figura 6), también refleja que la tendencia de inversión en ciberseguridad es la siguiente:

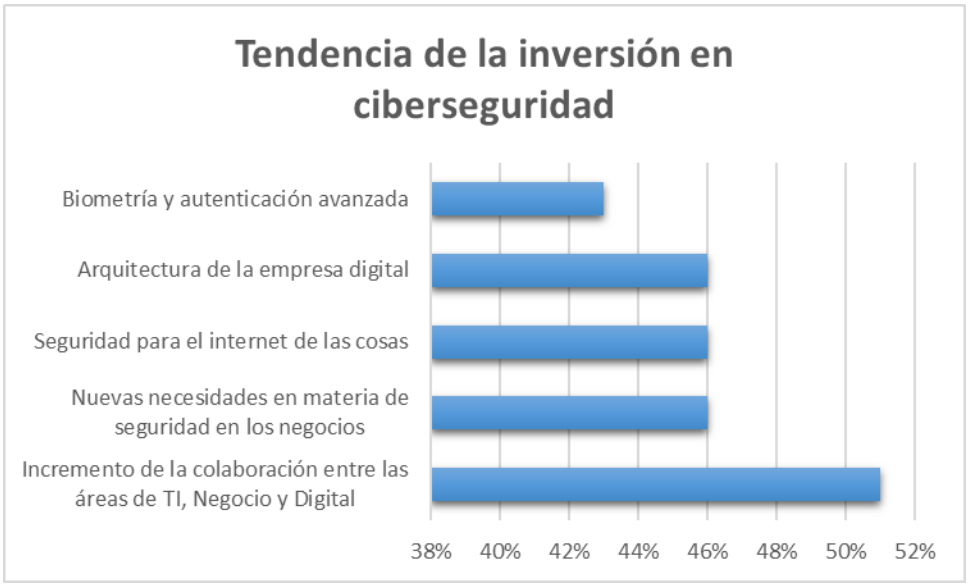

Figura 6. Tendencia de la inversión en ciberseguridad. Fuente: elaboración propia con base en (PwC, 2017)

De acuerdo con la publicación más reciente de la encuesta “The Global State of Information Security”, en la actualidad las empresas de todo el mundo sufren aproximadamente 3.4 incidentes de seguridad al año y pérdidas de 4.8 millones de dólares. Asimismo, se menciona que el 47% de los ciberataques que tienen origen dentro de la compañía son realizados por empleados o exempleados y el 40.7% por proveedores. Estas cifras tan altas justifican la creación e implementación de una cultura en seguridad de la información que sea adoptada por todos los empleados, para lo cual, la estrategia que se ejecute comenzará siempre con la concientización.

De esta manera, poco a poco las empresas, principalmente los grandes corporativos, comienzan a comprender la necesidad de la ciberseguridad y cómo las soluciones de TI pueden facilitar el crecimiento del negocio y crear ventajas competitivas. Además, estas compañías están integrando ciberseguridad, privacidad y ética digital desde un principio, lo que les permite interactuar de mejor manera con sus clientes y atraer nuevos.

Actualmente, derivado del proceso de digitalización de los negocios las empresas están incluyendo a su estrategia de seguridad: cifrado de datos, firewalls de nueva generación, segmentación de red e identidad y gestión de acceso.

Conforme a la encuesta “The Global State of Information Security” (PwC, 2017) existen cinco principales prácticas en materia de ciberseguridad:

Figura 7. Prácticas de ciberseguridad. Fuente: (PwC, 2017)

Almacenamiento en la nube: El almacenamiento basado en la nube puede ser más seguro y menos costoso para las empresas, ya que no necesitan gastar grandes cantidades en infraestructura. Se están almacenando procesos de negocio críticos y funciones como contabilidad, finanzas, operaciones y recursos humanos.

Apoyo externo: Empresas con recursos limitados optan por contratar los servicios de administración de la seguridad de manera externa; de acuerdo con la encuesta “The Global State of Information Security” (PwC, 2017) el 67% de los encuestados mencionaron hacer uso de proveedores de servicios de seguridad para operar y mejorar sus programas de ciberseguridad.

Algunos de los factores que propician esta tendencia son los pocos recursos financieros con los que puede contar una empresa y la escasez mundial de especialistas en ciberseguridad calificados, por consecuencia resulta muy costoso tener un equipo integral de seguridad cibernética de tiempo completo en la empresa.

Técnicas de data analytics: En cuanto a la detección de amenazas y ataques, los sistemas de análisis de datos avanzados y en tiempo real están ganando peso entre las empresas, esto de acuerdo con el 51% de los directivos encuestados en “The Global State of Information Security” (PwC, 2017). Hacerlo, no obstante, supone un desafío muy importante para las empresas por la gran cantidad de datos que debe almacenar y procesar, así como por el uso de sofisticados algoritmos y

por la escasez de los perfiles profesionales adecuados. Un punto en contra es la falta de profesionales especializados en Big Data, por lo que nuevamente recurren a la contratación de grandes proveedores de servicios.

Uso de sistemas de Autenticación: La falta de prácticas de contraseñas sólidas por parte de los usuarios, hace que las empresas recurran a la autenticación avanzada, con el fin de agregar una capa adicional de seguridad. En la encuesta "The Global State of Information Security" (PwC, 2017) el 57% de los directivos mencionó la utilización de autenticación biométrica. Asimismo, el 46% de organizaciones que emplean autenticación avanzada dijeron que ha hecho que las transacciones en línea sean más seguras, aumentando la confianza del cliente.

Uso de software de código abierto: La adopción de software de código abierto representa un cambio importante en la forma en que las organizaciones desarrollan y ejecutan soluciones locales y entregan servicios, ya que, se han mejorado notablemente los programas de seguridad de las empresas.

Los directivos encuestados en "The Global State of Information Security" (PwC, 2017) también mencionaron tener prioridades de ciberseguridad para el año 2018, enlistándolas de mayor a menor, son:

- Prioridades de entrenamiento y concientización.
- Prioridades de políticas y procedimientos.
- Prioridades de evaluaciones.
- Prioridades de respuesta a incidentes.

Por otra parte, en el artículo "Cibersecurity: construyendo una confianza en el entorno digital" (PwC, 2016) se mencionan algunas tendencias en prácticas de valor, para ser aplicadas por los responsables de la seguridad de la información en las empresas:

- Establecer prioridades: proteger los activos de hardware y software más importantes.
- Construir inteligencia basada en la información que se posee: respuesta a incidentes, monitoreo y detección.

- Maximizar el retorno de la inversión de la tecnología: aplicación de inteligencia de seguridad y administración de acceso e identidades.
- Construir una estrategia que genere confianza digital y cumplir con las regulaciones de privacidad.
- Construir y mantener una cultura de seguridad: gestión de amenazas internas.

Con la información anterior, se puede observar nuevamente que, dentro de las tendencias, se encuentra la creación de una cultura en seguridad de la información, la cual, ya está contemplada por en el Gobierno Mexicano dentro de la Estrategia Digital Nacional y la Estrategia Nacional de Ciberseguridad creada en 2017.

Capítulo 2. La seguridad de la información en Instituciones Gubernamentales

La situación de la seguridad de la información en las instituciones gubernamentales en México es un reflejo de las estrategias y sus resultados que implementa el gobierno federal y que a su vez emanan del Plan Nacional de Desarrollo, los siguientes dos subtemas están encaminados a conocer primeramente el contexto de la seguridad de la información en México y su marco legal, de esta manera será más fácil comprender el escenario que tienen estas instituciones.

2.1 La Seguridad de la Información en México

México ocupa el lugar 28 en ciberseguridad de acuerdo con el *Informe Global Cibersecurity 2017* (Union International Telecommunication, 2017) y el lugar número tres en América con una puntuación de .66 y una brecha de 26 puntos con respecto al primer lugar de la región, Estados Unidos.

El *Índice mundial de ciberseguridad y perfiles de ciber bienestar del 2015* (Unión Internacional de Telecomunicaciónes, 2015, pág. 328) proporciona el perfil que tiene México en temas de ciberseguridad, el cual, se muestra a continuación:

Legislación
• El cibercrimen se ha promulgado en el Código Penal Federal
Medidas Técnicas
• México cuenta con un Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT, del inglés Computer Security Incidente Response Team), conocido como CERT-MX que es el Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal. El CERT-MX se encarga de prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país. • México exige el cumplimiento de los requisitos de la norma ISO 27001 para un sistema de gestión de seguridad de la información de todas las instituciones gubernamentales, por medio de las normas NMX-I-27001-NYCE-2015 y NMX-I-27002-NYCE-2015.

- En México no existe un marco de ciberseguridad para la certificación y acreditación de agencias nacionales y profesionales del sector público.

Medidas de organización

- Creación del Comité Especializado de Seguridad de la Información para desarrollar una estrategia nacional para seguridad de la información, que guie todas las acciones que debe emprender el gobierno federal.
- La policía federal de México posee una estrategia de ciberseguridad
- No hay proyectos o programas para investigación y desarrollo de estándares de ciberseguridad y mejores prácticas.
- El personal de la división científica ha recibido capacitación especializada del Sistema de Desarrollo Policial de México (SIDEPOL).
- México no cuenta con agencias certificadas del gobierno bajo estándares reconocidos internacionalmente en ciberseguridad.

Cooperación

- No hay información sobre ningún marco para compartir activos de ciberseguridad con otros países.
- México comparte activos de ciberseguridad en programas nacionales por medio de las autoridades del Comité Especializado de la Seguridad de la Información (CESI). También se desarrolló un protocolo de colaboración entre CERT-MX y las diversas dependencias del gobierno central mexicano para abordar y responder a incidentes cibernéticos.
- México es miembro de La Organización de los Estados Americanos (OEA) y participa en su Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) y del Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST), con el fin de facilitar la participación en plataformas y foros de ciberseguridad regional / internacional.

Protección para niños en línea

- México se ha adherido a los artículos 16, 17 (e) y 34 (c) de la Convención sobre los Derechos del Niño, y a los artículos 2 y 3 del Protocolo Facultativo de la Convención sobre los Derechos del Niño sobre la Venta de Niños, la Prostitución Infantil y la Pornografía Infantil.
- El departamento de seguridad pública, difunde información sobre ciber amenazas.
- La alianza de seguridad para México brinda espacio para quejas en su sitio web, así como correo y números de contacto.

Tabla 3, Perfil de México en ciberseguridad. Fuente: elaboración propia con base en (Unión Internacional de Telecomunicaciónes, 2015, pág. 328)

Por otra parte, existen datos como los publicados en el informe *Tendencias de Seguridad Cibernética en América Latina y el Caribe* (Organización de los Estados Americanos, 2014), en el cual, se estima que los costos inherentes a la comisión de los delitos informáticos alrededor del mundo ascendieron a 113,000 millones de dólares y en México representaron 3,000 millones dólares.

Además, de acuerdo con la *Estrategia Nacional de Ciberseguridad 2017* en México el número de incidentes cibernéticos identificados, se ha triplicado de 2013 a 2016, pasando de cerca de 20 mil incidentes a más de 60 mil; mientras que la presencia de sitios web apócrifos con fines de fraude, se incrementó un 11 por ciento entre 2015 y 2016, llegando a cerca de 5 mil; la propagación de virus informáticos con afectaciones en México creció un 57 por ciento de 2015 a 2016, llegando a cerca de 40 mil eventos, de lo cual, se destaca el grado de sofisticación utilizado por los ciberdelincuentes en algunos de los casos.

Con los datos anteriores se concluye que, sin bien, México tiene una gran brecha en ciberseguridad con respecto a países con economías más desarrolladas, se han realizado en la administración pública varias acciones encaminadas a reducir dicha brecha, otorgándole el tercer lugar en el continente americano y el primer lugar en ciberseguridad en América latina. El camino de romper con los paradigmas, de crear un gobierno digital y generar mayor conciencia y cultura en seguridad de la información, ya comenzó para México. Ahora, parte de los esfuerzos técnicos,

humanos y financieros se están trasladado a la implementación y ejecución de las acciones convenidas, adicionalmente habría que vigilar la correcta ejecución para asegurar su continuidad.

2.2 Marco legal de la seguridad de la información en México

Con el auge de las tecnologías de la información se ha tenido la necesidad de regular en materia jurídica los actos relacionados con los sistemas informáticos y por consecuencia la información que se genera procesa y transfiere por medios de estos sistemas.

En el ámbito de la seguridad de la información, existen algunos requisitos que las empresas deben cumplir de manera obligatoria, por ejemplo, las legislaciones relacionadas con la protección de datos personales de los usuarios o clientes, así como la protección de la información propia o de terceros. Como ya se ha explicado anteriormente, hay información sumamente sensible que es generada y procesada por las organizaciones de los diferentes sectores, principalmente del sector financiero, por lo que adoptan medidas de protección informática como la adquisición de dispositivos especializados en seguridad de datos que son conectados a la red empresarial y la contratación de profesionales en la materia.

También se ha vuelto relevante, en los últimos años, la adopción de estándares de seguridad ya sea por voluntad propia o por cumplimiento de algún requisito contractual o regulatorio. En este sentido, la norma ISO/IEC 27001 es un estándar internacionalmente utilizado para gestionar la seguridad de la información, su implementación debe realizarse en función de las características, necesidades y condiciones de cada empresa. Dicha norma se basa en dos principios básicos los cuales son: la alineación de la organización con un sistema de gestión de la información y un conjunto de objetivos de controles de seguridad.

Desde la aparición del derecho a la privacidad como parte de la Declaración de los Derechos Humanos, el cual establece que ninguna persona debe ser objeto de injerencias arbitrarias a su condición intima, todo esto se vuelve complejo, ya que la información personal se maneja cada vez más de manera digital, resultando difícil la búsqueda de un balance entre la intimidad de los individuos y el manejo de su información. Es por lo que los últimos años y hasta el 2014, más de cien países han adoptado leyes de privacidad y protección de datos en posesión de gobiernos y empresas privadas.

En México, se ha trabajado para la adecuación del marco jurídico en la aplicación de los sistemas informáticos, en cuanto a la seguridad de la información, que soportan las operaciones federales y las realizadas por cualquier empresa privada en donde se maneje información. Como consecuencia, ha surgido legislación para la protección en materia de propiedad industrial y derechos de autor, expresada por la Ley de Propiedad Industrial, la Ley Federal de Derechos de Autor y el Código Penal Federal en donde se establece, en su título noveno, las posibles conductas constitutivas de delito en la materia, así como las sanciones a quienes accedan de manera ilícita a sistemas y equipos de informática. Asimismo, se creó, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Transparencia y Acceso a la Información Pública, en respuesta a la creciente demanda de mayor seguridad y transparencia en las operaciones que realizan los particulares y el estado.

En México existen diversas disposiciones aplicables, relacionadas con los sistemas informáticos y la información que operan, algunos ejemplos son:

- Código de Comercio, artículos 30 bis, 80 y 89
- Ley de Instituciones de Crédito, articulo 52
- Ley Federal de Protección al Consumidor, Articulo 1 fracción VIII
- Código Civil, artículos 1803 y 1811

Lo que se pretende con la legislación anterior, es sentar las bases para validar los actos jurídicos que se realizan con medios informáticos.

También existen disposiciones que impulsan la protección de derechos de propiedad intelectual y los derechos de autor de los sistemas informáticos, tales como:

- Ley de Propiedad Industrial, artículo 178 bis
- Ley Federal del Derecho de Autor, artículos 101 al 107 y del 110 al 114
- Código Penal Federal, articulo 426

Con esta legislación se busca resguardar la propiedad intelectual y establecer los delitos en los que incurriría el individuo que obtenga acceso no autorizado a la misma y realice actos lucrativos.

En el sector financiero hay regulaciones específicas que tienen que cumplir los sistemas informáticos de las instituciones bancarias, cuyo cumplimiento es exigido por la Comisión Nacional Bancaria y de Valores (CNBV) como son: la circular única de bancos en el capítulo X, las establecidas en las Disposiciones de carácter general aplicables a las instituciones de crédito, o el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI DSS, entre otros.

En cuanto a los sistemas informáticos como fuente de acceso a la información gubernamental, se creó la Ley de Transparencia y Acceso a la Información Pública Gubernamental, con la finalidad de garantizar el acceso a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal y cualquier otra entidad federal. En este caso, los sistemas informáticos juegan un papel crucial para las dependencias y entidades que operan un gran flujo de información a través de medios electrónicos.

Existen disposiciones donde el gobierno utiliza procesos informáticos legales, algunas muestras son:

- Ley de Adquisiciones, Arredramientos y Servicios del Sector Público, articulo 27
- Ley de Obras Públicas y Servicios relacionados con las mismas, articulo 28
- Ley de Responsabilidades Administrativas de los Servidores Públicos, articulo 38

Asimismo, también se creó el *Acuerdo por el que se reforma y adiciona el diverso por el que se establecen las disposiciones administrativas en materia de tecnologías de la información y comunicaciones y de seguridad de la información*, y se expide el Manual Administrativo de Aplicación General en esas materias. DOF: 22/08/2012. Este acuerdo se refiere conforme a su artículo primero a establecer las reglas, acciones y procesos que en materia de tecnologías de la información y comunicaciones deberán observar de manera obligatoria, las dependencias y entidades de la Administración Pública Federal y, cuando corresponda, la Procuraduría General de la República.

Otro claro ejemplo del uso de los sistemas informáticos y la seguridad de la información en el ámbito gubernamental, son los servicios que ofrece, así como la forma de operar del Servicio de Administración Tributaria (SAT), el uso de la firma electrónica, la presentación de declaraciones de impuestos y diversos trámites se realizan por medios electrónicos.

Cabe señalar que hay requisitos y documentación que establece cada institución, lo cual está encaminado a la seguridad de la información como: manuales de organización, manuales de procedimientos, políticas y reglamentos internos que buscan reforzar la integridad, disponibilidad y confidencialidad.

2.3 Las Tecnologías de la Información en las Instituciones Gubernamentales Mexicanas.

El Gobierno Federal en el Plan Nacional de Desarrollo manifestó, su interés en generar acciones orientadas al fortalecimiento de las Tecnologías de la Información y Comunicación, para que contribuyan a que se potencialicen diferentes sectores de la economía. En la figura 9 se puede observar un esquema del Plan Nacional de Desarrollo donde se puntualiza la estrategia: Gobierno Cercano y Moderno, la cual, tiene por objetivo: "Establecer una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las tecnologías dela información y la comunicación, e impulsar un gobierno eficaz que inserte a México en l Sociedad del Conocimiento" (Gobierno de la República Mexicana, 2013).

FIGURA 1.1. ESQUEMA DEL PLAN NACIONAL DE DESARROLLO 2013-2018.

Figura 8, Esquema del Plan Nacional de Desarrollo 2013-2018. Fuente: (Gobierno de la República Mexicana, 2013)

Del Plan Nacional de Desarrollo se desprende el Programa para un Gobierno Cercano y Moderno, en el cual, el objetivo 5 establece la Estrategia Digital Nacional en la que se busca fomentar la adopción y desarrollo de las TIC´s para el apoyo de las funciones de la Administración Pública Federal, a su vez facilita la transparencia

y rendición de cuentas en el ejercicio de los recursos públicos. A continuación, se muestra en la figura 10 un esquema de la Estrategia Digital Nacional.

Figura 9, Objetivos de la Estrategia Digital Nacional. Fuente: (Secretaría de la Función Pública, 2017).

Con la Estrategia Digital Nacional se estableció la Ventanilla Única Nacional para los Trámites e Información del Gobierno a través del portal de Internet www.gob.mx, el cual propició la interoperabilidad de los sistemas electrónicos de las instituciones públicas. Esta medida originó un gran esfuerzo en la Administración Pública, ya que, se requirieron mejores sistemas informáticos y, por lo tanto, una mejor gestión de la información que puede traer varias ventajas, como mejor acceso a la información pública, mayor agilidad en los trámites, transparencia en los recursos y, en conclusión, un mejor servicio a la ciudadanía.

A su vez, esta estrategia digital conllevó a la creación de políticas en tecnologías de la información y comunicación, así como en seguridad de la información, muestra de ello son las siguientes:

- Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.
- Contrato Marco para la adquisición de Licencias de Software de diversas funcionalidades y la prestación de servicios de implementación y de soporte técnico.
- Ley de Firma Electrónica Avanzada, su reglamento y sus disposiciones generales.
- Código de comercio, código civil federal, Norma Oficial Mexicana, NOM-151-SCFI-2016, Ley Federal de Protección al Consumidor.

Asimismo, cabe resaltar que se realizaron otras acciones para impulsar el uso de las tecnologías, como convertir en un derecho constitucional el uso de las TIC y garantizar el acceso a Internet, establecido en el artículo 6, párrafo tercero de la Constitución Política de los Estados Unidos Mexicanos, el establecimiento por ley de una Política Universal de Inclusión Digital en el artículo 3, fracción XLIII de la Ley Federal de Telecomunicaciones y Radiodifusión y la creación del Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, el cual, tiene por objeto: “Crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, cuyo fin será promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones, mediante la adecuada coordinación de las acciones que al efecto proponga la Secretaría de la Función Pública, con las dependencias de la Administración Pública Federal y, a través de éstas, con las entidades paraestatales” (Secretaría de la Función Pública, 2017).

Adicionalmente, la Estrategia Digital Nacional cuya finalidad es impulsar la digitalización de México, a través de acciones como: gobierno digital, datos abiertos, inclusión y habilidades digitales, servicios de salud y educación a través de las TIC,

el uso de TIC en servicios financieros, entre otras, originó que en todas las agencias gubernamentales las tecnologías se actualicen regularmente, se realicen copias de seguridad y se adhieran a las disposiciones del Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), el cual se desarrolló con base a normas internacionales como ISO 27001, *Information Technology Infrastructure Library (ITIL)* y *Control Objectives for Information and Related Technology (COBIT)*, entre otras. Por otra parte, están en marcha planes de redundancia digital.

En esta misma línea el Gobierno Federal creó, en noviembre de 2017, la Estrategia Nacional de Ciberseguridad, la cual establece cuatro Objetivos Estratégicos y ocho Ejes Trasversales como se muestra en la figura 8.

Figura 10, Objetivos de la Estrategia Nacional de Ciberseguridad. Fuente: (Gobierno de la República Mexicana, 2017)

El eje transversal que contempla el enfoque de este estudio es: Concientización, Cultura de ciberseguridad y prevención; este eje se refiere al conjunto de valores, principios y acciones en materia de concientización, educación y formación, que se

llevan a cabo por la sociedad, academia, sector privado e instituciones públicas, que inciden en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible. La cultura de ciberseguridad abonará al cumplimiento de los cinco objetivos estratégicos, mediante el desarrollo de políticas públicas, estrategias, programas, proyectos, acciones e iniciativas que:

- Contribuyan a la promoción, cumplimiento y protección de los derechos de individuos y organizaciones públicas y privadas, con énfasis en la protección de niñas, niños y adolescentes en el ciberespacio y sus derechos.
- Favorezcan el máximo aprovechamiento y uso responsable de las tecnologías de la información y comunicación, la convivencia armónica y el desarrollo de actividades en el ciberespacio.
- Incentiven la innovación y la economía para el desarrollo sostenible.
- Fortalezcan la prevención de riesgos y conductas delictivas que afectan a individuos, organizaciones privadas y públicas.
- Incrementen la confianza y continuidad de los servicios y trámites digitales públicos y privados.
- Contribuyan a la prevención de riesgos que pudieran afectar a las infraestructuras críticas de información y operación.
  (Gobierno de la República Mexicana, 2017)

La creación de la Estrategia Nacional de Ciberseguridad es una muestra del esfuerzo del Gobierno Mexicano para generar una cultura de seguridad de la información que se implemente a nivel nacional e impacte en el sector privado y público. Desde inicios del actual sexenio (2013-2018), el reto ha consistido en la implementación, ejecución y control de los recursos técnicos, humanos y financieros que se requieren para que todas las instituciones gubernamentales se coordinen y puedan cumplir con los objetivos de la estrategia.

Ahora bien, para conocer la situación de las tecnologías de la información y comunicación de la administración pública, la Auditoría Superior de la Federación emitió en febrero de 2016 un informe especial denominado: “Estudio General sobre las Tecnologías de la Información y Comunicaciones en la Administración Pública Federal”. Dicho estudio abarcó los Poderes Ejecutivo, Legislativo y Judicial, así como Órganos Constitucionales Autónomos a nivel Federal, con un total 265 entidades evaluadas, permitiendo diagnosticar la situación de las TIC en las instituciones participantes, así como identificar áreas de oportunidad relevantes. En el estudio se evaluaron aspectos de infraestructura y presupuesto de TIC, así como la implementación de mejores prácticas tomando como marco de referencia COBIT 5.0 *(Control Objectives for Information Systems and related Technology)*[2]. A continuación, se muestran los resultados más relevantes de ambos aspectos evaluados.

1. Sección de infraestructura; Los resultados de esta sección evaluada reflejan carencia de estrategias, debido a la desproporción del aprovechamiento en los recursos humanos, financieros y tecnológicos. Una muestra de esta desproporción se observa en la figura 11, en donde se plasma el número de concentración de servidores (físicos y virtualizados) promedio por cada Centro de Datos reportados en la Administración Pública Federal.

[2] COBIT es el marco aceptado internacionalmente como una buena práctica para el control de la información, Tecnologías de la Información y los riesgos que conllevan. Mantenida por ISACA (Information Systems Audit and Control Association) y el IT GI (IT Governance Institute). COBIT se utiliza para implementar el gobierno de TI y mejorar los controles. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

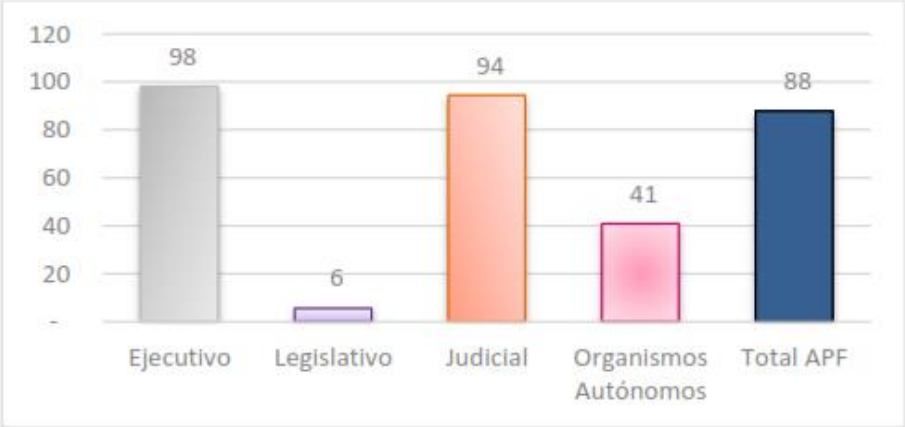

Figura 11, Servidores por Centro de Datos. Fuente: (Auditoría Superior de la Federación, 2016, pág. 2)

Asimismo, en la figura 12 se observa el nivel de virtualización como el porcentaje de servidores físicos y virtuales respecto al total de servidores de una entidad. Hay que tomar en cuenta que un mayor nivel de virtualización lleva a un mejor aprovechamiento en las capacidades de cómputo.

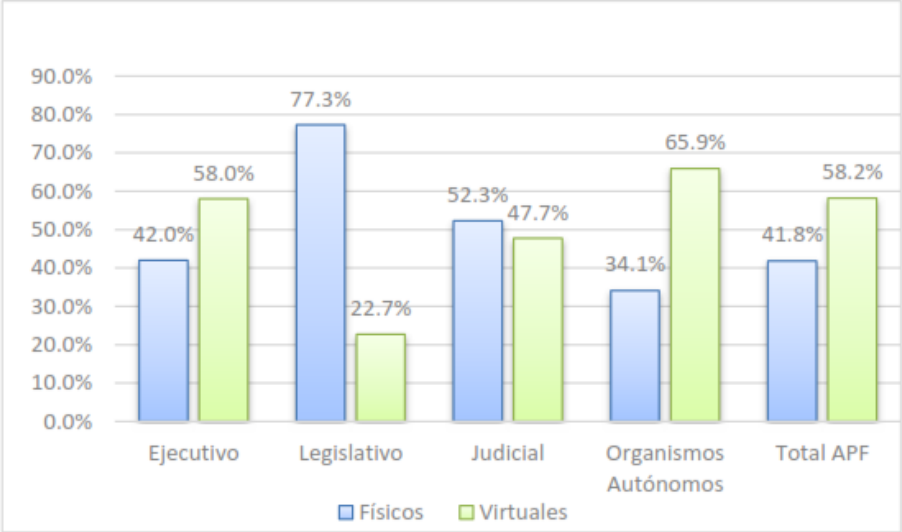

Figura 12, Nivel de virtualización, (Auditoría Superior de la Federación, 2016, pág. 2)

2. Sección de mejores prácticas; en esta sección se evaluaron los cinco dominios y 33 procesos contemplados en el marco de referencia COBIT 5.0, el cual, se muestra en la figura 13.

   Dominios

   - Gobierno de TIC (Evaluar, dirigir y monitorear)
   - Gestión de TIC (Alinear, planear y organizar)
   - Desarrollo de Soluciones Tecnológicas (Construir, adquirir e implementar)
   - Operación, seguridad y continuidad de TIC (Entregar, dar servicio y soporte)
   - Monitoreo de TIC (Supervisar, evaluar y valorar)

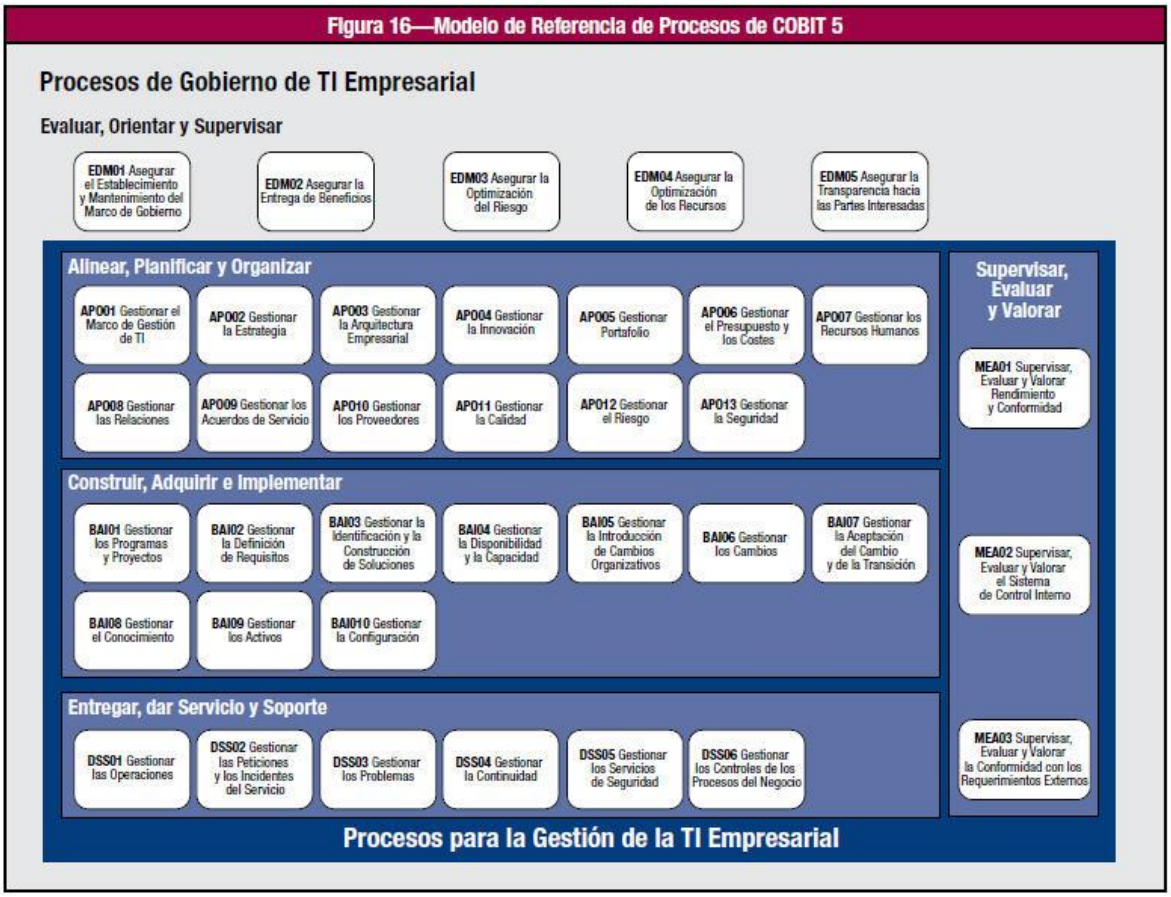

Figura 13, Modelo de referencia de procesos de COBIT 5.0, (Ramírez Díaz, 2012)

Los resultados arrojaron que el 95.85% de las entidades se encuentran en un estatus bajo, y el 4.15% en un estatus medio, ninguna entidad en estatus alto. Todos los procesos evaluados presentaron bajos niveles de madurez siendo los de mayor riesgo el de Operación, seguridad, continuidad y Monitoreo de TIC. El bajo nivel de madurez obtenido por las entidades de administración pública refleja dificultades en los procesos para gobernar, administrar, dar soporte, continuidad de la operación, seguridad en el manejo de la información de forma efectiva y eficiente a las TIC, para lo cual, el informe (Auditoría Superior de la Federación, 2016) presenta los siguientes riesgos en la Administración Pública Federal:

- Falta de alineación de las TIC con las estrategias de la entidad.
- Elevados costos en la operación y en el desarrollo de proyectos.
- Deficiencia en la segregación de funciones y asignación de los roles y responsabilidades del personal.
- Pérdida de información sensible e indisponibilidad de servicios críticos.
- Deficiente entrega de servicios e incumplimiento de programas de trabajo.

A continuación, en la figura 14, se muestra un análisis más detallado del diagnóstico realizado por la Auditoría Superior de la Federación.

Sector	Número de instituciones en el sector	Porcentaje de cumplimiento promedio alcanzado
Defensa Nacional	2	8.48 %
Función Pública	2	10.3 %
Marina	1	47.87 %
Hacienda y Crédito Público	24	10.73 %
Salud	40	1.38 %
Gobernación	18	9.44 %
Turismo	6	1.71 %
Relaciones Exteriores	3	18.18 %
Comunicaciones y Transportes	27	5.30 %
Trabajo y Previsión Social	5	5.09 %

Economía	10	6.21 %
Energía	11	4.62 %
Medio Ambiente y Recursos Naturales	8	7.35 %
Desarrollo Agrario, Territorial y Urbano	7	3.03 %
Consejo Nacional de Ciencia y Tecnología	28	5.36 %
Procuraduría General de la República	4	6.96 %
Desarrollo Social	10	3.21 %
Educación Pública	41	4.38 %
Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación	17	2.72 %
Instituciones no sectorizadas	8	8.56 %
Oficina de la Presidencia de la República	2	7.57 %
Empresa Productivas del Estado	2	6.66 %
Poder Legislativo	2	2.42 %
Poder Judicial de la Federación	3	10.90 %
Órganos Constitucionales Autónomos	9	8.28 %

Tabla 4, Resultados de la evaluación por sector. Fuente: elaboración propia con base en (Auditoría Superior de la Federación, 2016, pág. 5)

De acuerdo con la evaluación realizada a las Instituciones Gubernamentales, en una escala de 0 a 165 puntos de los 165 aspectos valorados (un punto por cada cumplimiento en los aspectos valorados), se observa en resumen lo siguiente:

Poderes de la Unión	Puntaje promedio obtenido
Poder Ejecutivo	9.32
Poder Legislativo	4
Poder Judicial	18
Órganos Constitucionales Autónomos	13.66

Tabla 5, Resultados por poderes de la Unión de la evaluación con base en COBIT 5.0. Fuente: elaboración propia con base en (Auditoría Superior de la Federación, 2016, pág. 13)

Como se observa anteriormente, ningún sector de la Administración Pública alcanza el 10% de cumplimiento con respecto a lo requerido en el marco de

referencia COBIT 5.0, lo que deja ver que las instituciones gubernamentales en México tienen rezagos en la implementación y ejecución de mejores prácticas en sus operaciones.

En este capítulo se constata que en México comienza a haber concientización en seguridad de la información, puesto que existen medidas que se han adoptado como el gobierno digital y reformas a la legislación que favorecen la adopción de tecnologías de la información y comunicación en los procesos cotidianos gubernamentales y por ende en los servicios a la ciudadanía. Sin embargo, la existencia de una cultura en seguridad de la información aún está distante.

Capítulo 3 El papel de las normas y mejores prácticas en la seguridad de la información.

Este capítulo tiene por objetivo conocer las normas y mejores prácticas que están orientadas a la seguridad de la información y de qué manera influyen en el proceso de concientización y generación de cultura organizacional en seguridad de la información.

3.1 Norma ISO 27000

La Organización Internacional de Normas (ISO, International Standarizsation Organization, por sus siglas en inglés) tiene como función principal la de buscar la estandarización de normas de productos y seguridad para las empresas y organizaciones a nivel mundial. Muchas organizaciones de todo el mundo deciden adoptar estas normas con el fin de implementar las mejores prácticas en sus procesos de negocio.

Para el ámbito de la seguridad de la información existe la serie de normas ISO/IEC 27000 como estándares de seguridad que contienen las mejores prácticas recomendadas para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). (Acevedo Juárez, 2011).

La idea de esta norma es preservar la confidencialidad, integridad y disponibilidad de la Información estableciendo un sistema, formado por un conjunto de procesos, gente y tecnología, que analice los riesgos de la información y establezca medidas para eliminarlos o minimizarlos de manera recurrente mediante un ciclo de mejora continua, manteniendo siempre el control de los riesgos para saber en todo momento la postura de seguridad de la organización. Es precisamente este sistema el que recibe el nombre de Sistema de Gestión de Seguridad de la Información, que es el punto central de la norma y que básicamente exige que cada organización que cumpla con ISO-27001 lleve a cabo cuatro grandes actividades:

- Establecer el sistema.
- Implementar y operar el sistema.
- Mantener y mejorar el sistema.

- Monitorear y revisar el sistema.

La norma marca que el Sistema de Gestión de la Información antes mencionado se basa el ciclo de mejora continua o de Deming. Dicho ciclo consiste en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act). Tomando en cuenta este ciclo de información, la familia de normas ISO 27000 contempla diferentes tipos de seguridad, como: organizativa, lógica, física y legal, desde el nivel estratégico y operativo en cualquier organización como se muestra en la figura 14.

Figura 14, Esquema de los tipos de seguridad contemplados por la norma ISO 27000. Fuente: (Instituto Uruguayo de Normas Técnicas, 2013)

De acuerdo con (Audisec, s.f.) algunas de las normas más importantes que integran la familia ISO 27000, son:

- ISO 27001: es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por la norma.

- ISO 27002: se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, los cuales contienen un total de 144 controles.

- ISO 27003: es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.

- ISO 27004: describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la Seguridad de la Información. Especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos.

- ISO 27005: es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.

- ISO 27006: es un conjunto de requisitos de acreditación para las organizaciones certificadoras.

- ISO 27007: es una guía para auditar SGI. Establece qué auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, entre otros.

La figura 15 muestra un esquema más comprensible de la razón de ser de las principales normas que contempla la ISO 27000.

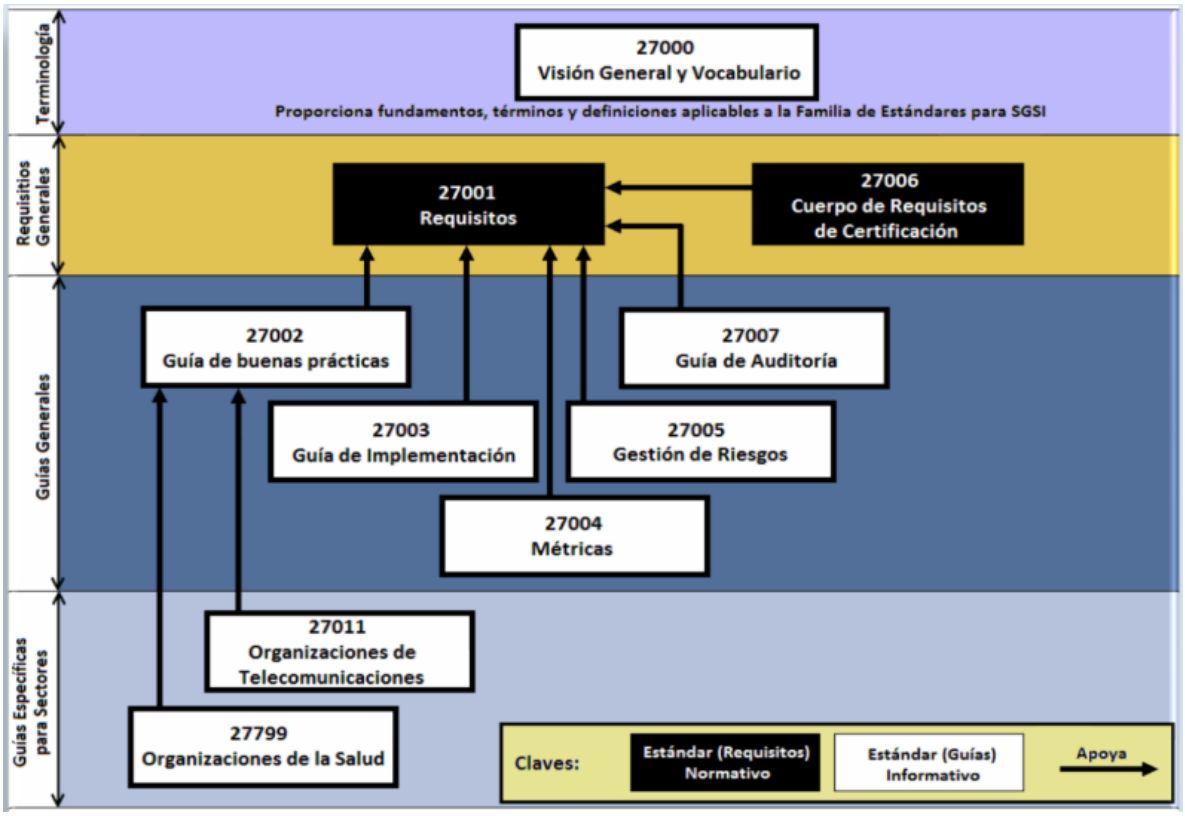

Figura 15, Esquema de la familia de la norma ISO 27000. Fuente: (VI Congreso Iberoamericano de Seguridad Informática, 2011)

Si bien toda la familia de normas ISO 27000 contempla aspectos de gestión de la información, para el tema de seguridad existe la norma ISO 27002, ya que tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de la organización (Blog especializado en Sistemas de Gestión , 2016).

La importancia de disponer de información actualizada, completa y veraz es la clave para la realización de todas las actividades de cualquier organización. Sin embargo, es crucial mantener dicha información segura para que no se pierda, sea robada o se deteriore de cualquier forma, ya que, la información y los datos de que dispone una organización son uno de los activos más valiosos que pueden marcar su vigencia y posicionamiento en el mercado.

La norma ISO 27002 se encuentra estructurada en 14 capítulos, 35 objetivos y 114 controles que describen los aspectos a considerar para garantizar la seguridad de la información de la que se dispone. A continuación, se enlistan los aspectos generales:

- Políticas de Seguridad de la Información
- Organización de la Seguridad de la Información
- Seguridad relativa a los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisiciones, desarrollo y mantenimiento de los sistemas de información
- Relación de proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad de negocio
- Cumplimiento

Cabe destacar que en esta norma se hace énfasis en la concienciación, educación y capacitación en seguridad de la información en el punto nombrado como “seguridad ligada a los recursos humanos”, de esta manera se confirma la relevancia que tiene el factor humano en la seguridad de la información, ya que, muchos ataques a los sistemas informáticos suelen provenir de errores humanos en el uso de sus dispositivos de cómputo.

Implementar las normas de la familia ISO 27000 permite a las organizaciones demostrar que dispone de los controles y procedimientos adecuados para asegurar el tratamiento de los datos y la información con la que se trata. Además, funge como elemento diferenciador para destacar sobre la competencia, ayuda al cumplimiento

de la legislación relativa a la protección de los datos, se disminuyen costos y favorece la organización interna.

3.2 NIST SP 800-50

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology (NIST), por sus siglas en inglés) es una agencia federal no regulada que forma parte del Departamento de Comercio de los Estados Unidos. Su misión consiste en elaborar y promover patrones de la medición, los estándares y le tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida.

Las publicaciones especiales de la serie SP 800 presentan los documentos de interés general relativos a la seguridad de la información y evaluación de riesgos. La diversidad de las publicaciones especiales de esta serie presenta manuales, guías técnicas, recomendaciones y buenas prácticas.

Al igual de la serie de normas ISO 27000, la serie SP 800 proporciona información que cubre la gestión y las prácticas operativas de seguridad de la información, pero en un mayor número de documentos. Por ejemplo, para realizar la integración de la gestión de riesgos de seguridad de la información con las operaciones de la empresa, la serie NIST SP 800 tiene el documento SP 800-39-Gestión de Riesgos de Seguridad.

Asimismo, como lo menciona (Blog especializado en Sistemas de Gestión , 2016) para realizar la evaluación de los riesgos, la serie SP 800 tiene un conjunto de documentos que han sido creados utilizando la metodología de riesgo en seis pasos, los cuales son:

- Categorizar: se debe dar prioridad a los sistemas de información que se basan en la evaluación del impacto. El detalle se encuentra en el documento SP 800-60.

- Seleccionar: se definen los controles a aplicar, con base en la evaluación del impacto y las bases de SP 800-53, siendo un documento de referencia para este paso.
- Poner en práctica: implementar los controles y la elaboración de los documentos. El detalle se encuentra en el documento SP 800-160.
- Evaluar: la confirmación de que los controles se implantan de forma correcta, opera según lo previsto, y producen los resultados deseados. El detalle se encuentra en el documento SP 800-53.
- Autorizar: la aceptación del escenario de riesgo, y la autorización para la operación de los sistemas de información y utilización. El detalle se encuentra en el documento SP 800-37.
- Monitorear: se acompaña de forma continua de los sistemas de información y el entorno operativo para establecer la eficiencia y el cumplimiento de los controles. El detalle se encuentra en el documento SP 800-137.

También la serie SP 800 hace referencia a la serie SP 8001-53 que organiza en categorías temas relacionados con la gestión de la seguridad de la información, por ejemplo, las series:

- SP 800-61: Directrices para detectar, analizar, priorizar y gestionar los incidentes de responder a ellas de forma eficiente y eficaz.
- SP 800-50: Pautas para el diseño, desarrollo, implantación y evaluación de un programa de sensibilización y formación.
- SP 800-116: Es el riesgo basado en la selección de los mecanismos de autenticación apropiados para gestionar el acceso físico.
- SP 800-46: Prácticas para mitigar los riesgos asociados con las tecnologías utilizadas para el teletrabajo.
- SP 800-122: Orientaciones para la protección de la confidencialidad de la información de identificación de personal con el apoyo de los sistemas de información.
- SP 800-161: Guía para identificar, evaluar, seleccionar e implantar la gestión de riesgos y controles para gestionar los riesgos e la cadena de suministro.

- SP 800-92: Orientación sobre el desarrollo, implantación y mantenimiento de las prácticas de gestión de riesgos eficientes para apoyo.
- SP 800-88: Recomendaciones para la implantación de un programa de saneamiento de los medios, teniendo en cuenta las técnicas y controles para la desinfección y eliminación de la información confidencial.
- SP 800-83: Orientación sobre la prevención de ataques de este tipo y responder a los incidentes de programa maligno (malware).
- SP 800-64: Descripción de las funciones de seguridad y responsabilidades clave necesarios en el desarrollo de los sistemas de información, y la información sobre la relación entre la seguridad de la información y el ciclo de vida del software de desarrollo.
- SP 800-45: Proporciona prácticas de seguridad para el diseño, implantación y sistemas de correo electrónico de funcionamiento en las redes públicas y privadas de apoyo.
- SP 800-44: Presenta las prácticas de seguridad para el diseño, implantación y operación de los servidores web de acceso público e infraestructura de la red relacionada.
- SP 800-41: Proporciona una guía durante el desarrollo de las políticas y la selección de firewall, configuración, prueba, implantación y administración de servidores de seguridad.
- SP 800-34: Proporciona información sobre el sistema de información de la planificación y contingencia y otros tipos de planes de seguridad y emergencia de contingencia.

Es bien sabido que las personas son uno de los eslabones más débiles en los intentos de asegurar sistemas y redes, pues el "factor personas" - no la tecnología - es clave para proporcionar un servicio adecuado y apropiado nivel de seguridad. Si las personas son la clave y a la vez un eslabón débil, se debe prestar más y mejor atención a este factor, por lo que un programa de sensibilización y capacitación sólido es primordial para garantizar que las personas entienden sus

responsabilidades de seguridad de TI, las políticas de la organización y cómo usar y proteger los recursos tecnológicos.

Por esta razón, la serie SP 800, como se redactó en las viñetas anteriores, contempla el documento “SP 800-50 Construcción de un Programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información” en el cual se marcan las pautas para el diseño, desarrollo, implantación y evaluación de un programa de sensibilización y formación de una cultura en seguridad de la información. A su vez, (NIST SP 800-50, 2003) establece que un “programa de concientización debe comenzar con un esfuerzo que pueda implementarse de diversas maneras y esté dirigido a todos los niveles de la organización”, ya que, la efectividad de este esfuerzo generalmente determinará la efectividad del programa de concientización y entrenamiento.

El documento describe tres componentes principales de un programa para desarrollar la cultura en seguridad de la información: concientización, entrenamiento y educación. En la figura 16 se puede observar un esquema:

- Concientización. Su propósito es enfocar la atención en seguridad de la información para posibilitar que el público objetivo reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar, por ejemplo; mantener el escritorio limpio, usar de forma adecuada las contraseñas, elaborar copias de respaldo, usar el correo responsablemente, entre otros.
- Entrenamiento. Se centra en generar habilidades y competencias en seguridad de la información con el fin de que el público objetivo las aprenda y aplique en el día a día.
- Educación. Integra habilidades de seguridad y competencias de las diferentes especialidades funcionales dentro de un cuerpo común de conocimientos, enfocándose en producir especialistas en seguridad. Por ejemplo, capacitación en sistemas de gestión de seguridad de la información o en auditoría interna.

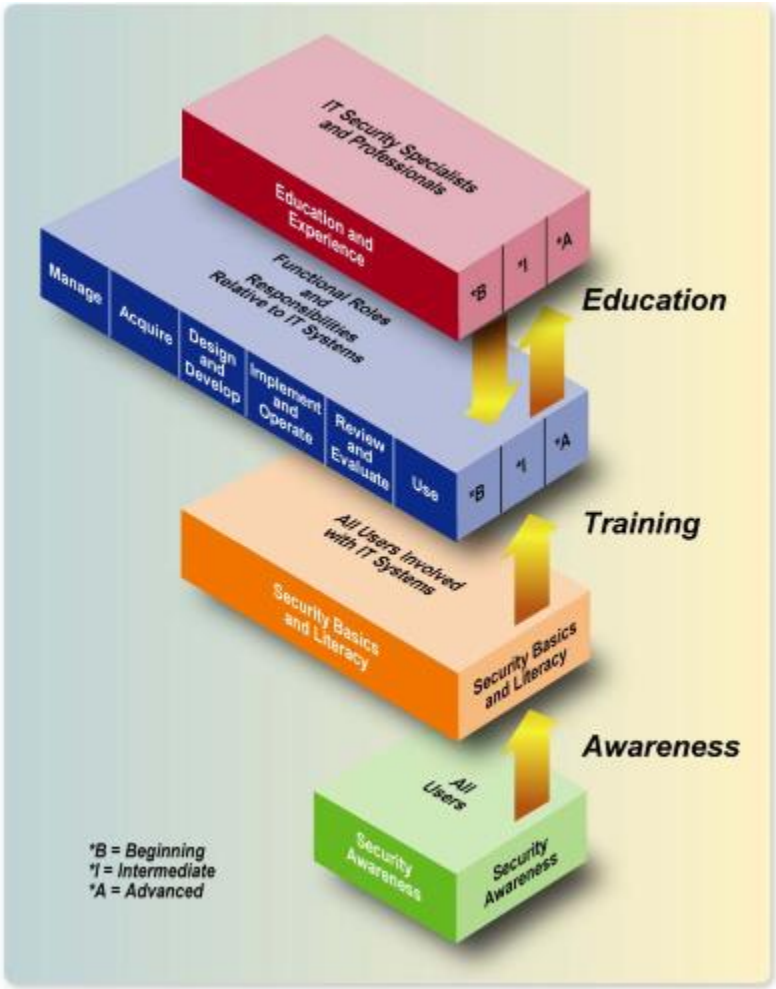

Figura 16, Aprendizaje continuo en seguridad de la información. Fuente: (NIST SP 800-50, 2003, pág. 8)

El esquema representa la relación entre la conciencia, la capacitación y la educación, lo que hace que se constituya un aprendizaje continuo. El aprendizaje continuo; comienza con la conciencia, se basa en la capacitación y evoluciona hacia la educación. El aprendizaje continuo se describe más detalladamente en la publicación especial NIST 800-16 “Requisitos de capacitación en seguridad de la tecnología de la información: un modelo basado en función y rendimiento”.

En este documento, (NIST SP 800-50, 2003) también describe cuatro fases principales para el desarrollo de los planes de concientización y entrenamiento en seguridad de la información y sus tareas asociadas, las cuales se resumen en la figura 17:

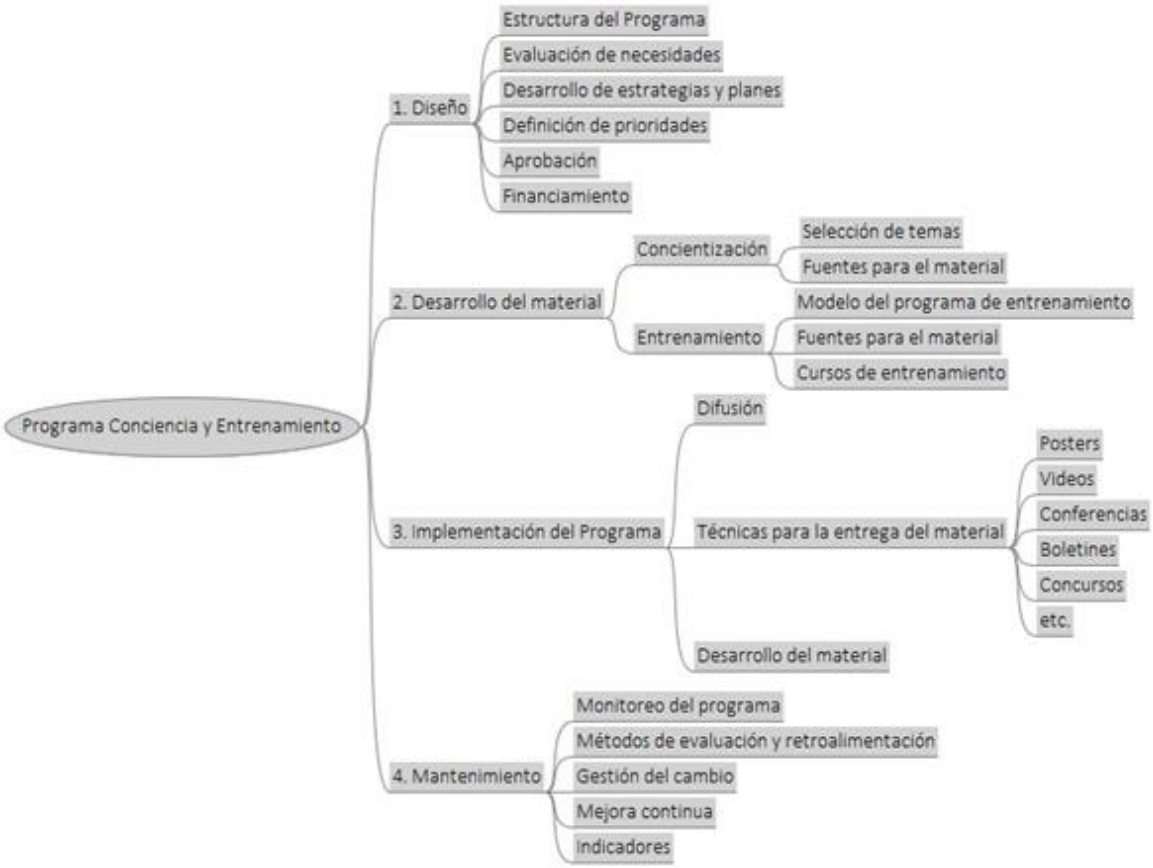

Figura 17, Fases del programa de concientización y entrenamiento. Fuente: (Villamizar, 2013)

Un programa efectivo de concientización y seguridad en TI explica a todos los interesados las reglas de conducta adecuadas para el uso de los sistemas e información. El programa deberá comunicar las políticas de seguridad de TI y los procedimientos que deben seguirse, para esto, los usuarios primero deben ser informados de las expectativas del programa.

En resumen, ambas normas ISO 27002 y NIST SP 800-50 conciben como parte de las buenas prácticas en seguridad de la información, a la actividad de concientización del recurso humano en cualquier empresa. Hay que destacar que el objetivo de las presentaciones de sensibilización es simplemente centrar la atención en la seguridad. Las presentaciones de concientización están destinadas a permitir que las personas reconozcan los problemas de seguridad de TI y respondan en consecuencia.

Estas normas y mejores prácticas son la base para crear una cultura en seguridad de la información, la cual, es la mejor herramienta para propiciar que las personas trabajen de forma segura y para ello, es necesario que las personas quieran hacerlo, lo cual, implica la existencia de una auténtica y robusta cultura de seguridad, bienestar y alto desempeño que funja como un sólido fundamento, ya que de lo contrario es predecible que sigan existiendo accidentes graves y fatalidades en el manejo de la información, además de todos los impactos directos e indirectos que dicho ambiente provoca.

Capítulo 4. Caso de estudio: Auditoría Superior de la Federación

4.1 Justificación del estudio de caso

La información que se maneja en las instituciones de gobierno es inmensa y la vulnerabilidad a la que está expuesta puede ser muy grande, dependiendo de las estrategias y controles que lleve a cabo cada institución para asegurar su confidencialidad, integridad y disponibilidad de esta.

La información, de las instituciones gubernamentales específicamente la generada en la Auditoría Superior de la Federación (ASF), utilizada en los procesos de auditoría es de alta confidencialidad, debido a que puede ser muy susceptible a que personas no autorizadas la utilicen para su beneficio, repercutiendo en fraudes, desvió de recursos y, crecimiento de la corrupción, entre otros.

Cabe destacar que la ASF es la encargada de la revisión de la cuenta pública y como máximo órgano fiscalizador en México tiene acceso a mucha información confidencial de entidades gubernamentales y privadas, tanto de nivel ejecutivo, legislativo o judicial, ya que revisa la correcta aplicación de los recursos federales. Por lo anterior, la información que recibe como la que genera es de alta confidencialidad y su tratamiento requiere máximos niveles de seguridad.

Es por esto que resulta importante conocer la situación actual de la seguridad de la información en instituciones gubernamentales que son clave, como la Auditoria Superior de la Federación, para ello, el primer paso como lo marcan las normas y mejores prácticas es constatar el nivel de concientización que tiene el personal que labora en la institución con respecto al manejo de la información sensible, esta evaluación resulta preponderante por la cantidad de documentación clasificada como reservada a la que tienen acceso y que es propiedad de otras entidades de gobierno. Si bien la ASF realiza auditorias sobre el aprovechamiento de recursos, infraestructura y servicios de TIC a diferentes entidades de gobierno, en las cuales emite acciones como recomendaciones e incluso sanciones de responsabilidad administrativa sancionatoria que están encaminadas a la seguridad en las redes de datos, resulta interesante conocer si cuentan con estrategias internas de seguridad de la información que abarquen al personal y el nivel de cultura en seguridad que

poseen, ya que, el recurso humano es uno de los eslabones más sensibles que tiene cualquier organización.

4.2 Planteamiento del problema

La actividad principal de la Auditoría Especial de Gasto Federalizado es verificar que los recursos públicos federales se hayan recaudado, administrado, controlado y ejercido de conformidad con la normatividad aplicable, así como verificar el cumplimiento de los objetivos, metas, políticas y programas públicos (Dirección General de Administración de la ASF, 2010), por lo que la Dirección General de Auditoría a los Recursos Federales Transferidos “B” (DGARFT”B”) al ser parte de ella, realiza auditorías a programas y fondos federales orientados a verificar principalmente su cumplimiento financiero. Cabe señalar que en esta Dirección General es en donde se analizará la evaluación de la concientización y cultura en seguridad de la información del proceso de auditoría para el presente caso de estudio, asimismo, otra área de apoyo será la Dirección General de Sistemas (DGS), especialmente la comunicación que tienen estas dos áreas y cómo es que la DGS provee a la DGARFT”B” de los servicios de cómputo.

Debido a la representación de la ASF como máxima institución fiscalizadora en México, y por funciones que desempeña, resultan cruciales los procesos de seguridad de la información que se realicen. Para ello, el cuestionamiento base de la investigación es: *¿Cuáles son los beneficios de la concientización y la cultura de la seguridad de la información en una institución de gobierno en México?* Tomando en cuenta esto, se vuelve relevante conocer las prácticas que llevan a cabo los empleados, así como el nivel en cultura de seguridad de la información que poseen. Cabe señalar que una de las motivaciones por las que se eligió este tema para el caso de estudio deriva de mi experiencia como auditor y empleada de la institución, tiempo en el que pude detectar malas prácticas por parte de los usuarios en el manejo de la información y que comprometieron la información de las auditorías.

Una vez que se haya analizado la situación actual del nivel de concientización que tiene el personal, se estará en posición de generar recomendaciones en materia de creación de estrategias para la gestión de la seguridad de la información.

4.3 Estudio de caso

El presente estudio de caso se realizará de manera observacional, debido a que se tienen variables como niveles de confidencialidad, disponibilidad e integridad de la información, así como el nivel de concientización por parte de los empleados, estas variables no pueden ser manipuladas sino descritas para explicar las medidas que actualmente se implementan y la situación de la Auditoría Superior de la Federación en cuanto a la seguridad de la información en su proceso de auditoría.

Es observacional porque se analizarán las etapas del proceso de ejecución de auditoria, es decir, desde la generación de la orden de auditoría, el análisis de la información preliminar, la ejecución de los procesos de auditoría en campo, la presentación de los resultados preliminares, análisis de la documentación en respuesta a resultados preliminares, emisión de resultados finales, análisis de la documentación en respuesta a los resultados finales y la generación del informe de auditoría, todo esto desde la observación de cómo se maneja la información en cada una de las etapas antes mencionadas.

Este estudio también será de tipo transversal, es decir, el nivel de seguridad de información y el uso de la tecnología utilizada en los procesos de auditoría serán evaluados una sola vez en un periodo determinado. Asimismo, la investigación será descriptiva, ya que se pretende conocer la situación actual de la concientización y cultura en seguridad de la información que tiene el personal de la Auditoría Superior de la Federación, a partir del análisis de su documentación y las principales prácticas y procedimientos que llevan a cabo para la realización de sus operaciones.

4.4 Matriz de congruencia

Pregunta Principal	Objetivo General	Hipótesis Principal
¿Cuáles son los beneficios o repercusiones de fomentar la concientización y la cultura en seguridad de la información en una institución de gobierno en México?	Evaluar la conciencia de la seguridad de la información expresada a través de normas y mejores prácticas para identificar áreas de oportunidad.	La concientización y la cultura en la seguridad de la información en una Institución de Gobierno en México (Auditoría Superior de la Federación) propicia la integridad, disponibilidad y confidencialidad de los datos que procesa, y a su vez favorece la transparencia de las actividades del servicio público.
Pregunta secundaria	Objetivo específico	Hipótesis secundaria
¿Cuáles son las medidas que lleva a cabo la ASF para asegurar la confidencialidad, disponibilidad e integridad de su información?	Conocer cuáles son las medidas que lleva a cabo la ASF para asegurar la confidencialidad, disponibilidad e integridad de su información. ¿para qué?	Las medidas que lleva a cabo la ASF son más normativas (reglamento interno, código de ética, manuales de procedimientos) y poco técnicas y operativas (utilización de sistemas informáticos y vinculación con usuarios), lo que ocasiona que no en todos los niveles (estratégico, táctico y operativo) se apliquen.
¿En qué parte del proceso de auditoría existe más vulnerabilidad en la información?	Identificar en qué parte del proceso de auditoría existe más vulnerabilidad en la información	Existe más vulnerabilidad de la información en dos partes del proceso: 1. Recepción de la información preliminar 2. Ejecución de la auditoría en campo
¿Qué repercusiones se han tenido con la pérdida de información?	Conocer qué repercusiones se han tenido con la pérdida de información	La pérdida de información ocasiona retrabajos e incluso resultados erróneos en las auditorías que derivan en acciones

		emitidas mal fundamentadas, así como repercusiones económicas.

Tabla 6, Matriz de congruencia. Fuente: elaboración propia

4.5 Método

El método por utilizar es el estudio de caso deductivo, ya que se partirá del estudio general de la importancia de la seguridad de la información en las empresas e instituciones gubernamentales, se estudiará el entorno internacional y nacional, determinando el marco legislativo regulatorio, así como las principales tendencias de la ciberseguridad. Posteriormente se realizará un análisis de la seguridad de la información en las instituciones gubernamentales mexicanas, teniendo como caso de estudio la Auditoría Superior de la Federación como máximo órgano de fiscalización en México y a partir de eso se analizará la concientización y cultura en seguridad de la información que posee esa institución.

Este estudio se llevó a cabo de la siguiente forma:

- Operativización de variables:
    - Variable independiente:
      (X_1) La concientización y la cultura de la seguridad de la información.
    - Variables dependientes:
      (Y_1) Integridad, disponibilidad y confidencialidad de los datos.

  Tomando en cuenta las normas y mejores prácticas, la evaluación de las variables se realizará de acuerdo con los niveles de concientización establecidos en el *Modelo de Madurez de Conciencia de Seguridad* del Instituto SANS (SysAdmin Audit, Networking and Security Institute) el cual está formado de miles de profesionales en seguridad informática.

Este modelo establece que el nivel de riesgo humano puede mitigarse cambiando el comportamiento del usuario final. Este modelo permite a las organizaciones identificar su nivel de madurez actual de su programa de concientización, lo cual ayuda a determinar el camino hacia la mejora. El modelo se puede observar en la figura 18.

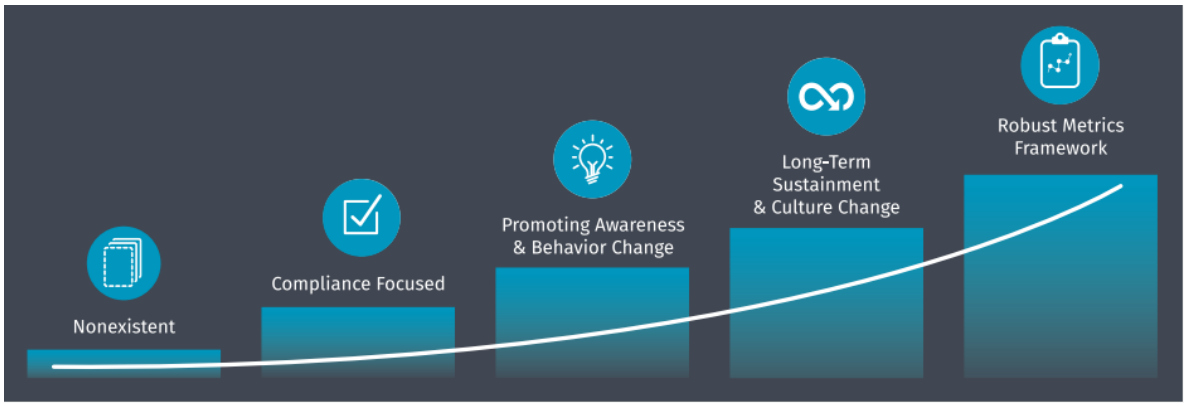

Figura 18, Modelo de Madurez de Conciencia de Seguridad. Fuente: (SANS Institute, 2018, pág. 9)

Como se observa el modelo consta de cinco niveles, los cuales son:

1. Inexistente:

El programa no existe. Los empleados tienen poca o ninguna idea de que son un objetivo cibernético y que sus acciones tienen un impacto directo en la seguridad de la organización, además de que no conocen ni entienden las políticas de la organización y son víctimas de ataques fácilmente.

2. Enfocado en el cumplimiento:

El programa está diseñado principalmente para cumplir requisitos específicos de cumplimiento o auditoría, la capacitación se limita a una anual o ad-hoc. El éxito del programa se basa en la participación, los empleados no están seguros de las políticas de la organización y/o su rol en la protección de los activos de información de su organización.

3. Promover la conciencia y el cambio de comportamiento:

El programa identifica los temas de capacitación que tienen el mayor impacto para apoyar la misión de la organización y se centra en esos temas

clave. Va más allá de la capacitación anual y a menudo incluye un refuerzo continuo durante todo el año, el contenido se comunica de una manera atractiva y positiva que fomenta el cambio de comportamiento en el trabajo y en el hogar. Como resultado, las personas entienden y siguen las políticas de la organización y activamente reconocen, previenen y denuncian incidentes. El éxito del programa se amplía para incluir una reducción en el comportamiento relacionado con el riesgo y un mayor conocimiento de las políticas.

4. Mantenimiento a largo plazo y cambio cultural:

El programa cuenta con los procesos, recursos y apoyo de liderazgo para un ciclo de vida a largo plazo, que incluye como mínimo una revisión y actualización anual del programa. Como resultado, el programa y los principios básicos de un buen comportamiento y aprendizaje de seguridad cibernética son una parte establecida de la cultura de la organización. Éxito del programa se extiende para incluir la aceptación generalizada y cultural del buen comportamiento cibernético (y el rechazo de los malos comportamientos), así como la comprensión general y la aceptación del programa de concienciación sobre la seguridad y su valor.

5. Marco de métricas:

El programa es lo suficientemente robusto como para proporcionar métricas, como; el progreso y el impacto en el comportamiento. Además, como resultado, el programa mejora continuamente y puede demostrar el retorno de la inversión. Si bien se señala que un marco de medición se enumera como la última etapa del modelo, las métricas son una parte importante de cada etapa. Esta etapa refuerza aún más que para tener verdaderamente un programa maduro, no solo debe sustentar un cambio en el comportamiento y la cultura, sino también tener las métricas para demostrarlo. El éxito se amplía aún más para incluir métricas que se adaptan a los temas de concientización sobre seguridad que muestran no solo la participación, el cumplimiento y la mejora del comportamiento, sino también

cambios en la comprensión y la competencia de seguridad cibernética en toda la organización.

De acuerdo con lo anterior, desde el nivel 3 denominado: *Promover la conciencia y el cambio de comportamiento* se está considerando el cumplimiento de lo que se determinó como variable dependiente en este estudio (propiciar la integridad, disponibilidad y confidencialidad de los datos) y en el nivel 4 denominado: *Mantenimiento a largo plazo y cambio cultural*, se está considerando tener una cultura en seguridad de la información, concepto que también se evaluará en el caso de estudio.

De acuerdo con los niveles que establece este modelo, se diseñó una métrica basada en los criterios y parámetros de acuerdo con los niveles de madurez del modelo, los cuales se muestran a continuación:

Criterios de evaluación	**Nivel de Madurez**
No existe un plan de seguridad ni políticas establecidas. No hay interés de los directivos No hay control de accesos a áreas, sistemas y dispositivos informáticos. No existe seguridad lógica para los sistemas o es muy básica. No hay un área o encargado de sistemas Los empleados desconocen las medidas de seguridad informática básicas	1.inexistente
Las políticas de seguridad no se encuentran documentadas. Existe un área de sistemas encargada de la seguridad, sin embargo, no hay comunicación efectiva con los usuarios. Cuentan con escasas herramientas lógicas y físicas para la seguridad informática	2.Enfocado en el cumplimiento

El esfuerzo está orientado a cumplir solo con lo alguna ley o normativa que están obligados a cumplir.	
Las políticas de seguridad están documentadas y son comunicadas al personal. Realizan campañas de capacitación más de una vez al año para los usuarios. Hay mayor interés por parte de los directivos, por lo que existe un presupuesto específico para el área de sistemas El personal de sistemas cuenta con algunas certificaciones orientadas a la seguridad de la información. La mayoría del personal es capaz de reconocer una amenaza cibernética.	3.Promover la conciencia y el cambio de comportamiento
Existe un plan de seguridad de la información a largo plazo, el cual, se revisa y actualiza una vez al año como mínimo. El personal cuenta con los conocimientos para reconocer cualquier tipo de amenaza cibernética y reportarla. El personal es consciente de la importancia de la seguridad de la información y aplica sus conocimientos en todas sus actividades laborales y personales. Se cuenta con equipos y software especializado en seguridad informática.	4.Mantenimiento a largo plazo y cambio cultural
Además de cumplir con todo lo indicado en el *nivel 4 Mantenimiento a largo plazo y cambio cultural*, el área de sistemas es lo suficientemente robusta como para tener un programa de mejora continua con métricas y evaluaciones financieras. Todos los empleados son conscientes y tienen una cultura arraigada en seguridad de la información.	5.Marco de métricas

Tabla 7, Criterios y niveles de madurez del modelo SANS de Conciencia de Seguridad. Fuente: elaboración propia.

- Métodos de recolección de datos para la realización del estudio de caso:
    A. Análisis documental: se verificó que la ASF cuente con lineamientos, normativas, políticas y manuales relacionados con las seguridades de la información y que estén debidamente documentados y autorizados.
        - Políticas de seguridad de la información con las que cuenta la ASF.
        - Información circulante, relativa a la vinculación entre la Dirección General de Sistemas y los usuarios finales.
    B. Pruebas informáticas: se aplicaron distintas pruebas mediante software libre para conocer de manera general los controles de seguridad que pueda tener la ASF:
        - Aplicación de la prueba CA Security (para evaluar página web)
        - Aplicación de Tor Browser (navegador anónimo, para evaluar la negación o acceso a navegación web a usuarios)
        - Aplicación de Angry IP Scanner (para conocer número de computadoras en red)
        - Aplicación de la prueba de ataque dirigido
    C. Uso de los activos informáticos y cultura en seguridad de la información: se aplicó una simulación de un ataque cibernético, así como entrevistas a empleados para conocer sus hábitos en el manejo de la información y la vinculación con la tecnología.
        - Aplicación de cuestionario y entrevistas con personal interno de la ASF (auditores, jefes de departamento, subdirectores y directores)

La recolección de datos por análisis documental, pruebas informáticas y entrevistas con el personal permitió conocer más a fondo el proceso de información y las practicas cotidianas. Esto, con la finalidad de comprender la problemática y posteriormente describir los resultados del estudio.

4.6 Atribuciones y funcionamiento de la ASF

La Auditoría Superior de la Federación, en su carácter de entidad de fiscalización superior, fue creada para apoyar a la Honorable Cámara de Diputados en el ejercicio de sus atribuciones constitucionales relativas a revisión de la Cuenta de la Hacienda Pública Federal, con objeto de conocer los resultados de la gestión financiera, comprobar si ésta se ajustó a los lineamientos señalados por el presupuesto y constatar la consecución de los objetivos y las metas contenidas en los programas de gobierno.

De acuerdo con el artículo primero del Reglamento Interior de la Auditoría Superior de la Federación de la Cámara de Diputados, este órgano, es la entidad de fiscalización superior de la Federación que tiene a su cargo la revisión de la Cuenta Pública, así como las demás funciones que expresamente le encomienden la Constitución Política de los Estados Unidos Mexicanos, la Ley de Fiscalización Superior de la Federación y demás ordenamientos legales aplicables.

La Constitución Política de los Estados Unidos Mexicanos señala en su artículo 79, lo siguiente: “La entidad de fiscalización superior de la Federación, de la Cámara de Diputados, tendrá autonomía técnica y de gestión en el ejercicio de sus atribuciones y para decidir sobre su organización interna, funcionamiento y resoluciones, en los términos que disponga la Ley.”

Ahora bien, podemos resumir que la ASF tiene como misión fiscalizar la Cuenta Pública mediante auditorías que se efectúan a los tres Poderes de la Unión, a los órganos constitucionalmente autónomos, a las entidades federativas y municipios del país, así como a todo ente que ejerza recursos públicos federales, incluyendo a los particulares. Conforme a su mandato legal, el propósito es verificar el cumplimiento de los objetivos contenidos en las políticas y programas gubernamentales, el adecuado desempeño de las entidades fiscalizadas, y el correcto manejo tanto del ingreso como del gasto público.

La fiscalización superior es uno de los instrumentos que tiene el país para contribuir a la mejora de la acción gubernamental y generar la confianza de la sociedad.

Por un lado, permite que las instituciones auditadas cuenten con un diagnóstico objetivo de su actuación y, por el otro, ofrece a la sociedad un panorama técnico y objetivo acerca del manejo de los recursos públicos.

4.7 Marco Jurídico de la ASF

El marco jurídico de actuación de la Auditoria Superior de la Federación se basa principalmente en:

Principales Ordenamientos Jurídicos

- Constitución Política de los Estados Unidos Mexicanos.

Leyes y Reglamentos

- Ley de Fiscalización y Rendición de Cuentas de la Federación.
- Reglamento Interior de la Auditoría Superior de la Federación.

Funcionamiento de la ASF

Como órgano técnico especializado de la Cámara de Diputados, dotado de autonomía técnica y de gestión, su actuación se rige por un marco jurídico, técnico y ético.

En cuanto a su desempeño técnico, la ASF ha emitido diversos instrumentos en los que establece las normas y procedimientos de auditoría que utiliza para llevar a cabo sus funciones y tareas.

Por su calidad y características, las normas técnicas de la institución son comparables con las utilizadas por países con mayor grado de desarrollo en el mundo, y se encuentran en un proceso permanente de actualización que garantiza su constante mejora, por ejemplo, su participación en la Asociación Nacional de

Organismos de Fiscalización Superior y Control Gubernamental. Del mismo modo, con el fin de que los servidores públicos desempeñen su función de manera diligente, imparcial y objetiva, la ASF ha desarrollado un Código de Ética que recoge los valores centrales de la función de fiscalización superior, como lo son la integridad, la equidad, la competencia profesional, la confiabilidad y la independencia. Este conjunto de preceptos tiene como finalidad colocar a la fiscalización superior bajo una óptica de servicio a la sociedad, con base en rigurosas normas de conducta y valores institucionales aplicables a todos sus integrantes.

La ASF, dentro de su marco rector constituido por el ámbito legal (Constitución y Ley de Fiscalización y Rendición de Cuentas de la Federación), ámbito ético (Código de Ética) y ámbito técnico (normativa interna que rige el funcionamiento de la institución), ha plasmado su razón de ser y la visión que tiene como la máxima institución fiscalizadora en México de la siguiente forma:

Misión

La misión de la ASF es fiscalizar la Cuenta Pública mediante auditorías que se efectúan a los tres Poderes de la Unión, a los órganos constitucionalmente autónomos, a las entidades federativas y municipios del país, así como a todo ente que ejerza recursos públicos federales, incluyendo a los particulares. Conforme a su mandato legal, el propósito es verificar el cumplimiento de los objetivos contenidos en las políticas y programas gubernamentales, el adecuado desempeño de las entidades fiscalizadas, y el correcto manejo tanto del ingreso como del gasto público.

Visión

Al llevar a cabo su misión, la ASF busca posicionarse como una institución objetiva e imparcial, técnicamente sólida y sujeta a un proceso de mejora continua, cuyos productos puedan constituirse en un elemento central para el Poder Legislativo en la definición de las asignaciones presupuestarias de los programas, proyectos y políticas públicas. De esta manera, contribuirá a generar confianza en

la ciudadanía respecto al manejo de los recursos y a fortalecer una cultura gubernamental de transparencia y rendición de cuentas.

Existen objetivos generales que la ASF busca cumplir, como son:

a) Revisar la Cuenta de la Hacienda Pública Federal de manera objetiva, imparcial y oportuna para merecer la confianza y credibilidad de la Honorable Cámara de Diputados y de la sociedad.

b) Fomentar gestiones públicas responsables, orientadas a la obtención de resultados y a la satisfacción de las necesidades de la población.

c) Apoyar al Honorable Congreso de la Unión y al Gobierno Federal en la solución de problemas estructurales y en la identificación de oportunidades para mejorar el desempeño de las instituciones públicas.

d) Consolidar la transición de la entidad de fiscalización superior de la Federación, maximizar el valor de sus servicios a la Honorable Cámara de Diputados y convertirla en una institución modelo de clase mundial.

e) Establecer programas de aseguramiento de la calidad con el fin de constatar que se aplican las técnicas de auditoría apropiadas; que el tamaño de las muestras seleccionadas para cada caso asegure la representatividad y los niveles de confianza requeridos; que el contenido y calidad de los informes sean acordes con los objetivos previstos; y que el sistema automatizado de seguimiento y control de las acciones promovidas permita conocer su impacto económico y social.

Además de los objetivos generales, la Auditoría Superior de la Federación tiene como acción prioritaria de su encomienda, y visión institucional, un enfoque que contribuye a la mejora de la gestión gubernamental mediante la atención de las líneas estratégicas de actuación siguientes:

- Impulsar la fiscalización de alto impacto
- Propiciar la eficiencia y eficacia de la acción pública
- Promover la implantación de mejores prácticas gubernamentales
- Promover y contribuir a mejorar los procesos de rendición de cuentas

Como se mencionó anteriormente, la actividad principal de la ASF es la verificación de la rendición de cuentas, es decir; las personas, los organismos y las organizaciones (de carácter público, privado y de la sociedad civil) tienen la responsabilidad del adecuado cumplimiento de sus funciones y por lo tanto la auditoría se encarga de verificar la transparencia en la rendición de cuentas. Esta labor es tan trascendente para la generación de finanzas públicas sanas, como los siguientes aspectos fundamentales que se deben considerar en el personal auditor y en la institución sobre la rendición de cuentas y la fiscalización superior:

Principios para la fiscalización:	Criterios de ejecución de auditorías:	Valores y principios del Código de Ética:
1. Posterioridad 2. Anualidad 3. Legalidad 4. Definitividad 5. Imparcialidad 6. Confidencialidad	1. Profesionalismo 2. Objetividad 3. Imparcialidad 4. Honestidad 5. Confidencialidad 6. Responsabilidad 7. Integridad 8. Neutralidad	1. Profesionalismo competente 2. Independencia 3. Objetividad 4. Imparcialidad 5. Confidencialidad 6. Actitud constructiva 7. Integridad

Figura 19, Aspectos fundamentales a considerar sobre la rendición de cuentas y la fiscalización superior.
Fuente: elaboración propia con base en. (Auditoría Superior de la Federación, 2013)

Estos aspectos forman parte de la cultura organizacional que se trasmite a los empleados en todos los niveles jerárquicos. Asimismo, para las funciones de la

ASF, es muy importante que el servidor público conduzca su actuación con transparencia, honestidad, lealtad, cooperación, austeridad, sin ostentación y con una clara orientación al interés público, tal como lo marca el Código de Ética de los servidores públicos del gobierno federal.

Ahora bien, la estructura de la Auditoría Superior de la Federación se puede conocer fácilmente por medio de su organigrama, el cual está representado de forma general de acuerdo con sus funciones y facultades que tiene para la fiscalización de los diferentes programas federales, a continuación, se representa gráficamente:

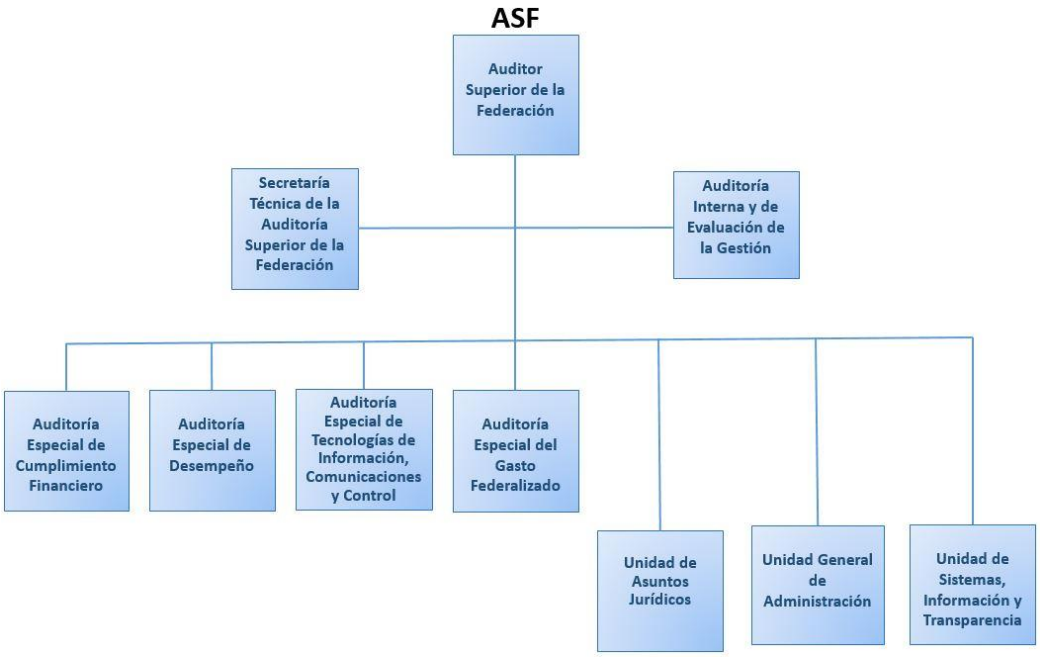

Figura 20, Estructura orgánica de la ASF. Fuente: (Auditoría Superior de la Federación, 2018)

La estructura jerárquica antes mostrada se debe a la especialización de los tipos de auditoría que cada área realiza, los cuales son los siguientes (Auditoría Superior de la Federación, 2018):

Conforme al marco de normas profesionales de auditoría emitido por la Organización Internacional de las Entidades Fiscalizadoras Superiores, existen tres modalidades de auditoría gubernamental: cumplimiento, financiera y desempeño,

de los cuales la ASF practica dos tipos de revisiones: de cumplimiento financiero y de desempeño. A continuación, se describen estas dos categorías junto con los enfoques que se derivan de ellas.

1.Auditoría de cumplimiento financiero

Se revisa que la recaudación, captación, administración, ejercicio y aplicación de recursos aprobados por el Congreso se lleven a cabo de acuerdo con la normativa correspondiente y que su manejo y registro financiero haya sido correcto.

Bajo este rubro se incluyen las siguientes cinco modalidades:

- Auditoría de inversiones físicas: Su materia de análisis son los procesos de adquisición, el desarrollo de las obras públicas, la justificación de las inversiones, el cumplimiento de los estándares de calidad previstos, la razonabilidad de los montos invertidos, así como la conclusión de las obras en tiempo y forma.
- Auditoría forense: Consiste en la aplicación de una metodología de fiscalización que conlleva la revisión rigurosa y pormenorizada de procesos, hechos y evidencias, con el propósito de documentar la existencia de un presunto acto irregular.
- Auditoría a las tecnologías de la información y comunicaciones: En estos enfoques se revisan las adquisiciones, administración, aprovechamiento de sistemas e infraestructuras, calidad de los datos y la seguridad de la información de las entidades públicas.
- Auditoría a los sistemas de control interno: Se evalúan las políticas, procesos y actividades que aseguran el cumplimiento de los objetivos institucionales.
- Auditoría al gasto federalizado: Consiste en fiscalizar el uso de los recursos y el cumplimiento de metas y objetivos de los fondos y programas financiados con recursos federales transferidos a estados y municipios, para renglones como educación, salud, creación de infraestructura básica, abatimiento de la pobreza y seguridad pública. De la misma forma, bajo este rubro se revisan las Participaciones Federales.

2.Auditoría de desempeño

Se orienta a evaluar el grado de cumplimiento de metas y objetivos de los programas gubernamentales; si éstos fueron ejecutados con eficacia, eficiencia y economía, así como la verificación de su impacto social y económico y los correspondientes beneficios para la ciudadanía.

3.Actividades complementarias

La ASF lleva a cabo las siguientes actividades complementarias que representan una óptica distinta a la de la fiscalización tradicional y que permiten contar con análisis y perspectivas complementarias sobre temas de impacto en materia de gestión pública.

Evaluaciones de políticas públicas: Se evalúa si las decisiones del Estado que involucran recursos presupuestales para abordar problemas específicos han tenido como resultado, efectivamente, la atención del asunto público. En particular, se analizan los cambios producidos por la acción gubernamental en comparación con lo pretendido.

Estudios: Se refieren a investigaciones de temas diversos que coadyuvan a obtener una imagen integral de la implementación de las políticas públicas y su impacto sobre el desarrollo del sector gubernamental.

Resultados del proceso de fiscalización

Una vez concluidas las auditorías que fueron programadas, la ASF integra Informes Individuales, los cuales, se entregan a la Cámara de Diputados a través de la Comisión de Vigilancia de la Auditoría Superior de la Federación, el último día hábil de los meses de junio y octubre, así como el 20 de febrero del año siguiente al de la presentación de la Cuenta Pública. Asimismo, en esta última fecha, se entrega el Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

La ASF está obligada legalmente a mantener reserva y secrecía sobre los resultados y contenido de las auditorías, hasta que se entregan a la Cámara de Diputados. A partir de ese momento son de carácter público y se ponen a la disposición de la ciudadanía a través del sitio web de la ASF (Auditoría Superior de la Federación, 2018).

La importancia de la ASF y el impacto de sus actividades se puede constatar en el monto de las recuperaciones derivadas de la fiscalización superior y de los procedimientos resarcitorios (observaciones no atendidas), muestra de esto son los $114,801,145.4 miles de pesos y los $2,126,456.7 miles de pesos recuperados respectivamente en el periodo de las cuentas públicas 2001 a 2016 de acuerdo con (Granados Martin del campo, 2018). Las cifras antes mencionadas manifiestan la trascendencia de sus actividades y por ende el valor de mantener la seguridad en la información que procesa.

Capítulo 5. Análisis de los datos

5.1 Estado actual de la conciencia en seguridad de la información en la ASF

Como se mencionó en el capítulo anterior, la Dirección General de Auditoría a los Recursos Federales Transferidos “B” (DGARFT”B”) es en donde se realizará la evaluación de la concientización y cultura en seguridad de la información en el proceso de auditoría. La DGARFT”B” es parte de la Auditoría Especial de Gasto Federalizado, quien se encarga de las auditorías de Cumplimiento Financiero y tiene por objetivo; revisar que la recaudación, captación, administración, ejercicio y aplicación de recursos aprobados por el Congreso se lleven a cabo de acuerdo con la normativa correspondiente y que su manejo y registro financiero haya sido correcto.

La Auditoría al Gasto Federalizado como lo menciona la ASF (Auditoría Superior de la Federación , 2018) en su portal web, consiste en: fiscalizar el uso de los recursos y el cumplimiento de metas y objetivos de los fondos y programas financiados con recursos federales transferidos a estados y municipios, para renglones como educación, salud, creación de infraestructura básica, abatimiento de la pobreza y seguridad pública. De la misma forma, bajo este rubro se revisan las Participaciones Federales.

Por lo anterior, las actividades que se llevan a cabo por las auditorías realizadas por la DGARFT”B” tienen injerencia en múltiples entidades de la Administración Pública, al tener acceso a información financiera para la revisión del gasto público. Por lo tanto, la información que manejan es muy sensible y su gestión tiene que ser sumamente controlada, por esta razón, de acuerdo con las normas y mejores prácticas es crucial que toda organización cuente con una cultura en seguridad de la información, y el presente estudio está enfocado a conocer el nivel que tiene la ASF en este rubro y los beneficios que conlleva su adopción.

A continuación, se muestra el organigrama de la Dirección General de Auditoría a los Recursos Federales Transferidos “B” (DGARFT”B”), objeto del presente estudio.

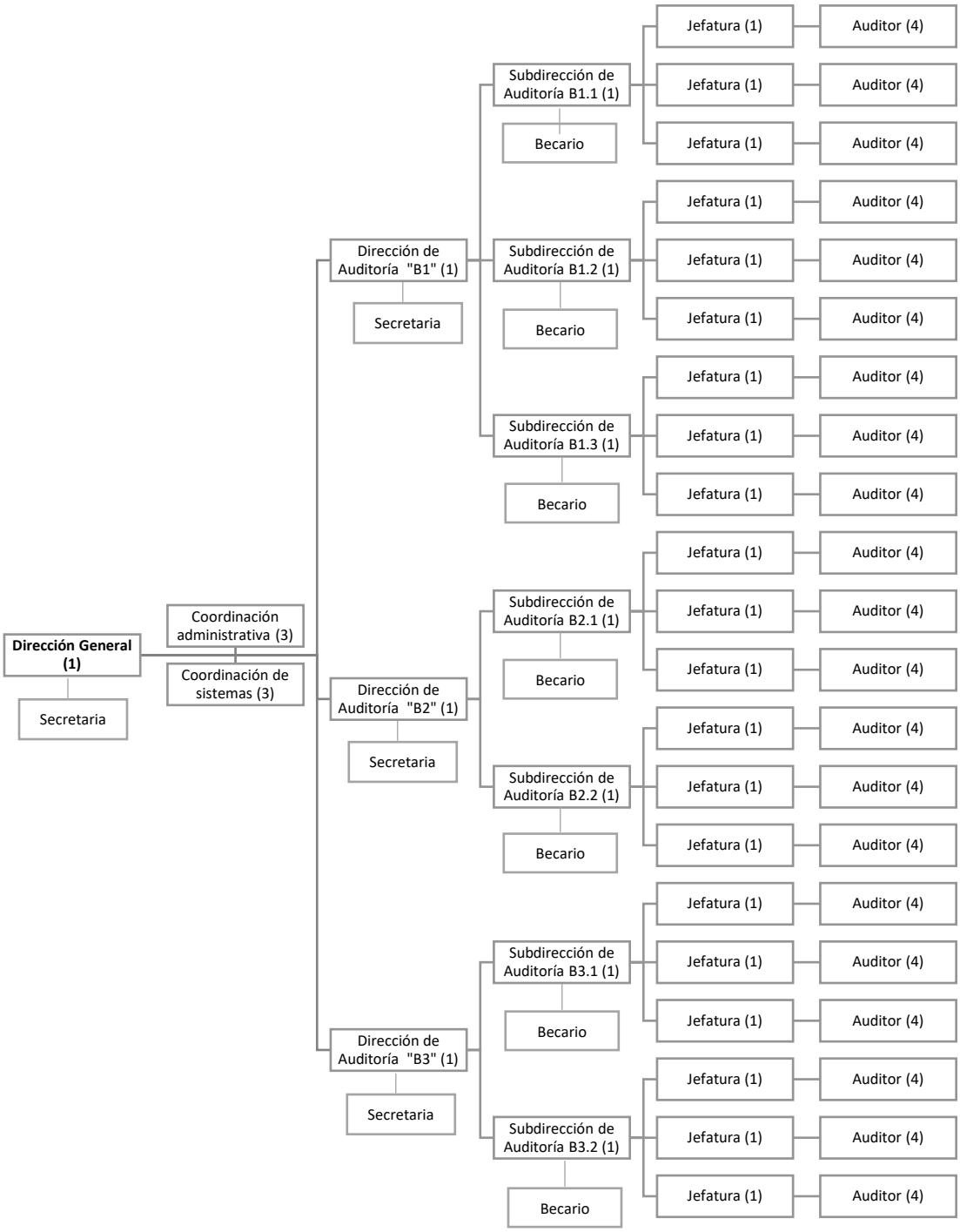

Figura 21, Organigrama de la Dirección General de Auditoría a los Recursos Federales Transferidos “B” (DGARFT”B”). Fuente: elaboración propia con base en (Dirección General de Administración de la ASF, 2010)

5.1.1 Aplicación de los métodos de recolección de datos

5.1.1.1 Análisis documental

El primer método de recolección de datos que se realizó para este estudio y que se describe en el capítulo 4, es el: *Análisis documental*, lo anterior consta en verificar que documentalmente la ASF cuenta con lineamientos, políticas, manuales, entre otros documentos, que acrediten que esta institución cuenta con medidas específicas orientadas a la seguridad de la información y la vinculación que tiene el área emisora y los usuarios finales, para lo cual, se realizó lo siguiente:

Se entrevistó al coordinador de sistemas de la DGARFT"B" y al coordinador de la Dirección de Infraestructura Tecnológica de la Dirección General de Sistemas (DGS), este último esta encargada de lo relativo a la seguridad y control de riesgos de la ASF, en dicha entrevista se realizó un cuestionario (ver anexo A) el cual se basó, para su elaboración, en lo recomendado por la norma ISO 27002, los resultados más sobresalientes son:

- La Auditoría Superior de la Federación cuenta con una subdirección denominada: *Subdirección de Seguridad y Control de Riesgos*, la cual, se encarga de todo lo relativo a la seguridad de la información y seguridad informática.
- La ASF aún no cuenta con una certificación en Seguridad de la Información como la ISO 27001, sin embargo, si se apega a ciertos aspectos como contar con un Plan en Seguridad de la Información que contiene documentos como:
    - Política de gestión de contraseñas
    - Política de uso de software
    - Política de gestión de usuarios

    (se exhibieron al momento de la entrevista diversos archivos digitales con políticas orientadas a la seguridad de la información, así como el manual de procedimientos de la Dirección General de Sistemas)

- El personal perteneciente a la DGS en su mayoría tiene perfiles profesionales como licenciados en informática, ingenieros en sistemas e ingenieros en computación. Ocasionalmente la ASF capacita al personal en temas de seguridad informática, sin embargo, no existe un plan de capacitación ni exige certificaciones especificas al personal.
- Existen canales de comunicación que estableció la DGS con los usuarios (correo electrónico y personal enlace con cada Dirección General), regularmente la mayoría de los comunicados se hacen llegar a los empleados vía correo electrónico, lo anterior con la finalidad de distribuir información relativa a las operaciones de los sistemas o recomendaciones en seguridad de la información que de manera directa involucra a los usuarios.
- La clasificación de la información se lleva a cabo de manera adecuada conforme a lo establecido por la Ley General de Transparencia y Acceso a la Información Pública.
- Las principales medidas para el control de acceso a aplicaciones, servicios en general y sistemas internos como:
    - Sistema de Control de Seguimiento de auditoría (SICSA)
    - Sistema de Seguimiento de denuncias
    - Sistema de control de adquisiciones
    - Sistema de reserva de salas

    Las cuentas son asignadas a personal específico siguiendo los criterios de; puesto y actividades encomendadas. Estas cuentas están protegidas con un usuario y contraseña, sin embargo, en la práctica suelen “prestarse” dichas cuentas entre los usuarios.

    También, todos los empleados tienen una computadora asignada con usuario y contraseña, esta última cumple con los criterios alfanuméricos y de símbolos recomendados para ser considerada como una contraseña “segura”, la cual se cambiada cada 90 días.

    Asimismo, las medidas de seguridad física se basan en:

- Personal de vigilancia las 24 horas del día, haciendo rondines de manera recurrente a lo largo de las instalaciones y se apoyan con cámaras de vigilancia.
- El acceso a las instalaciones es por medio de una credencial de identificación con chip para liberar los torniquetes de la entrada principal al edificio.
- Escaneo de los bolsos y maletas en la entrada del edificio por medio de una banda transportadora.
- Existe una política de que todas las computadoras portátiles deberán tener un candado que las sujete al escritorio.
- La Oficialía de Partes es el área encargada de recibir toda la documentación impresa, en CD o en USB y que forma parte de los requerimientos para las auditorías.

Cabe mencionar que lo descrito anteriormente se constató mediante la presentación de pruebas documentales, por parte de los coordinadores, como archivos digitales y la inspección física de las instalaciones y equipos informáticos.

Algunas evidencias son las capturas de pantalla de la intranet en donde se encuentran distintos servicios disponibles para los empleados, como los mostrados en las figuras 22 y 23.

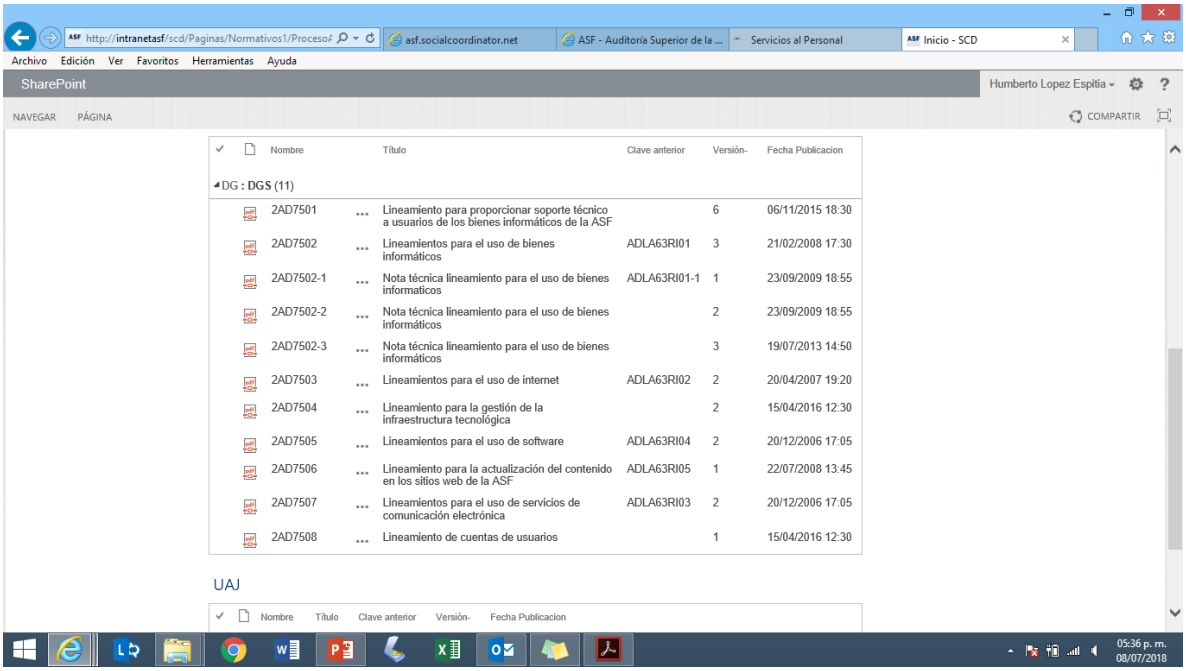

Figura 22, Captura de pantalla como evidencia de lineamientos informáticos publicados en la intranet de la ASF. Fuente: elaboración propia.

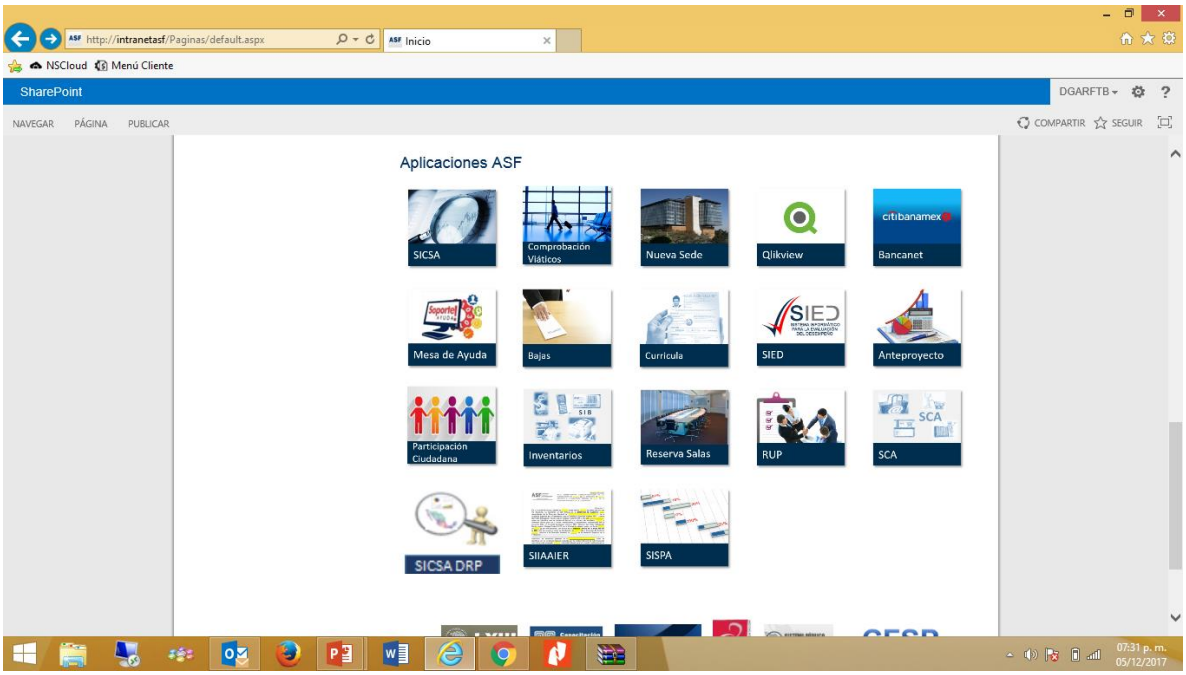

Figura 23, Captura de pantalla como evidencia de servicios disponibles en la intranet de la ASF. Fuente: elaboración propia.

El otro punto evaluado en el análisis documental es: “información circulante, relativa a la vinculación entre la DGS y los usuarios”, para ello, se realizó una revisión aleatoria de las computadoras de los usuarios de distintas direcciones, de esta manera se pudo recopilar lo siguiente:

La Dirección General de Sistemas comunica frecuentemente a los usuarios sobre los cambios en los sistemas, como se muestra en la figura 24.

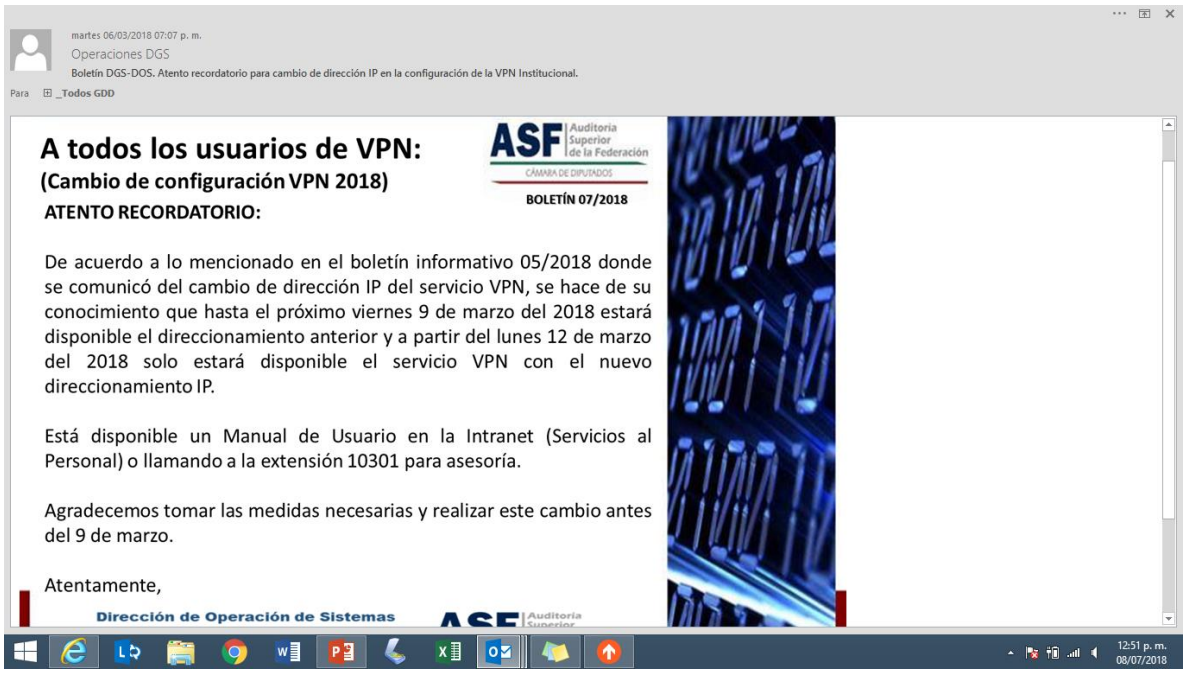

Figura 24, Captura de pantalla como evidencia de comunicados de la DGS de cambios en los sistemas informáticos. Fuente: elaboración propia.

Asimismo, se recopiló evidencia de los comunicados en materia de seguridad informática que la DGS hace llegar a los usuarios por medio de correo electrónico, como se muestra en las figuras 25 y 26.

Figura 25, Captura de pantalla como evidencia de comunicados de la DGS a usuarios sobre amenazas informáticas. Fuente: elaboración propia.

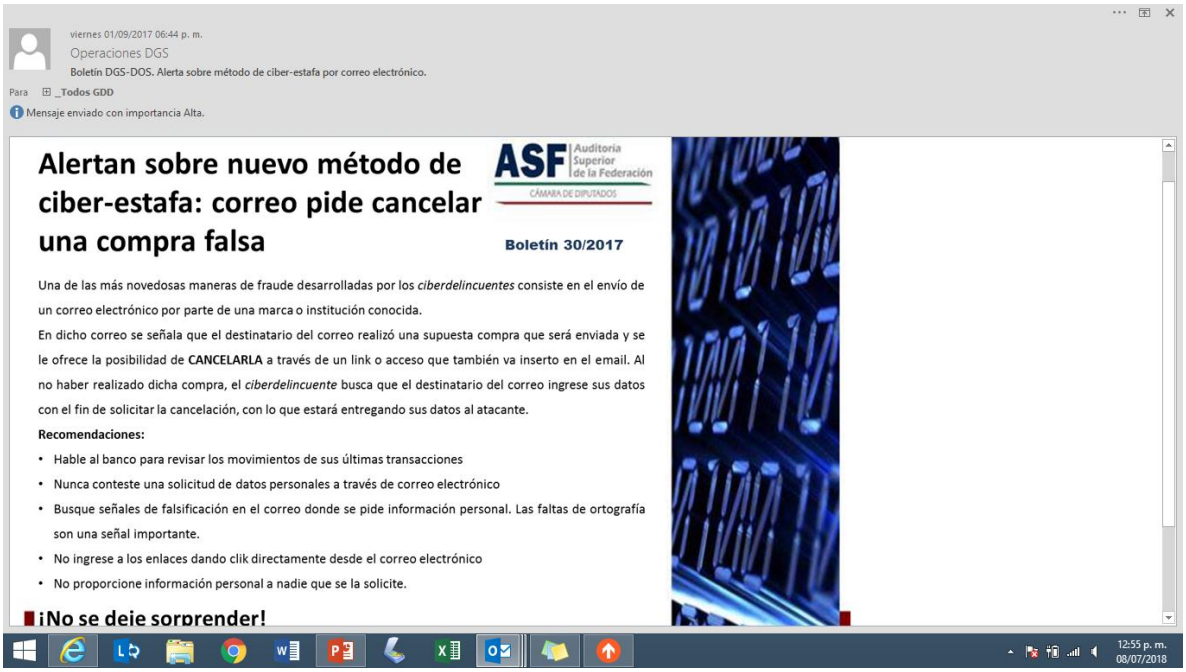

Figura 26, Captura de pantalla como evidencia de comunicados de la DGS a usuarios sobre amenazas informáticas. Fuente: elaboración propia.

Lo comunicación de la DGS con los usuarios finales radica principalmente por correo electrónico y en ocasiones a través del personal de sistemas en cada una de las direcciones generales, sin embargo, en muchas ocasiones estos correos suelen ser ignorados por los usuarios, lo que ha causado que disminuya la efectividad del canal de comunicación.

5.1.1.2 Pruebas informáticas

Las pruebas informáticas se realizaron para conocer de manera general el estado de seguridad de la información que tiene la ASF con respecto a servicios dirigidos a usuarios finales, tales como: página web y servicio de navegación de internet a empleados.

5.1.1.2.1 Verificación de sitio web

Se utilizó una herramienta de verificación de sitios web de CA Security Council, esta organización tiene como propósito la exploración y promoción de las mejores prácticas que promueven la implementación confiable de SSL (Secure Sockets Layer, protocolo para navegadores y servidores web) y las operaciones de CA (autoridad de certificación), así como la seguridad de internet en general.

La verificación del sitio web se realizó en el siguiente enlace https://casecurity.ssllabs.com/, como se muestra en la figura 27.

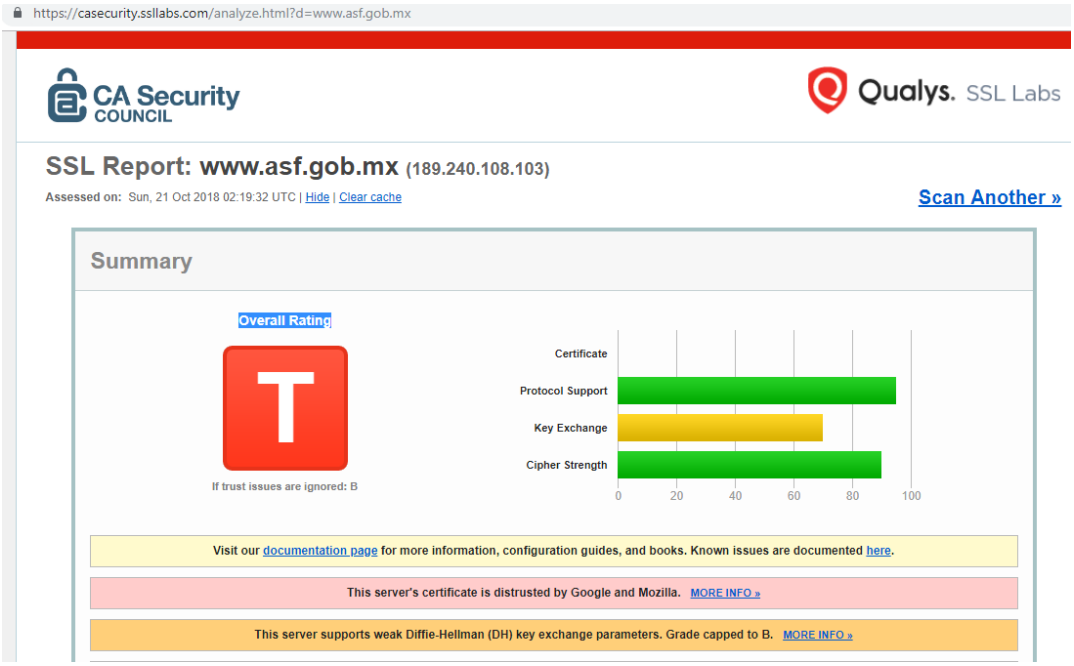

Figura 27, Captura de pantalla de la evaluación de sitio web en https://casecurity.ssllabs.com/. Fuente: elaboración propia.

La calificación que se obtuvo de la página www.asf.gob.mx es: no confiable, debido a problemas en las categorías de: certificado inválido, configuración inválida y autoridad de certificación desconocida. A pesar de que para la ASF no es necesario cumplir con protocolos de seguridad web más estrictos, ya que, solo es una página de consulta, es importante que cumpla con las actualizaciones de sus certificados web, para obtener una calificación de: confiable. El resultado de la evaluación completa se encuentra en el Anexo B.

5.1.1.2.2 Aplicación de prueba de navegador anónimo

Se realizó una prueba de navegador anónimo con la intención de verificar el filtrado de contenido que tiene la ASF con respecto a la navegación de internet para los distintos usuarios.

Para esta prueba se utilizó el navegador anónimo *Tor Browser*, el cual, nos ayudó a constatar si era posible o no entrar a distintas páginas web clasificadas comúnmente como no recomendables o con contenidos violentos, de apuestas o

contenidos sexuales, que son considerados no apropiados para ambientes laborales. Cabe destacar la relevancia de implementar filtrado de contenido en la navegación a internet, debido a que muchos ataques cibernéticos se realizan por medio de portales web falsos a los que son atraídos algunos usuarios por medio de prácticas como el phishing.

La práctica consistió en tratar de instalar el programa Tor Browser en una laptop destinada a los auditores, para lo cual, se seleccionó una aleatoriamente, obteniendo los siguientes resultados:

- No fue posible instalar el programa en la laptop debido a las reglas de acceso y contenido que han sido configuradas en los equipos de cómputo por parte de la administración de sistemas, además de haber existido una alerta por parte del antivirus Tren Micro. Lo cual, se puede observar en la figura 28.

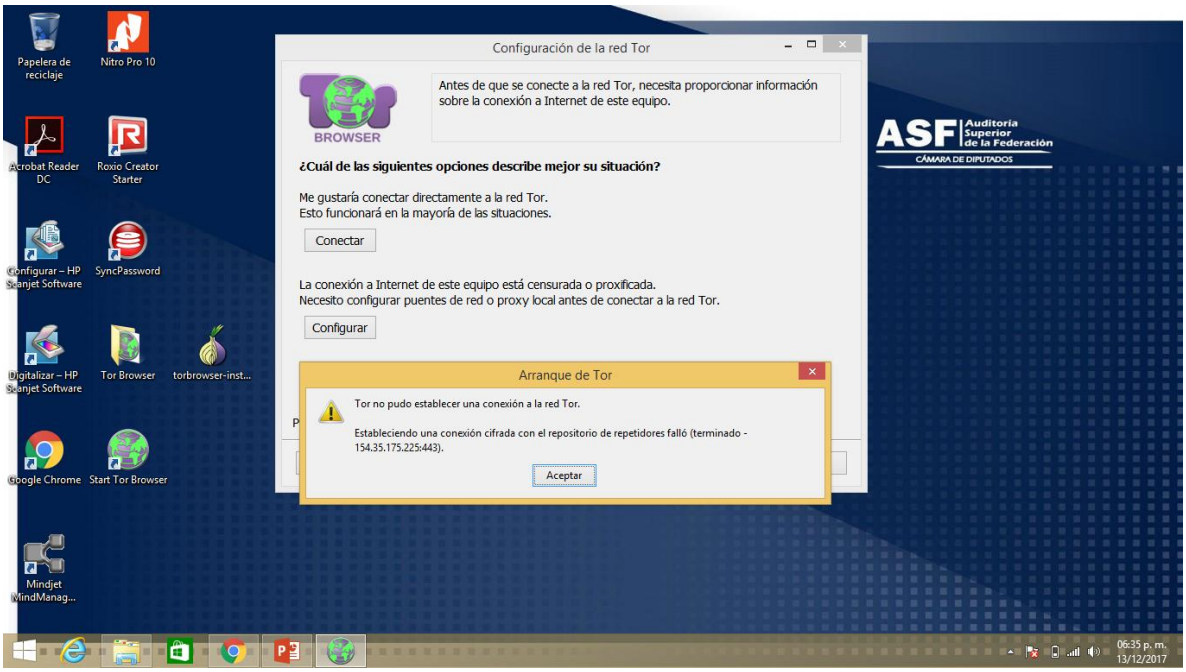

Figura 28, Captura de pantalla de prueba de instalación del programa Tor Browser. Fuente: elaboración propia.

- Se constató que existe filtrado de contenido web haciéndose pruebas de búsqueda en los distintos navegadores web (Explorer, Firefox, Mozilla y Google Chrome) para intentar iniciar sesión en: redes sociales, correo electrónico personal, YouTube, páginas de videojuegos online, páginas con contenido sexual, estos intentos fueron bloqueados por la herramienta de ForcePoint que se encuentra instalada y es parte de las políticas implementadas por la DGS. Como se muestra en las figuras 29 y 30.

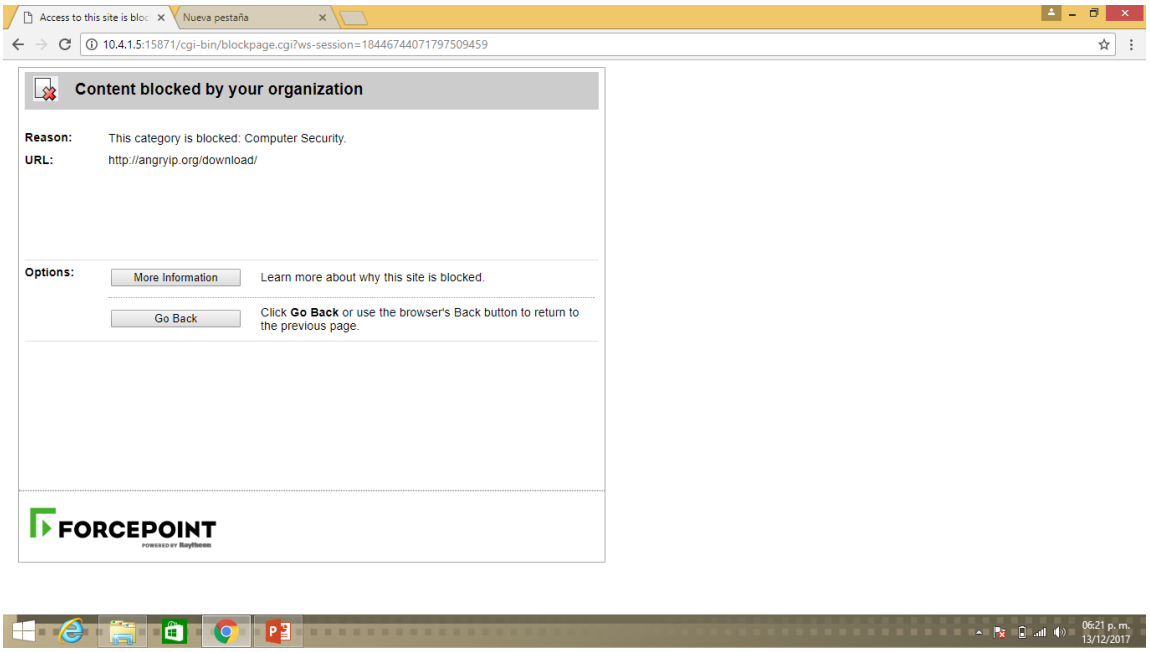

Figura 29, Captura de pantalla de prueba de filtrado de contenido web para páginas de videojuegos, apuestas y de contenido sexual. Fuente: elaboración propia.

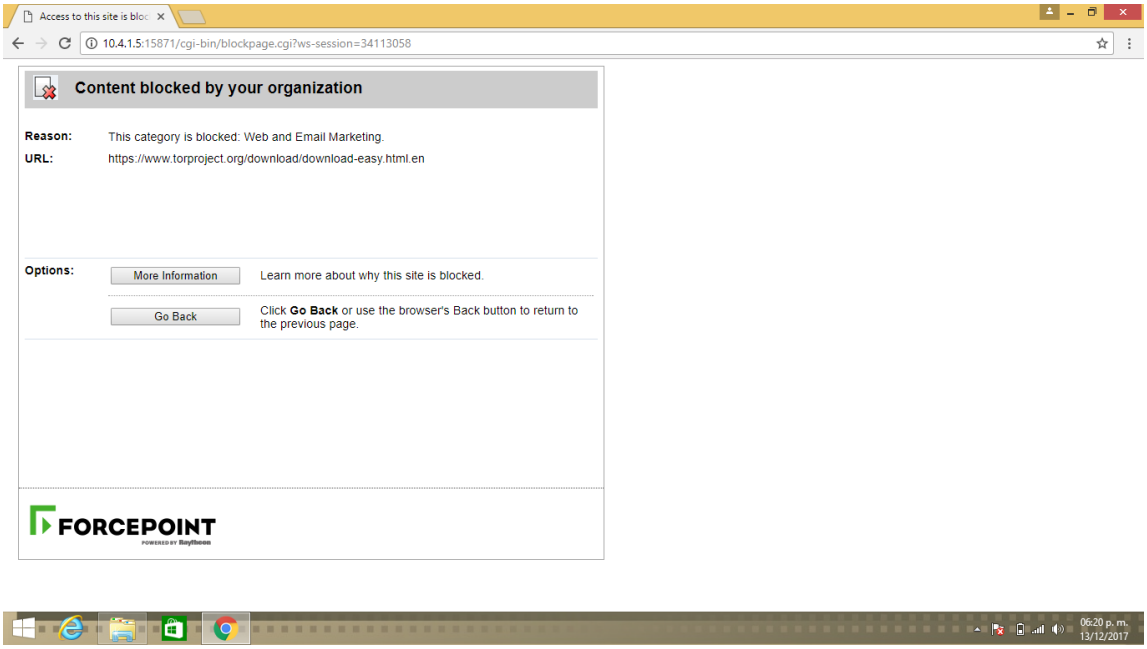

Figura 30, Captura de pantalla de prueba de filtrado de contenido web para inicio de sesión en correo personal. Fuente: elaboración propia.

Las pruebas de filtrado de contenido en la red constataron que las políticas que se encuentran documentadas y que anteriormente fueron exhibidas por la DGS son efectivamente aplicadas y se encuentran reguladas.

5.1.1.2.3 Aplicación de Angry IP Scanner (para conocer número de computadoras en red)

Angry IP Scanner es una herramienta que ayuda a conocer el número de dispositivos conectados a una red por medio de un escáner de direcciones IP. Se aplicó esta herramienta en la red de la DGARFT “B” instalando el programa en una laptop seleccionada aleatoriamente con la finalidad de observar de manera general la arquitectura de red que tienen implementada, ya que, cabe mencionar que una buena práctica en seguridad de la información es tener seccionada la red de acuerdo con los servicios prestados y su nivel de importancia, para disminuir vulnerabilidad frente a los posibles ataques cibernéticos.

Una muestra de la aplicación de la prueba se puede visualizar en las figuras 31 a 33.

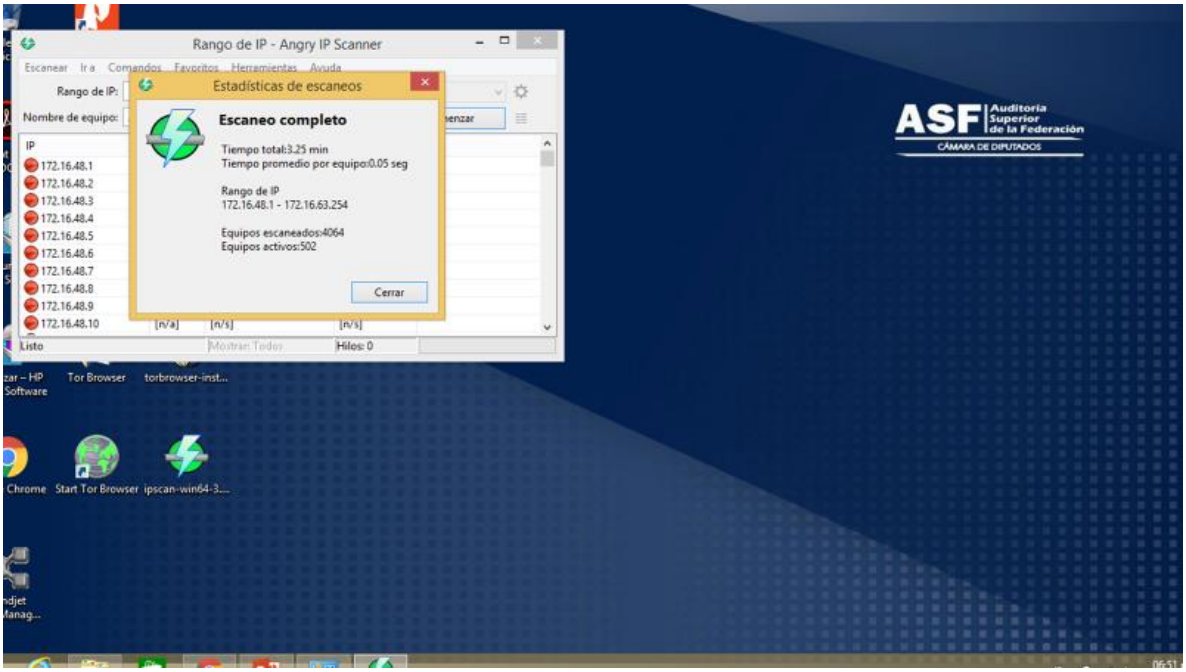

Figura 31, Captura de pantalla de prueba de escáner de direcciones IP, total de dispositivos encontrados. Fuente: elaboración propia.

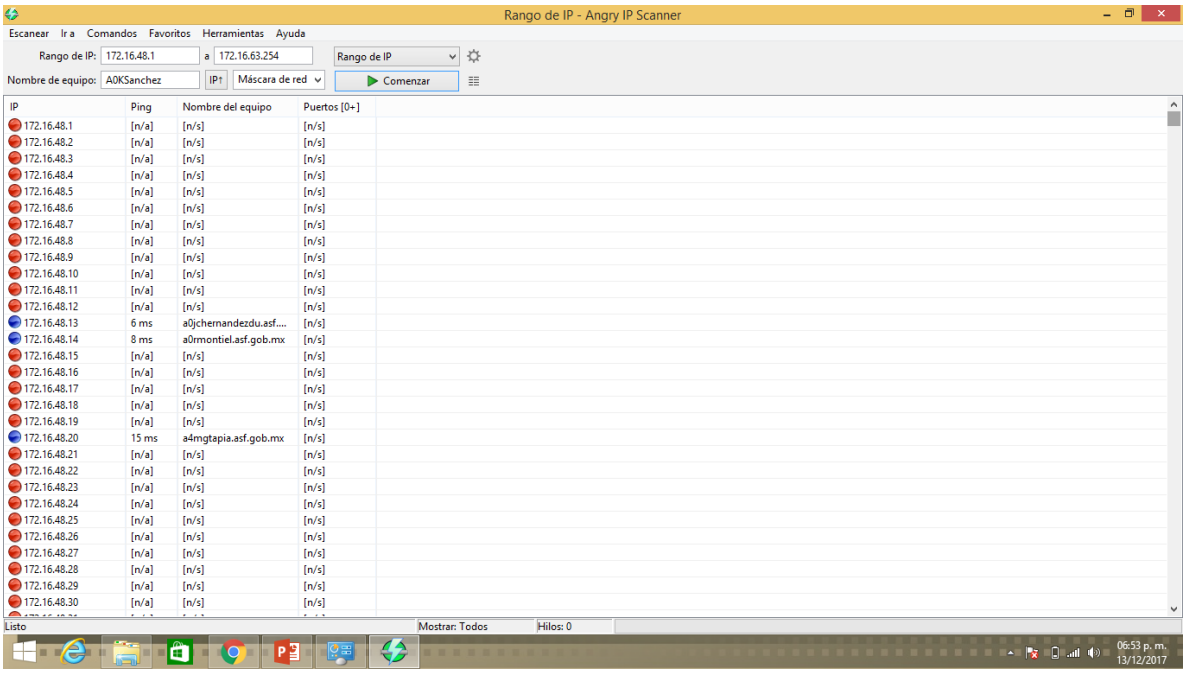

Figura 32, Captura de pantalla de prueba de escáner de direcciones IP, ejemplo de dispositivos. Fuente: elaboración propia.

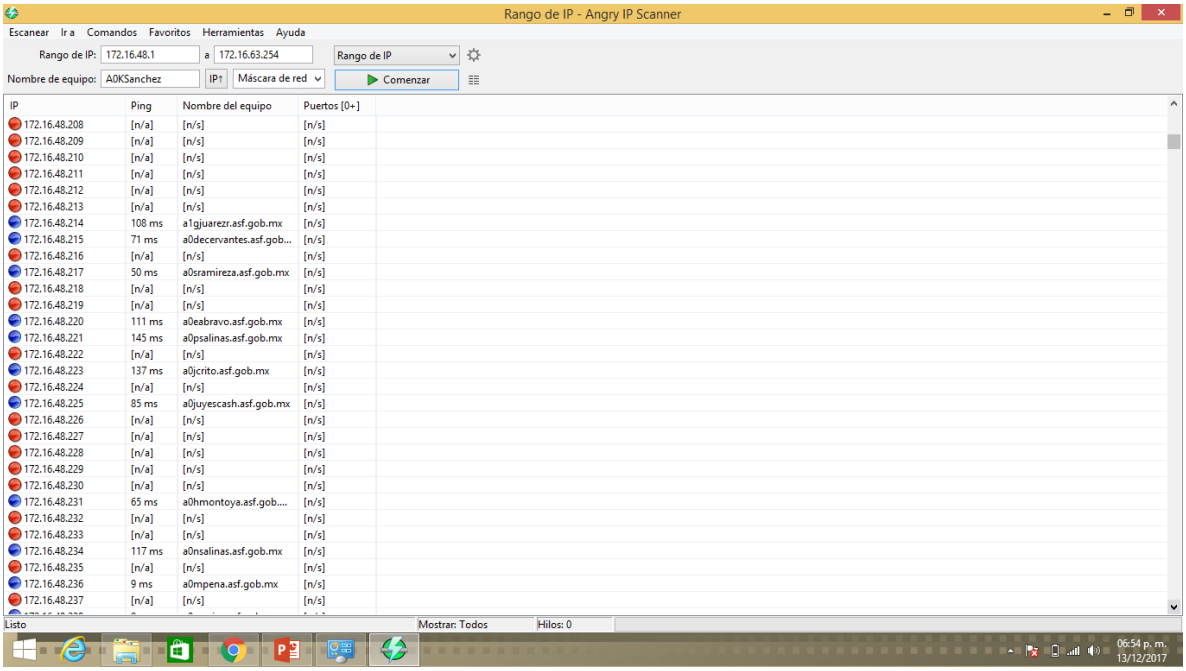

Figura 33, Captura de pantalla de prueba de escáner de direcciones IP, ejemplo de dispositivos. Fuente: elaboración propia.

Las figuras anteriores muestran un total de 4,064 equipos detectados, de los cuales, 502 equipos están activos, con esto se constata que probablemente no existe un adecuado diseño de red por ser demasiado alto el número de equipos conectados y tan bajo el número de equipos activos, lo que puede aumentar el riesgo de vulnerabilidad.

5.1.1.2.4 Aplicación de prueba de ataque dirigido.

En la DGARFT"B" se aplicó una prueba recomendada por el Instituto Nacional de Ciberseguridad Español (INCIBE), dicha prueba se basó en la presencia de un fichero infectado en una memoria USB extraviada, el cual, al ser ejecutado, muestra al usuario un portal web del INCIBE advirtiéndole del peligro que supone lo que acaba de hacer.

Cabe destacar que se eligió aplicar esta prueba debido a que una de las principales fuentes de infección en las organizaciones y en los hogares es a través de malware alojado en dispositivos de almacenamiento externos, usualmente memorias USB. Por esta razón, es fundamental el concientizar a los usuarios de las posibles consecuencias que puede conllevar el mal uso de esos dispositivos tecnológicos y en los que con regularidad se recibe información confidencial por parte de las entidades fiscalizadas.

La presente prueba tuvo como objetivo mostrar al usuario que el hecho de encontrarse una USB y acceder al contenido interno del mismo, puede provocar una infección en su equipo y propagarse por toda la infraestructura de la empresa. Para ello, se preparó un fichero infectado que se obtuvo del sitio web del INCIBE como parte del kit de concientización que recomienda este instituto, dicho archivo fue almacenado en dos memorias USB y fueron «perdidas» en dos lugares visibles dentro de las oficinas de la Dirección General.

La prueba se aplicó durante un día en un horario de 10:00 am a 7:00 pm, periodo durante el cual se reportaron, por parte de los usuarios, los siguientes resultados:

- Se reportaron 4 incidentes de un total de 38 personas presentes en el área de la DGARFT”B”.
- De las dos USB puestas para la prueba, solo una fue regresada al coordinador de sistemas, por lo que, se desconoce el total de incidentes que pudieron darse con la otra USB.

A continuación, se muestra la pantalla que abre el fichero infectado, como prueba de lo fácil que puede ser infectar un equipo cuando el personal desconoce los principios básicos de seguridad de la información.

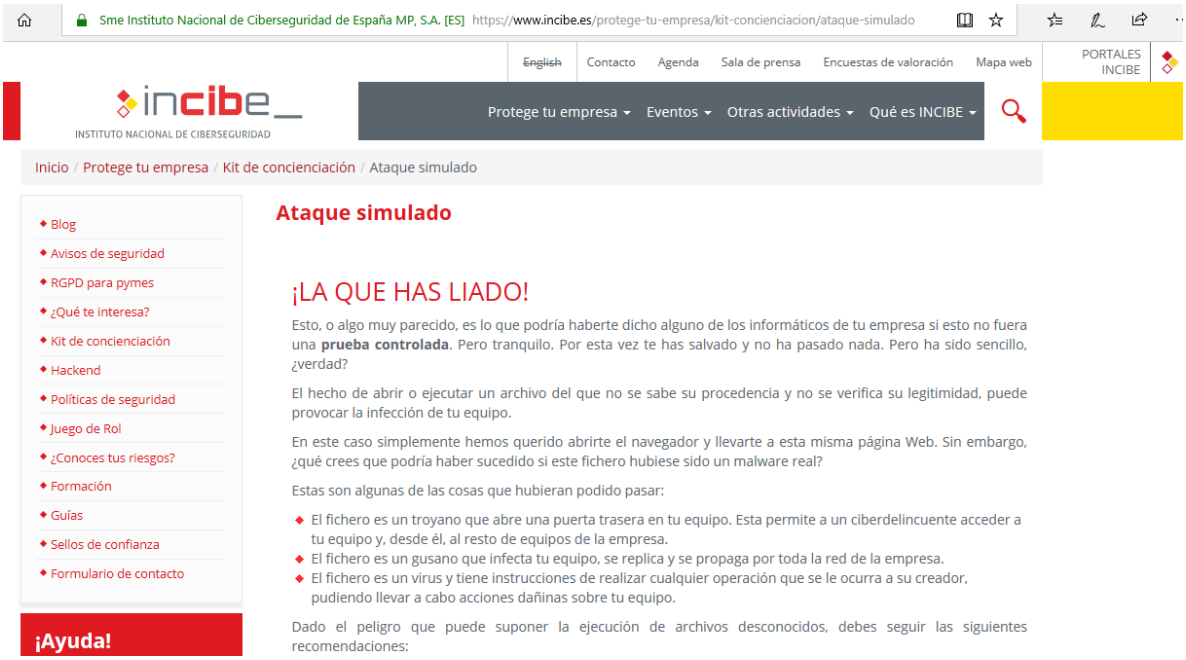

Figura 34, Captura de pantalla de prueba de ataque dirigido en la DGARFT"B". Fuente: elaboración propia.

La captura de pantalla anterior es el texto mostrado una vez que la persona abre el fichero infectado y que, a su vez, el personal confirmó haber participado en la prueba intencionalmente.

5.1.1.3 Uso de los activos informáticos y cultura en seguridad de la información

Antes de la aplicación del cuestionario y entrevistas a empleados para conocer el grado de concientización y cultura en seguridad de la información, se realizó un levantamiento de perfiles de usuarios e infraestructura tecnológica que tiene para su uso la DGARFT"B", con el objetivo de identificar posteriormente posibles vulnerabilidades entre las políticas establecidas y el actuar en sus labores cotidianas de los usuarios.

En la Dirección General, hay un total de 129 usuarios, cuyos perfiles se describen a continuación:

Perfiles de usuarios de la DGARFT"B"		
Usuario	**Dispositivo**	**Uso**
Director General	Computadora de escritorio	-Uso de paquetería Microsoft Office -Visualización de PDF -Uso de sistemas internos (SICSA, SISPA, Comprobación de viáticos) -Uso de la intranet -Navegación Web en general con Google Chrome o Explorer (correo electrónico personal, YouTube)
Coordinación - Administrativa	Computadora de escritorio	-Uso de paquetería Microsoft Office -Visualización y edición de PDF -Uso de sistemas internos (SIAC Comprobación de viáticos, Sistema de reserva de salas) -Uso de la intranet -Navegación Web en general con Google Chrome o Explorer
Coordinación de Sistemas	Computadora de escritorio	-Uso de paquetería Microsoft Office -Visualización y edición de PDF -Uso de sistemas internos (SICSA, SIAC, Comprobación de viáticos) -Uso de la intranet -Navegación Web en general con Google Chrome o Explorer (correo electrónico personal, YouTube)
Director de Área	Computadora de escritorio	-Uso de paquetería Microsoft Office -Visualización de PDF -Uso de sistemas internos (SICSA, Comprobación de viáticos) -Uso de la intranet

		-Navegación Web en general con Google Chrome o Explorer (correo electrónico personal, YouTube)
Subdirector	Laptop	-Uso de paquetería Microsoft Office -Visualización de PDF -Uso de sistemas internos (SICSA, Comprobación de viáticos) -Uso de la intranet -Navegación Web en general con Google Chrome o Explorer (correo electrónico personal, páginas gubernamentales, YouTube)
Jefe de Departamento	Laptop	-Uso de paquetería Microsoft Office -Visualización y edición de PDF -Uso de sistemas internos (SIAC, Comprobación de viáticos) -Uso de la intranet -Navegación Web en general con Google Chrome o Explorer
Auditor	Laptop	-Uso de paquetería Microsoft Office -Visualización y edición de PDF -Uso de sistemas internos (Comprobación de viáticos) -Uso de la intranet -Navegación Web en general con Google Chrome o Explorer

Tabla 8, Perfiles de usuarios de la DGARFT"B". Fuente: elaboración propia.

Cabe destacar que todos los usuarios tienen bloqueado el uso de redes sociales, páginas web con contenido sexual o violento y solo directores, subdirectores y jefes de departamento tienen acceso a su correo electrónico personal. Con estos

controles se comprueba que tienen las medidas básicas de seguridad para la navegación web.

Posteriormente se realizó un conteo de los principales activos informáticos que tiene la dirección general, sus principales usuarios y los posibles riesgos de acuerdo con la experiencia del coordinador de sistemas y la observación visual de las labores del personal durante las visitas que se realizaron.

Activos informáticos físicos y lógicos		
Activo	**Usuario**	**Riesgo**
Laptop (130)	Jefes de Departamento Auditores Becarios	Acceso no autorizado Pérdida de información Pérdida del activo por robo
PC (9)	Director General Directores de Área Coordinador de administración Coordinador de sistemas Secretarias	Acceso no autorizado Pérdida de información
Impresora (6)	Todo el personal	Falta de consumibles Desconexión de la red
Copiadora (4)	Todo el personal	Falta de consumibles Desconexión de la red
Trituradora (5)	Auditores Becarios	Descompostura inesperada
Escáner (70)	Auditores Becarios	Descompostura inesperada
Disco duro portátil (35)	Jefes de departamento Auditores	Pérdida de información Pérdida del activo por robo
Lectores de CD (40)	Jefes de departamento Auditores	Pérdida del activo por robo
Teléfonos Cisco (21)	Todo el personal	Desconexión de la red
Proyectores (2)	Coordinación de sistemas (responsable)	Descompostura inesperada

Equipo de videoconferencia (1)	Coordinación de sistemas (responsable)	Desconexión de la red
Sistema de Control y Seguimiento de auditoría (SICSA)	Director General Directores Subdirectores	Acceso no autorizado Modificación o pérdida de la información
Sistema Institucional de Almacenamiento Centralizado (SIAC)	Todo el personal	Modificación o pérdida de la información
Intranet	Todo el personal	Modificación o pérdida de la información
Sistema de Seguimiento de Denuncias	Director General Directores	Acceso no autorizado Modificación o pérdida de la información
Sistema de Control de Adquisiciones (SCA)	Personal de la Dirección General de Administración	Acceso no autorizado Modificación o pérdida de la información
Sistema para la integración y Seguimiento del Programa de Actividades (SISPA)	Director General Directores	Acceso no autorizado Modificación o pérdida de la información

Tabla 9, Activos informáticos físicos y lógicos Fuente: elaboración propia.

El principal riesgo identificado para los activos es el acceso no autorizado y la pérdida de información, lo anterior, debido a las actividades intrínsecas que conlleva la auditoria. El acceso no autorizado de un externo a información reservada puede generar muchos problemas en el proceso de auditoría, ya que, se estaría incumpliendo el principio de confidencialidad entre la ASF y la entidad fiscalizada, teniendo como consecuencia la cancelación de la auditoría sin repercusión para la entidad fiscalizada. Por esta razón, cualquier alteración, pérdida o robo de información tiene un alto impacto en el proceso de fiscalización, por lo que la seguridad de esta es indispensable.

Una vez que se conoce la infraestructura tecnológica perteneciente a la DGARFT”B” y la administración general de los usuarios que lleva la coordinación de sistemas, se realizaron entrevistas aleatorias a distintos empleados con diferentes puestos, con la finalidad de conocer cómo utilizan comúnmente los distintos activos tecnológicos, el manejo de la información que hacen por medio de ellos y el conocimiento y concientización de la seguridad de la información, para lo cual, algunos de los cuestionamientos y sus resultados son los mostrados en las siguientes figuras:

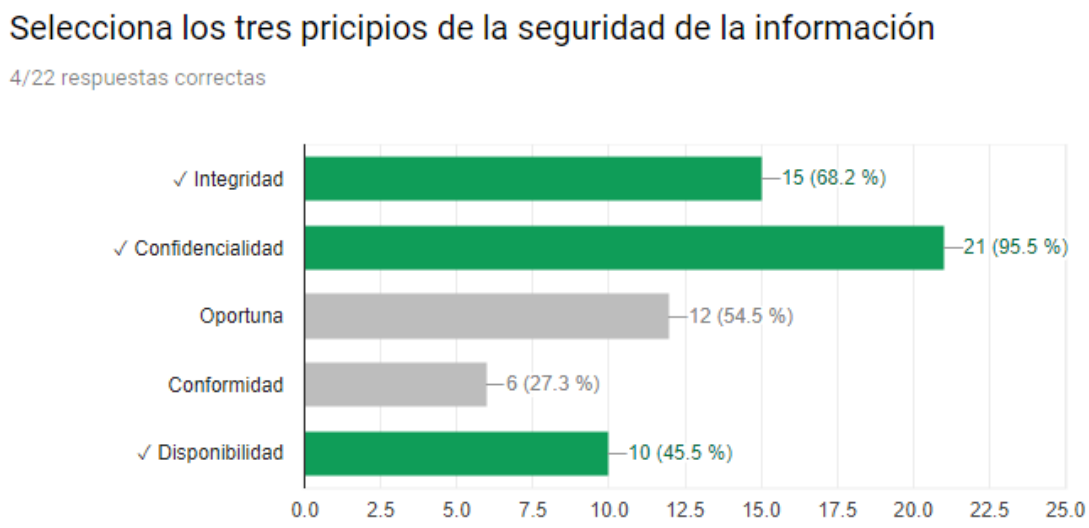

Figura 35, Gráfica de respuestas obtenidas en pregunta orientada a verificar el conocimiento de los usuarios en seguridad de la información. Fuente: elaboración propia.

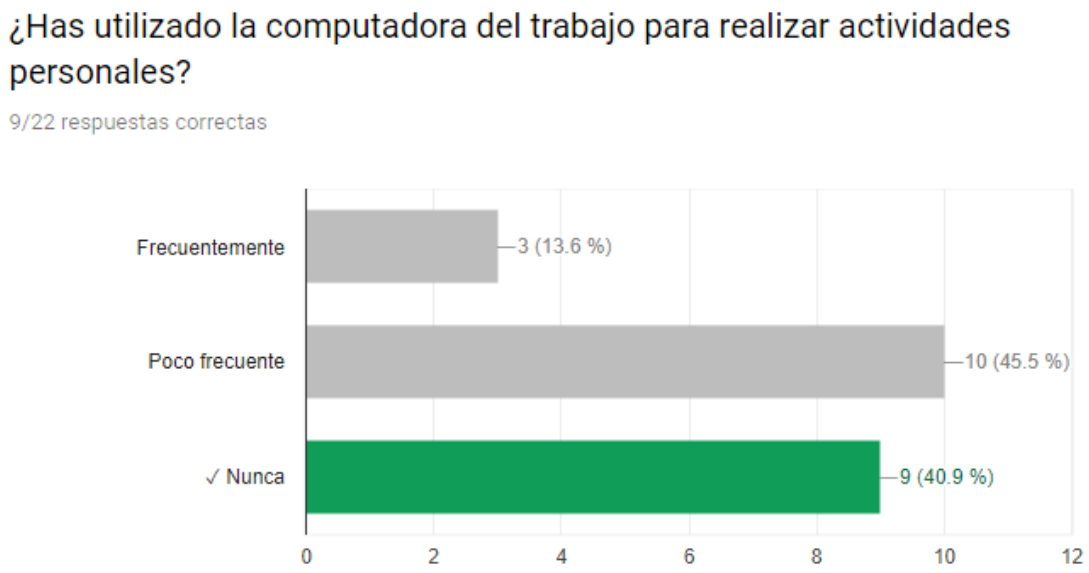

Figura 36, Gráfica de respuestas obtenidas en pregunta orientada a verificar las rutinas de los usuarios. Fuente: elaboración propia.

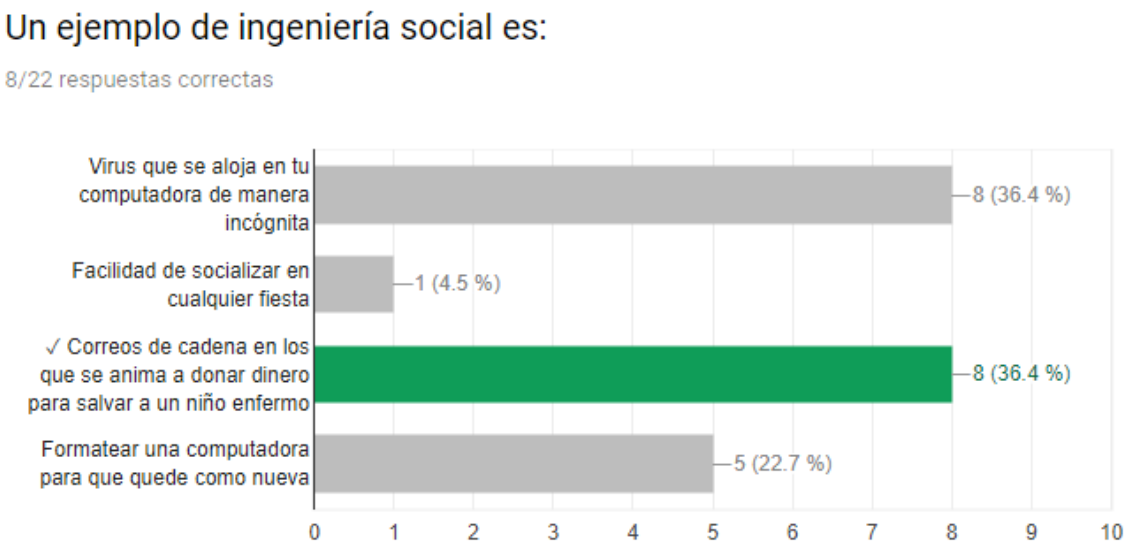

Figura 37, Gráfica de respuestas obtenidas en pregunta orientada a verificar el conocimiento de los usuarios en seguridad de la información. Fuente: elaboración propia.

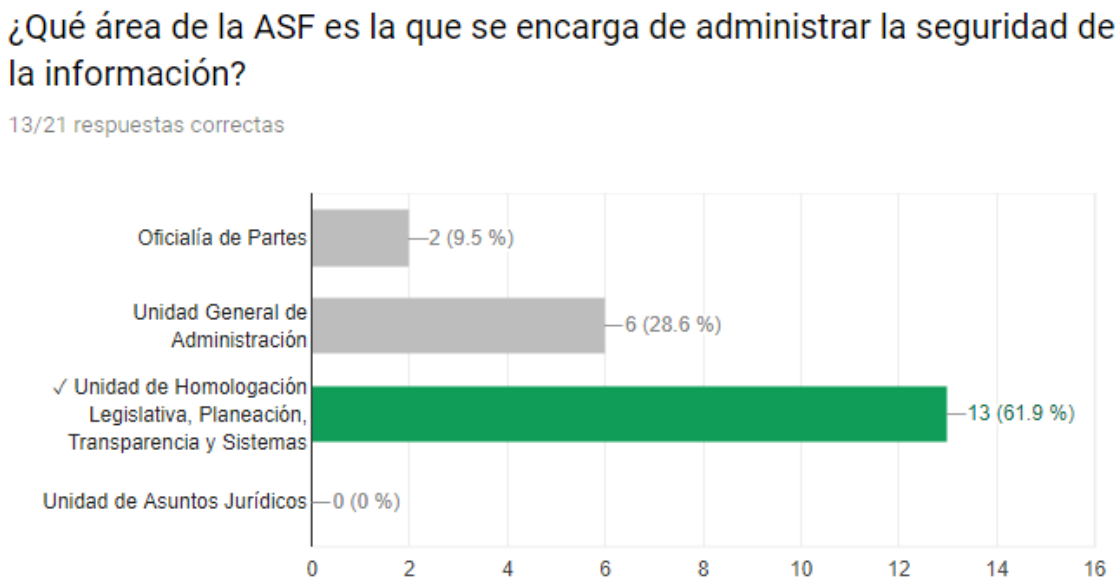

Figura 38, Gráfica de respuestas obtenidas en pregunta orientada a verificar la vinculación entre la ASF y los usuarios. Fuente: elaboración propia.

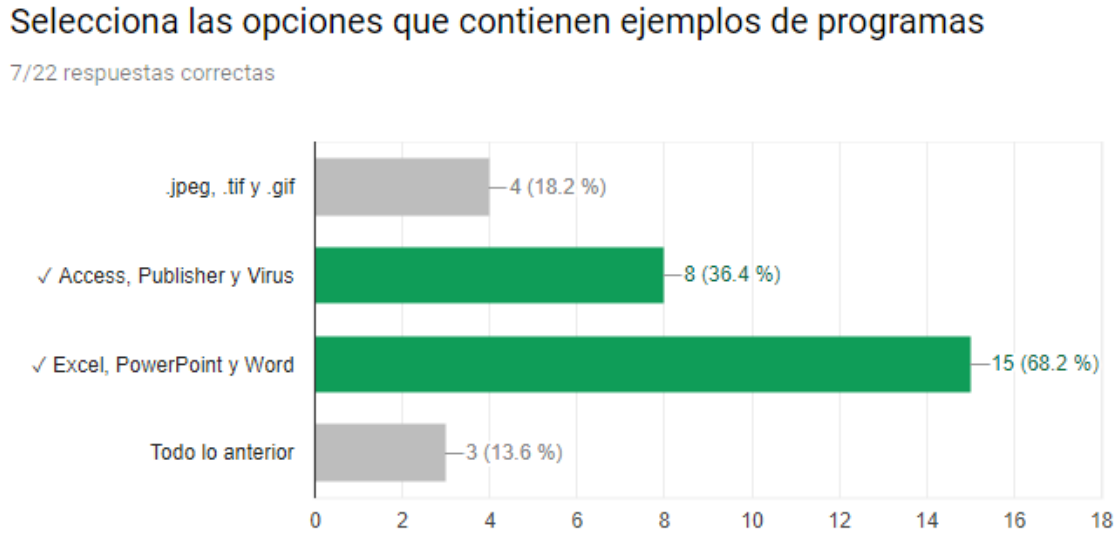

Figura 39, Gráfica de respuestas obtenidas en pregunta orientada a verificar el conocimiento de los usuarios en seguridad de la información. Fuente: elaboración propia.

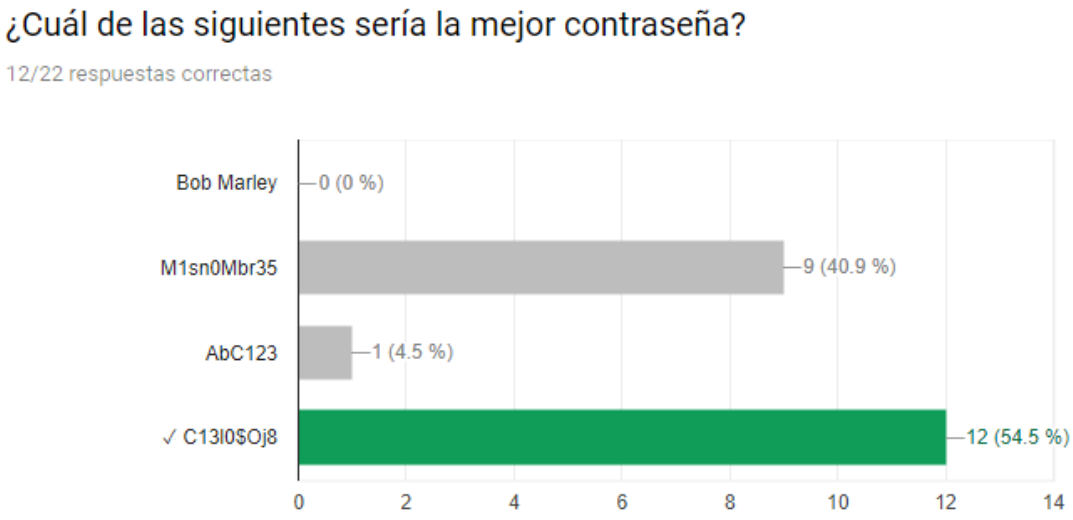

Figura 40, Gráfica de respuestas obtenidas en pregunta orientada a verificar el conocimiento de los usuarios en seguridad de la información. Fuente: elaboración propia.

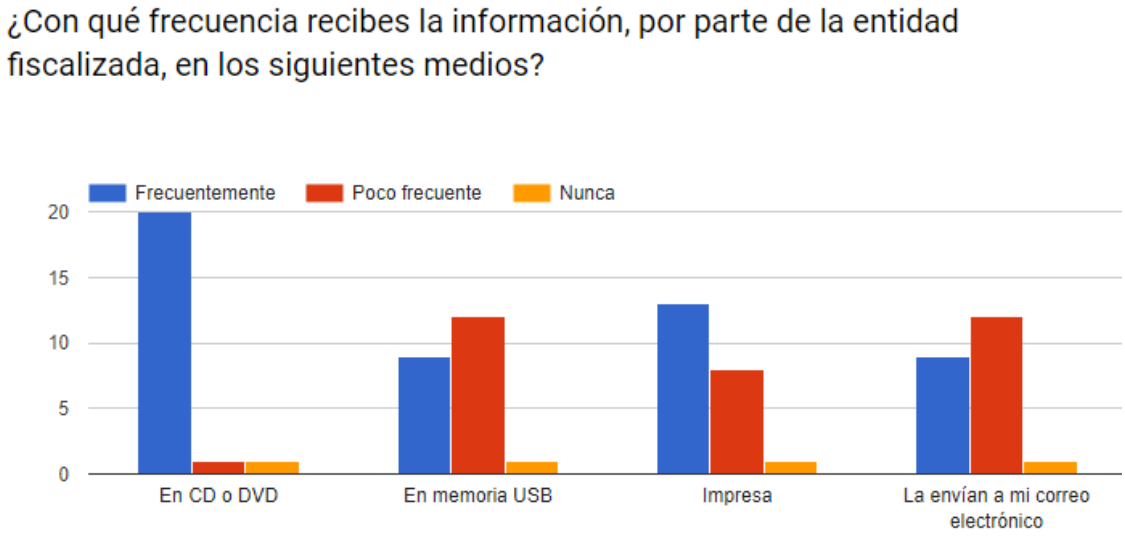

Figura 41, Gráfica de respuestas obtenidas en pregunta orientada a verificar las rutinas de los usuarios. Fuente: elaboración propia.

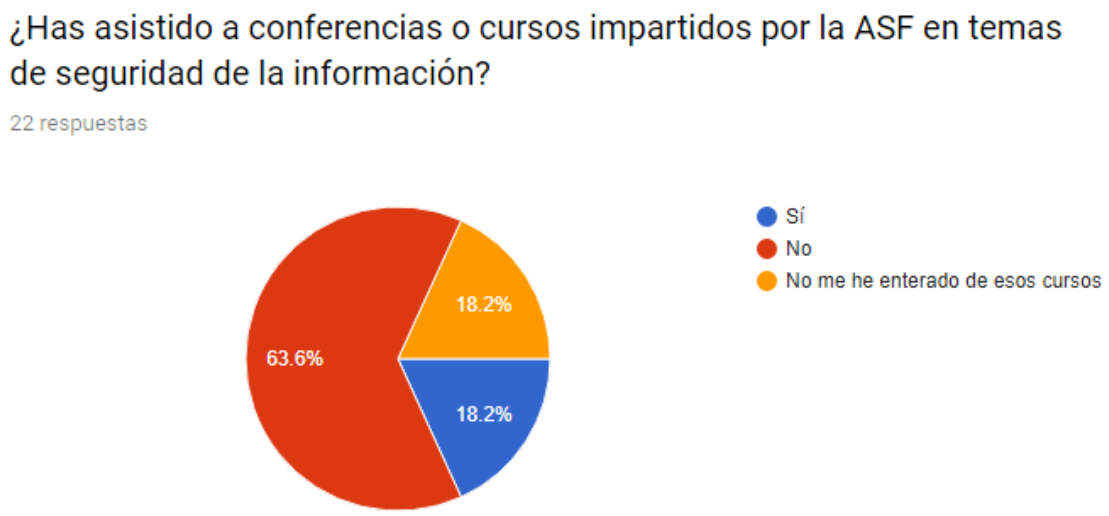

Figura 42, Gráfica de respuestas obtenidas en pregunta orientada a verificar la vinculación entre la ASF y los usuarios. Fuente: elaboración propia.

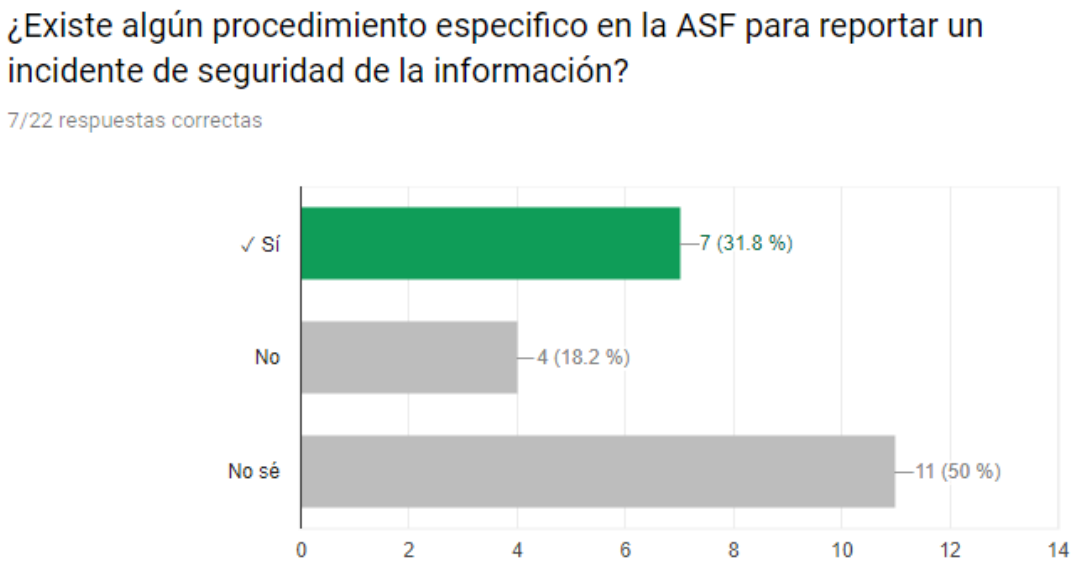

Figura 43, Gráfica de respuestas obtenidas en pregunta orientada a verificar la vinculación entre la ASF y los usuarios. Fuente: elaboración propia.

Con la muestra de gráficas anteriormente presentadas se observa que se verificaron aspectos como:

- Conocimiento en seguridad de la información

- Hábitos en el uso de activos y servicios informáticos
- Hábitos en el manejo de la información
- Efectividad en la comunicación existente entre la DGS y los usuarios
- Concientización en seguridad de la información

El total de la prueba consistió en 32 preguntas con los siguientes resultados estadísticos:

Promedio	Mediana	Rango
46.82 / 100 puntos	45 / 100 puntos	23 - 95 puntos

Tabla 10, Resultados estadísticos de la prueba aplicada durante las entrevistas. Fuente: elaboración propia.

Con estos resultados se observa que menos del 50% de los entrevistados cumple con los conocimientos básicos en seguridad de la información, ya que, sus hábitos en el uso de los activos y servicios informáticos pueden contribuir al incremento de vulnerabilidades en el proceso de auditoría, así como, en sus actividades diarias.

Este desconocimiento en seguridad de la información implica que la DGS no ha tenido una comunicación efectiva con los usuarios. A pesar de que el personal sabe qué área se encarga de la seguridad de la información institucional, desconoce cómo reportar un incidente de seguridad y si existe un procedimiento especifico. También se constató que el personal tiene el conocimiento y pone en práctica algunos aspectos como uso de contraseñas seguras y uso del equipo de cómputo para actividades solo laborales, sin embargo, el personal es susceptible a ser engañados en estrategias de ingeniería social como el phishing.

Asimismo, se confirmó en las entrevistas que el personal, si bien es consciente de la necesidad del resguardo de la información, no ha recibido la correcta capacitación por parte de la ASF y en muchas ocasiones sus hábitos en el trabajo pueden influir en la pérdida o robo de información. De acuerdo con los datos recabados, las etapas vulnerables en el proceso de auditoría son:

- En la recepción de la información preliminar
- En el análisis de la información

Dichas etapas se muestran en la figura 43:

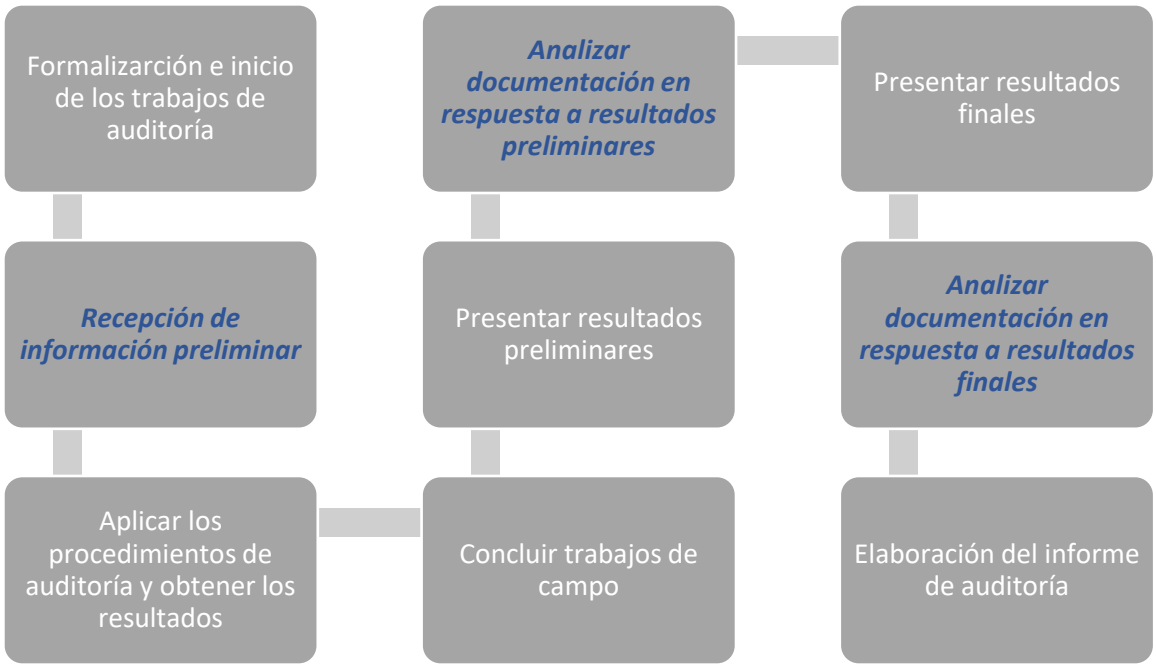

Figura 44
Elaboración propia con apoyo de: Manual, Normativa para la Fiscalización Superior, Tomo II Macroproceso para la revisión de la Cuenta Pública, pp. 26-28.

Cabe señalar que el proceso de auditoría se divide en planeación de la auditoria, ejecución de la auditoria, presentación del informe y seguimiento de las acciones emitidas. El presente estudio únicamente se basó en el análisis de la etapa de ejecución, ya que, en esta parte es donde se realiza la mayor recepción y generación de información, por lo que se requiere mayor control de seguridad y un correcto manejo de esta por parte de los auditores.

Una vez ejecutadas las distintas pruebas y aplicados los diferentes tipos de métodos de recolección de datos, fue posible hacer una evaluación de la concientización en seguridad de la información de la DGARFT"B" perteneciente a la ASF, como se muestra a continuación:

Las pruebas aplicadas fueron:

- Análisis documental: políticas en seguridad de la información, información de comunicación entre la DGS y los usuarios.
- Prueba informática: evaluación de la página web, evaluación de navegación web, evaluación de número de computadoras en la red y prueba de ataque dirigido.
- Análisis del uso de los activos informáticos y cultura en seguridad de la información: riesgos de los principales activos y entrevistas a usuarios.

Pruebas aplicadas	Resultado de la evaluación
Análisis documental	La ASF cuenta con políticas en seguridad de la información que son administradas y ejecutadas por la DGS, estas políticas son debidamente documentadas, las cuales, son del conocimiento de los miembros de dicha dirección y además son de libre acceso para su consulta Si bien, la ASF cuenta con un plan en seguridad de la información, aún no cuenta con una certificación como ISO 27001 o similar. Se lleva una adecuada clasificación de la información, sin embargo, durante el proceso de auditoría y el manejo de dicha información se suele disminuir los controles en su procesamiento, por lo que se ve afectada principalmente la confidencialidad de esta y comprometiendo también a su vez la integridad. Existen dos canales de difusión de información claramente identificados (correo electrónico y un coordinador de la DGS en cada Dirección General), sin embargo, se detectó que, si bien, existen comunicados con información referente a la

	seguridad de la información, ha disminuido su efectividad, ya que, muchos de los comunicados pasan desapercibidos, siendo también pocos los comunicados de capacitación para los empleados.
Pruebas informáticas	El sitio Web de la ASF obtuvo una calificación baja de acuerdo con CA Security Council, debido a que tiene problemas con las categorías de certificado de seguridad, por lo que fue calificado como un sitio no confiable. Cabe mencionar que, si bien el sitio web de la ASF no es utilizado para transacciones bancarias o almacenamiento de datos personales del público en general, aun así, es necesario que cumpla con los estándares básicos por ser una institución perteneciente al poder legislativo. Existen medidas de restricción de acceso a sitios web que pueden ser potencialmente peligrosos. Asimismo, se constató por medio de una prueba que algunos de los empleados aún no cuentan con la conciencia suficiente en cuanto a seguridad de la información, ya que, se detectaron casos de éxito en cuanto a la aplicación del ataque dirigido por medio de una USB que contenía un archivo infectado.
Análisis del uso de los activos informáticos y cultura en seguridad de la información	En la ASF existen perfiles de usuario definidos para el uso de los activos informáticos como computadoras de escritorio, laptops, sistemas de información y bases de datos, siendo los principales riesgos el acceso no autorizado y la pérdida de información. Asimismo, se constató con las entrevistas realizadas al Coordinador de Sistemas de la DGARFT”B” y a distintos empleados que; a pesar de que los usuarios reconocen la necesidad de la seguridad de la información, aun así, desconocen conceptos

	básicos y son susceptibles a ser afectados en prácticas comunes de ataques cibernéticos, además de no tener claro los controles y procedimientos a seguir. Además, con la observación visual y las entrevistas se lograron identificar los hábitos en el uso de la tecnología y manejo de la información por parte de los empleados, como el descuido en el resguardo de contraseñas y acceso a la información. Si bien, se difunden mensajes orientados a la seguridad de la información, son pocos los empleados que han recibido capacitación en el tema.

Tabla 11, Evaluación de los datos obtenidos. Fuente: elaboración propia.

Con base en los niveles de concientización establecidos en el *Modelo de Madurez de Conciencia de Seguridad* del Instituto SANS y en la evaluación anterior, se llegó al resultado de que la ASF se encuentra en transición entre el nivel 2 y el nivel 3, los cuales tienen las siguientes características:

Criterios	Nivel obtenido	
Las políticas de seguridad no se encuentran documentadas en su totalidad. Existe un área de sistemas encargada de la seguridad, sin embargo, no hay comunicación efectiva con los usuarios. Cuentan con escasas herramientas lógicas y físicas para la seguridad informática.	*Nivel 2* *Enfocado en el cumplimiento* El programa de concientización está diseñado principalmente para cumplir requisitos específicos de cumplimiento o auditoría, la capacitación se limita a una anual o ad-hoc. El éxito del programa se basa en la participación, los empleados no están seguros de las políticas de la organización y/o su rol en la protección de los activos de información de su organización.	✓

El esfuerzo está orientado a cumplir solo con lo alguna ley o normativa que están obligados a cumplir.		
Las políticas de seguridad están documentadas y son comunicadas al personal. Realizan campañas de capacitación más de una vez al año para los usuarios. Hay mayor interés por parte de los directivos, por lo que existe un presupuesto específico para el área de sistemas. El personal de sistemas cuenta con algunas certificaciones orientadas a la seguridad de la información. La mayoría del personal es capaz de reconocer una amenaza cibernética.	*Nivel 3* *Busca promover la conciencia y el cambio de comportamiento.* El programa identifica los temas de capacitación que tienen el mayor impacto para apoyar la misión de la organización y se centra en esos temas clave. Va más allá de la capacitación anual y a menudo incluye un refuerzo continuo durante todo el año, el contenido se comunica de una manera atractiva y positiva que fomenta el cambio de comportamiento en el trabajo y en el hogar. Como resultado, las personas entienden y siguen las políticas de la organización y activamente reconocen, previenen y denuncian incidentes. El éxito del programa se amplía para incluir una reducción en el comportamiento relacionado con el riesgo y un mayor conocimiento de las políticas.	✓

Tabla 12, Nivel obtenido de la ASF de acuerdo con el Modelo de Madurez de Conciencia de Seguridad del Instituto SANS Fuente: elaboración propia.

La Auditoría Superior de la Federación se encuentra en transición entre del nivel 2 al nivel 3 en concientización y cultura en seguridad de la información, contemplando a todos los empleados y al área de sistemas.

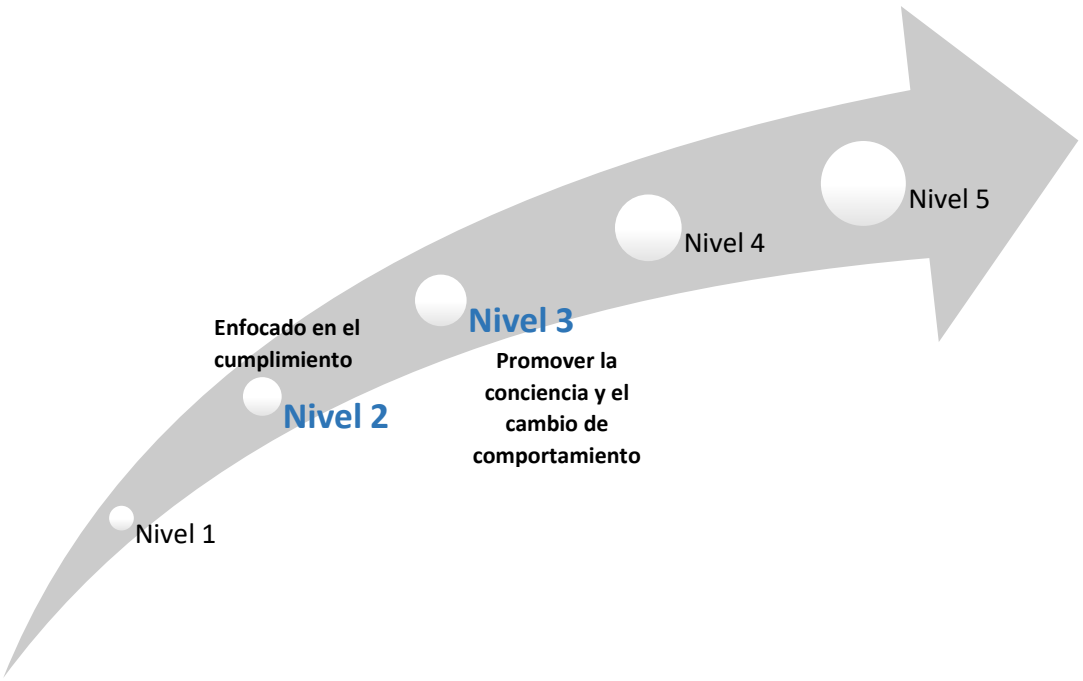

Figura 45, Posicionamiento de la ASF en los niveles de concientización de acuerdo con SANS. Fuente: elaboración propia.

5.2 Recomendaciones para el reforzamiento de una cultura en seguridad de la información

Derivado de la evaluación realizada es posible hacer las siguientes recomendaciones a la Dirección General de Sistemas (DGS) y sus correspondientes coordinaciones en cada una de las Direcciones Generales de la Auditoría Superior de la Federación (ASF).

- Capacitar al personal interno de la DGS en temas de ciberseguridad y creación de planes de concientización en seguridad de la información.
- Crear una campaña de concientización y cultura en seguridad de la información que refuerce los principios básicos y capte la atención de los usuarios, con base en la serie de publicaciones 800 del Instituto Nacional de Estándares y Tecnología (National Institute of Standars and Technology (NIST), por sus siglas en inglés).

- Crear políticas que aseguren la capacitación constante del personal de la DGS y de los usuarios en temas de seguridad informática y seguridad de la información.
- Crear en un plan a largo plazo que busque la certificación en ISO 27001.
- Extender controles en el proceso de recepción de información de las auditorías, donde puedan involucrarse consultas a bases de datos mediante enlaces de internet seguros.
- Monitorear el uso de los dispositivos de almacenamiento de información por parte de los empleados y establecer controles de seguridad informática.
- Monitorear los hábitos de trabajo de los empleados con respecto al uso de contraseñas y acceso a los sistemas.
- Incluir más medidas de seguridad en el procesamiento de la información, como negación o acceso de USB, control de envío de archivos específicos que pudieran contener datos sensibles, controles en el uso del correo personal e institucional.

Conclusiones

Con los datos obtenidos en el presente caso de estudio se evaluó que la Auditoría Superior de la Federación actualmente se encuentra en una etapa de transición entre el nivel 2 y el nivel 3 de concientización en seguridad de la información con respecto al *Modelo de Madurez de Conciencia de Seguridad* del Instituto SANS.

Este proceso de transición significa que pasa de un *enfoque en el cumplimiento -nivel 2* en donde el programa de concientización está diseñado principalmente para cumplir requisitos específicos de cumplimiento o auditoría, asimismo, la capacitación es limitada y el éxito del programa se basa en la participación, además de que los empleados no están seguros de las políticas de la organización y/o su rol en la protección de los activos de información de su organización, a pasar a un nivel 3 en donde se *busca promover la conciencia y el cambio de comportamiento,* para lo cual, el programa identifica los temas de

capacitación que tienen el mayor impacto para apoyar la misión de la organización y se centra en esos temas clave. Va más allá de la capacitación anual y a menudo incluye un refuerzo continuo durante todo el año, el contenido se comunica de una manera atractiva y positiva que fomenta el cambio de comportamiento en el trabajo y en el hogar. Como resultado, las personas entienden y siguen las políticas de la organización y activamente reconocen, previenen y denuncian incidentes. El éxito del programa se amplía para incluir una reducción en el comportamiento relacionado con el riesgo y un mayor conocimiento de las políticas.

Por lo anteriormente expuesto se determina que se cumplió con el objetivo general del caso de estudio, el cual era: “evaluar la consciencia de la seguridad de la información expresada a través de normas y mejores prácticas para identificar áreas de oportunidad”. Si bien, la ASF aún no cuenta con una certificación ISO 27001, se verificó que, si se apegan a las mejores prácticas para la gestión de la seguridad de la información establecidas en la ISO 27002, en las publicaciones especiales de la serie 800 del Instituto Nacional de Estándares y Tecnología y en demás publicaciones internacionales.

Ahora bien, con esta evaluación es posible dar respuesta a la hipótesis planteada, la cual es la siguiente:

“La concientización y la cultura en la seguridad de la información en una Institución de Gobierno en México (Auditoría Superior de la Federación) propicia la integridad, disponibilidad y confidencialidad de los datos que procesa, y a su vez favorece la transparencia de las actividades del servicio público”. Esta hipótesis principal es verdadera, ya que, establece que la concientización y cultura en seguridad de la información es benéfica para las instituciones, cómo se constató en la evaluación realizada a la ASF, en la cual, se detectó que gracias a los esfuerzos de establecimiento de políticas y comunicación con los usuarios (lo cual denota un grado de concientización), poco a poco se está logrando la transición de ser una institución “enfocada en el cumplimiento” a ser una institución que “promueve la consciencia y el cambio de comportamiento”.

La búsqueda de mantener la integridad, disponibilidad y confidencialidad en la información perteneciente a la ASF, se verificó mediante la evaluación de los hábitos de los empleados, ya que la integridad es controlada por medio de la certificación de archivos digitales y físicos por parte de la entidad fiscalizada, tratando de protegerlos de posibles modificaciones o alteraciones por terceros. Para procurar la disponibilidad de la información se constató que existen controles de generación de copias de la información de las auditorías, la cual es resguardada en servidores específicos. Finalmente, como muestra de confidencialidad de la información la ASF asigna auditores que estarán a cargo de realizar la auditoría, siendo los únicos autorizados para analizar la información entregada. Con los ejemplos anteriores se demuestra que la institución busca aumentar la seguridad de la información por medio de políticas o controles documentales que a su vez faciliten la transparencia de las actividades públicas.

Asimismo, se cumplió el objetivo específico de: “conocer cuáles son las medidas que lleva a cabo la ASF para asegurar la confidencialidad, disponibilidad e integridad de su información”, para lo cual, la hipótesis secundaria que se planteó fue:

“Las medidas que lleva acabo la ASF son más normativas (reglamento interno, código de ética, manuales de procedimientos) y poco técnicas y operativas (utilización de sistemas informáticos y vinculación con usuarios), lo que ocasiona que no en todos los niveles (estratégico, táctico y operativo) se apliquen”. Esta hipótesis se acepta debido a que se comprobó que a pesar de que existen básicamente dos medios de comunicación (correo institucional y comunicados por parte del coordinador de sistemas) ha disminuido la efectividad de estos medios, es decir, existen políticas y normativa debidamente documentada, sin embargo, la información que se transmite referente a la seguridad de la información, no está siendo del todo asimilada y puesta en práctica por los empleados.

El segundo objetivo específico se cumplió de igual manera, el cual menciona: “identificar en qué parte del proceso de auditoría existe más vulnerabilidad en la

información”. En vinculación con este objetivo se planteó la segunda hipótesis secundaria, la cual es la siguiente:

“Existe más vulnerabilidad de la información en dos partes del proceso: 1.recepción de la información preliminar y 2.ejecución de la auditoría en campo”. Esta hipótesis pudo comprobarse con las observaciones y entrevistas con los auditores, ya que, manifestaron sus hábitos en el manejo de la información y los medios tecnológicos con los que interactúan en esas etapas, siendo estas dos en las que se tiene mayor contacto con documentación digital y física clasificada como reservada.

Por último, se concluye que la concientización y cultura en seguridad de la información que tengan todos los miembros de la institución se propicia al generar un ambiente capaz de favorecer el resguardo del activo considerado como uno de los más valiosos en las organizaciones: la información.

Cabe señalar que el primer paso para generar una cultura es concientizar al personal sobre los beneficios o riesgos de adoptar o no ciertas medidas. De esta manera, las personas que están informadas toman mejores decisiones, por lo que los esfuerzos de capacitación pueden ser mejor aprovechados.

Glosario

Amenaza informática: todo elemento o acción capaz de atentar contra un sistema informático.

Ciberseguridad: es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios.

Confidencialidad: está relacionado con la privacidad de los datos, es decir, no develar los datos a personal no autorizado.

Disponibilidad: se refiere a que la información se encuentre accesible en todo momento al personal autorizado.

Integridad: es el aseguramiento de que los datos no hayan sido manipulados.

Fuentes de información consultadas

Acevedo Juárez, H. (8 de noviembre de 2011). *Magazcitum, ISO-27001: ¿Qué es y para qué sirve? (parte 1)*. Obtenido de http://www.magazcitum.com.mx/?p=1574#.W3o0_-gzbIU

Audisec. (s.f.). *Audisec, ISO 27000 y el conjunto de estándares de Seguridad de la Información*. Obtenido de https://www.audisec.es/en/iso-27000-estandares-de-seguridad-de-la-informacion/

Auditoría Superior de la Federación . (20 de agosto de 2018). *Auditoría Superior de la Federación* . Obtenido de https://www.asf.gob.mx/Section/53_Tipos_de_auditorias_desarrolladas

Auditoría Superior de la Federación. (2016). *Estudio General sobre las Tecnologías de la Información y Comunicaciones.* Ciudad de México.

Auditoría Superior de la Federación. (noviembre de 2018). *Auditoría Superior de la Federación*. Obtenido de https://www.asf.gob.mx/Section/53_Tipos_de_auditorias_desarrolladas

Auditoría Superior de la Federación. (noviembre de 2018). *Auditoría Superior de la Federación*. Obtenido de https://www.asf.gob.mx/Publication/34_Resultados_del_proceso_de_fiscalizacion

Blog especializado en Sistemas de Gestión . (6 de mayo de 2016). *Blog especializado en Sistemas de Gestión, ¿Cómo utilizar la serie SP 800 de la norma ISO 27001?* Obtenido de https://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/

Blog especializado en Sistemas de Gestión . (14 de junio de 2016). *Blog especializado en Sistemas de Gestión, la norma ISO 27002 complemento para la ISO 27001*. Obtenido de https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

Chiavenato, I. (2006). Introducción a la Teoría General de la Administración. México: Mc. Graw-Hill Interamericana.

Cisco. (2017). *IT and business management roles in cybersecurity.* Estados Unidos.

Código de ética profesional de la Auditoría Superior de la Federación (2001), Impresos ultrarrápidos S.A. de C.V., México D.F., pp.11.

Deloitte. (2016). *www2.deloitte.com*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf

Dirección General de Administración de la ASF. (2010). Manual de Organización de la ASF. Ciudad de México.

Gobierno de la República Mexicana. (2013). *Plan Nacional de Desarrollo 2013 - 2018.* Ciudad de México.

Gobierno de la República Mexicana. (2017). *Estrategia Nacional de Ciberseguridad.* Ciudad de México.

Granados Martin del campo, C. (2018). *Informe de las Recuperaciones Derivadas de la Fiscalización Superior y los Procedimientos Resarcitorio de las Cuentas Públicas 2001 a 2016, al 31 de marzo de 2018.* Ciudad de México: De la Paz, Costemalle - DFK, S.C.

Instituto Uruguayo de Normas Técnicas. (2013). *Instituto Uruguayo de Normas Técnicas*. Obtenido de https://www.unit.org.uy/normalizacion/sistema/27000/

Lacayo, M. H. (2013). Material de apoyo para la elaboración de un protocolo de investigación. 59. Ciudad de México.

Mandado, E. (2003). La innovación tecnológica en las organizaciones. México: Thomson.

Manual de inducción ASF (2013), “Plan de profesionalización de la ASF, programa institucional”, México D.F. pp. 195.

NIST SP 800-50. (2003). *Building an Information Technology Security Awareness and Training Program.* Gaithersburg.

Normativa para la fiscalización superior ASF (2015), “*Macroproceso para la revisión de la cuenta pública*, Tomo II, Volumen 2, proceso de desarrollo, pp.61

Organización de los Estados Americanos. (2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Washington.

PwC. (2016). *Cibersecurity: construyendo una confianza en el entorno digital.* Ciudad de México.

PwC. (2016). *The Global State of Information Security .* Moscú, Rusia.

PwC. (2017). *The Global State of Information Security .* Londres.

PwC. (2018). *The Global State of Information Security.* Londres.

Ramírez Díaz, R. J. (27 de septiembre de 2012). *Magazcitum, Cobit 5*. Obtenido de http://www.magazcitum.com.mx/?p=1893#.W3nvDugzbIU

Reglamento interior de la Auditoría Superior de la Federación, publicado en el Diario Oficial de la Federación el 12 de septiembre de 2001.

Santos, J. C. (2014). Seguridad Informática. Paracuellos de Jarama, Madrid: Ra-Ma.

Secretaría de la Función Pública. (16 de Noviembre de 2017). *Normatividad Gobierno Digital*. Obtenido de https://www.gob.mx/cms/uploads/attachment/file/273176/Normatividad_Gobierno_Digital__Estados_.pptx.pdf

Seger, A. (2016). *El estado actual de la legislación sobre el delito cibernético en América Latina y el Caribe: algunas observaciones.* Banco Interamericano de Desarrollo.

Unión Internacional de Telecomunicaciónes. (2015). *Indice Mundial de Ciberseguridad y Perfiles de Ciberbienestar.* Suiza.

Union International Telecommunication. (2017). *Global Cybersecurity Index 2017.* Ginebra, Suiza.

VI Congreso Iberoamericano de Seguridad Informática. (2 de noviembre de 2011). Obtenido de https://www.lawebdelprogramador.com/pdf/1754-VI-congreso-iberoamericano-de-seguridad-informatica-CIBSI-2011.html

Vieites, A. G. (2014). Enciclopedia de la Seguridad Informática. Paracuellos de Jamara, Madrid: Ra-Ma.

Vieites, A. G. (2014). *Seguridad en equipos informáticos.* Paracuellos de Jarama, Madrid: Ra-Ma.

Villamizar, C. (30 de agosto de 2013). *Magazcitum Jugando a crear cultura de seguridad de la información – De la teoría a la práctica*. Obtenido de http://www.magazcitum.com.mx/?p=2361#.W3tmfegzbIU

Anexos

Anexo A

Cuestionario aplicado al área de sistemas

1	*¿Cuentan con alguna certificación en seguridad de la información como ISO 27001 o similar*?
2	*¿Cuentan con un Plan de Seguridad Informática?, mencione las principales políticas con las que cuentan*
3	*¿Cuál es el área encargada de la Seguridad de la Información?*
4	*¿Cuántas personas son las que tienen relación directa en actividades de seguridad informática? Y ¿Con cuáles certificaciones cuenta?*
5	*¿Cuáles son los medios de comunicación que se tienen con el usuario final?*
6	*¿Se ha implementado alguna campaña de concientización en seguridad de la información dirigida a los usuarios finales?, ¿Cuáles fueron los principales temas que se abordaron?*
7	*¿Actualmente se implementan mecanismos para la creación o refuerzo de una cultura en seguridad de la información?, mencione algunos.*
8	*¿Existen políticas y controles para la gestión de los activos informáticos?, mencione algunos ejemplos.*
9	*¿Existe alguna normativa y/o procedimiento para la clasificación y gestión de la información?, mencione cual y de un ejemplo.*
10	*¿Cuáles son las medidas que se implementan para el control de accesos a sistemas, aplicaciones y servicios en general?, menciona algunos ejemplos.*
11	*¿Cuáles son las medidas de seguridad física y ambiental que se tienen para el resguardo físico de los equipos?*

12	*¿Con qué otras normativas o leyes cumplen los sistemas informáticos que tienen actualmente?*

Anexo B

Cuestionario aplicado al personal de la ASF

Evaluación

Conciencia en seguridad de la información

*Obligatorio

¿Cuál es el cargo que desempeñas en la ASF? *

Elegir

Selecciona los tres pricipios de la seguridad de la información *

- [ ] Conformidad
- [ ] Disponibilidad
- [ ] Oportuna
- [ ] Confidencialidad
- [ ] Integridad

Selecciona el concepto con la definición que le corresponda *

	Información Reservada	Información Confidencial
Es aquella con acceso restringido de manera temporal por razones de interés público. (ejemplo: los planos de una cárcel)	☐	☐
Esta vinculada con los datos personales. (ejemplo: los datos bancarios de una persona)	☐	☐

Cuando sales a comer en el horario laboral o tomas un descanso, ¿Cómo aseguras tu computadora? *

- [ ] Apagas el monitor
- [ ] Bloqueas la computadora

¿Has utilizado la computadora del trabajo para realizar actividades personales? *

- ◯ Frecuentemente
- ◯ Poco frecuente
- ◯ Nunca

Cuando recibes un correo electrónico que tiene un archivo adjunto y es de alguien desconocido, ¿Cómo reaccionas regularmente? *

- ◯ Me da curiosidad y abro el archivo adjunto para ver su contenido
- ◯ Borro el correo electrónico e informo al encargado de Sistemas
- ◯ Reenvío el correo electrónico a mis compañeros de trabajo para que abran el archivo adjunto primero
- ◯ Hago una pequeña inspección y sino me parece sospechoso abro el archivo adjunto

Un ejemplo de ingeniería social es: *

- ◯ Virus que se aloja en tu computadora de manera incógnita
- ◯ Facilidad de socializar en cualquier fiesta
- ◯ Correos de cadena en los que se anima a donar dinero para salvar a un niño enfermo
- ◯ Formatear una computadora para que quede como nueva

¿Qué área de la ASF es la que se encarga de administrar la seguridad de la información?

- ◯ Oficialía de Partes
- ◯ Unidad General de Administración
- ◯ Unidad de Homologación Legislativa, Planeación, Transparencia y

El correo no deseado, como en los correos masivos, es molesto pero inofensivo *

- ◯ Verdadero
- ◯ Falso

La única forma de evitar los virus es no abrir archivos adjuntos inesperados de fuentes desconocidas *

- ◯ Verdadero
- ◯ Falso

Selecciona el concepto con la definición que le corresponda *

	Phishing	Ransomware
Es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y cifra nuestros archivos quitándonos el control de toda la información y datos almacenados. El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual	☐	☐
Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. Comúnmente el engaño suele llevarse a cabo a través de correo electrónico	☐	☐

Selecciona las opciones que contienen ejemplos de programas *

- [ ] .jpeg, .tif y .gif
- [ ] Access, Publisher y Virus
- [ ] Excel, PowerPoint y Word
- [ ] Todo lo anterior

El SPAM lo respondo cuándo: *

- ◯ Nunca lo respondo
- ◯ Cuando tengo curiosidad, no todo puede ser tan malo.
- ◯ Cundo me doy de baja en esa página web

¿Cuál de las siguientes sería la mejor contraseña? *

- ◯ Bob Marley
- ◯ M1sn0Mbr35
- ◯ AbC123
- ◯ C13l0$Oj8

¿De qué manera sueles guardar tus contraseñas de correo electrónico, redes sociales, NIP de tarjeta bancaria, de sesión en laptop, patrón de desbloqueo para el celular, entre otras? *

- [ ] Las escribes en tu celular o en una libreta que llevas contigo
- [ ] Las escribes en un Post -it
- [ ] Tienes una excelente memoria y/o utilizas una aplicación para gestionar tus contraseñas
- [ ] Se las dices a quien mas confianza le tienes

¿Con qué frecuencia recibes la información, por parte de la entidad fiscalizada, en los siguientes medios? *

	Frecuentemente	Poco frecuente	Nunca
En CD o DVD	○	○	○
En memoria USB	○	○	○
Impresa	○	○	○
La envían a mi correo electrónico	○	○	○

¿Con qué frecuencia realizas copias de seguridad de la información que consideras importante? *

- ○ Frecuentemente (dos veces al mes o más)
- ○ Poco frecuente (una vez al mes)
- ○ Cada que se acuerda mi jefe
- ○ No sé, creo que el área de sistemas se encarga de eso

Señala los principios éticos de la ASF que están relacionados con la seguridad de la información *

- ☐ Integridad
- ☐ Independencia
- ☐ Confiabiliadad
- ☐ Confidencialidad

¿Has asistido a conferencias o cursos impartidos por la ASF en temas de seguridad de la información? *

- ○ Sí

¿Te aseguras de que antes de salir de comisión tu laptop cuente con todas las actualizaciones de software necesarias? *

- ◯ Sí
- ◯ No
- ◯ No lo he tomado en cuenta

¿Estas de acuerdo con la siguiente afirmación? El correo electrónico es privado y nadie más puede verlo *

- ◯ De acuerdo
- ◯ En desacuerdo

El cifrado de datos se refiere a: *

- ◯ Se le llama así a la contraseña más segura que puede existir
- ◯ La práctica de codificar y decodificar datos aplicando un algoritmo
- ◯ La práctica de realizar copias de la información de manera rutinaria, se lleva a cabo para hacer frente a la pérdida de datos
- ◯ Se le llama así al banco de datos que se encuentra en un servidor activo

Cuando se envía información confidencial a un colega por medio de Internet. ¿Cómo puedes proteger ese mensaje? *

- ◯ No sé
- ◯ Es mejor no enviar información confidencial por Internet
- ◯ Le aviso a mi compañero de sistemas que enviaré un correo muy importante
- ◯ Puedo usar un cifrado de documento o un archivo zip protegido con contraseña

¿Cuál es el mayor riesgo en seguridad de la información para una empresa? *

- ◯ Los hackers
- ◯ Tener equipos informáticos deficientes
- ◯ Los clientes y proveedores
- ◯ Los empleados

¿Qué marca de antivirus esta instalado en tu laptop del trabajo? *

- ◯ Kaspersky
- ◯ Mc Afee
- ◯ Trend Micro
- ◯ No sé

De las siguientes opciones, ¿Qué medio sería la mejor opción para resguardar una copia de seguridad de tu información? *

- ◯ En el Disco duro de mi Laptop o PC
- ◯ En mi correo electronico
- ◯ Con un proveedor en la nube
- ◯ En un CD o DVD
- ◯ En un disco duro externo

¿Existe algún procedimiento especifico en la ASF para reportar un incidente de seguridad de la información? *

- ◯ Sí
- ◯ No

Elige las opciones menos recomendables para guardar una contraseña *

- [ ] Escribirla en un papel
- [ ] Esforzarse en memorizarla
- [ ] Guardarla en el navegador y activar la opción "autocompletar". Sino fuera seguro no existiría esa opción.
- [ ] Guardarla en el celular
- [ ] Utilizar una aplicación para gestionar las contraseñas

Quieres descargar la canción Yesterday, de Los Beatles, y te encuentras con varias opciones en Internet. ¿Qué archivo descargarías? *

- ( ) Yesterday-Beatles-Song.scr
- ( ) Beatles_All_songs.zip
- ( ) Beatles_Yesterday.mp3.exe
- ( ) Betles-Yesturday.wma

Estas ingresando a la página web de un banco ¿Cuál de estas direcciones te parece segura? *

- ( ) https://Bancomer.com.ar
- ( ) http://BBVABancomer.com
- ( ) http://Bancomer.com
- ( ) https://Bancomer.com

¿Cómo reaccionas ante las páginas web que identifican tu ubicación y te despliegan anuncios con base en las páginas que has visitado y tu historial? *

- ◯ ¡Me gusta! Es muy útil
- ◯ No me gusta mucho pero así es como funciona Internet
- ◯ Utilizo el modo incógnito del navegador y activo las funciones que evitan este tipo de rastreo
- ◯ Nunca me ha importado

¿Qué datos personales de tus perfiles en redes sociales son visibles para todos y no solo para tus amigos? *

- ◯ Solo mi nombre y la foto de perfil
- ◯ Virtualmente todo. No me preocupan los ajustes de privacidad
- ◯ Mi nombre, algunas fotos, estatus y check-ins
- ◯ Nunca había pensado en ello

ENVIAR

Página 1 de 1