DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA CONTADURÍA GENERAL DE LA NACIÓN

Antonio Andrés Osorio Sánchez
(antonioosorios@gmail.com)
Universidad Piloto de Colombia

Resumen — Este documento tiene como fin, presentar aportes para generar la construcción de un Sistema de Gestión de Seguridad de la información (SGSI) para la Contaduría General de la Nación. Debido a los problemas diarios que se han presentado en el campo de la seguridad informática, es necesario implementar la norma ISO 27001, en el ámbito del negocio, definiendo un tiempo estimado, para resolver problemas de seguridad, con el fin de obtener un mejor servicio, garantizando la continuidad del servicio con calidad.

Abstract—This document is intended to , provide input to build an (ISMS) in the General Accounting Office , due to everyday problems that have arisen in the field of computer security , it is necessary , to comply with the standard ISO27001 , in the field of business, defining an estimated time to resolve security issues , obtaining better service and ensuring continuity of service

Índice *de Términos*— Vulnerabilidad, Seguridad, informática, ataques cibernéticos, SGSI, GIT, TIC, Información

I. INTRODUCCIÓN

Debido al constante crecimiento de delitos informáticos y a que en las organizaciones no se tiene un buen nivel de cultura informática, sobre la seguridad de la información, se ve en la necesidad de proponer un diseño de un SGSI para asegurar la confidencialidad, integridad y calidad de la información.

Toda organización tiene por objetivo general la búsqueda de un mercado de negocio y requiere que, desde los procesos de operaciones hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable. Si bien gran parte de la información se vincula con las computadoras y redes, hay otra parte que no está en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, y aquí entre en juego la necesidad de diseñar un Sistema de Gestión de Seguridad de la Información (SGSI).

Debido a que, en la actualidad, la empresa ha estado en constante cambio y ha sufrido ataques cibernéticos por virus, que personas inescrupulosas intentan diariamente atacar por medio de su página web, la empresa tiene como fin realizar las siguientes actividades. Se hace necesario, que las empresas tomen conciencia de la importancia de la información, debido a que los empleados que trabajan en las organizaciones no cuentan con un buen nivel de cultura informática, lo que hace que se presenten problemas de seguridad, debido a que desconocen las políticas y procedimientos que se han establecido con anterioridad.

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones(TIC) que proporciona la Contaduría General de la Nación a través del GIT de Apoyo Informático, contribuyendo a la mejora y cabal cumplimiento de los objetivos institucionales.

II. LEY DE DELITOS INFORMÁTICOS

[1] La ley colombiana según el especialista Alexander Díaz, según lo que dice es que Colombia es el primer país que tipifica de forma clara, los delitos de cuando alguien se apropia de información confidencial. En mi opinión, cuando alguien incurre en estos delitos la ley colombiana no es tan estricta como en otros países, ya que las leyes colombianas, cambian fácilmente, y se basa en una regulación local, debería contar con una legislación internacional, para que este tipo de delitos fueran castigados, drásticamente, ya que el error del [3] El estado colombiano es presumir que las personas conocen las leyes, y por eso no se les exime y se les juzga como delincuentes informáticos.

III. OBJETIVO DE LA NORMA ISO 27001

[2] El objetivo es el de proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan.

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti- virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

IV. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PROPÓSITO

La Contaduría General de la Nación busca preservar la confidencialidad, disponibilidad e integridad de su información, protegiéndola contra amenazas internas, externas, accidentales o deliberadas, mediante la implementación de buenas prácticas tendientes a reducir los riesgos identificados. Así mismo, busca garantizar que todos los requerimientos normativos y legales aplicables a la información se cumplan; que existan mecanismos de concientización en temas de seguridad para los usuarios; que los incidentes de seguridad sean reportados e investigados y que se propendan por la continuidad del funcionamiento de la Contaduría General de la Nación.

ALCANCE

Ésta Política de Seguridad Informática aplica a todos los activos de información de propiedad de la Contaduría General de la Nación, con excepción de aquellos que hayan sido específicamente definidos por el Contador General de la Nación o los Subcontadores, con el fin de divulgar información pública.

POLÍTICA

Las Políticas de Seguridad Informática de la Unidad Administrativa Especial Contaduría General de la Nación, identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información de la entidad. La implementación de las políticas busca reducir el riesgo de divulgar, modificar, destruir o usar en forma indebida los activos de información y operaciones críticas, ya sea accidental o intencionalmente. Al mismo tiempo se establecen políticas con el objeto de orientar y mejorar la administración de seguridad de los activos de información y proveer las bases para el monitoreo a través de toda la entidad.

Activos de información son:

ACTIVOS FÍSICOS

Infraestructura de TI: Edificios, oficinas, centro de datos, habitaciones de servidores y equipos, armarios de red (Racks), cableado, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos, dispositivos de identificación y autentificación, control de acceso del personal y otros dispositivos de seguridad como por ejemplo las cámaras (circuito cerrado de TV).

Controles del entorno de TI: Alarmas, sistema de refrigeración, supresión contra incendio, sistemas de alimentación ininterrumpida, alimentación de potencia y de red.

Hardware de TI: Estaciones de trabajo, computadores de escritorio y portátiles, dispositivos de almacenamiento, servidores, mainframes, módem, dispositivos de comunicaciones, impresoras, fax, escáneres, fotocopiadoras y equipos multifunción.

Documentación: Procedimientos, programas, guías, formatos, manuales y demás documentación física de propiedad de la Contaduría General de la Nación.

ACTIVOS DE SERVICIOS DE TI

Servicios de autenticación de usuario y administración de procesos de usuario, aplicaciones, firewalls, servidores proxy, servicios de red, servicios web, servicios inalámbricos, anti-virus, anti-spyware, anti-spam, detección y prevención de intrusiones, seguridad, FTP, bases de datos, correo electrónico y mensajería instantánea, herramientas de desarrollo, contratos de soporte y mantenimiento de software.

ACTIVOS HUMANOS

Empleados: servidores públicos y contratistas, en particular desarrolladores de software, probadores, administradores de sistemas y redes, administradores de seguridad, operadores, abogados, auditores, usuarios con poder y expertos en general.

Externos: Consultores externos o asesores especialistas, trabajadores temporales, pasantes, proveedores y socios.

La política de seguridad de la información de la Contaduría General de la Nación aplica a todos los activos de información durante su ciclo de vida, incluyendo creación, distribución, transmisión, almacenamiento y eliminación. De la misma forma, estas políticas están orientadas a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio,

portátiles, etc.) y de servicios como el Internet, el correo electrónico y el Orfeo, brindando a los servidores públicos, contratistas, terceros y público en general, pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida de activos de información sensitivos para la Contaduría General de la Nación.

Éstas políticas aplican a todos los servidores públicos, contratistas, terceros y público en general que acceden a activos de información de la Contaduría General de la Nación, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que los trabajadores de la entidad.

La información utilizada para el desarrollo de las actividades y funciones diarias o contratadas por la Contaduría General de la Nación, es propiedad de la entidad, por tal razón, todos los servidores públicos, contratistas y terceras partes están obligados a proteger dicha información, incluso una vez haya terminado su relación contractual y/o legal con la entidad.

a. Principios

Los siguientes principios básicos fundamentan las políticas de seguridad de la información para la infraestructura tecnológica y de información de la Contaduría General de la Nación.

b. Protección de la información

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para la entidad. La protección debe acentuar la confidencialidad, integridad y disponibilidad de los activos de información.

c. Protección de los recursos

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para la entidad. Dichos recursos deben ser utilizados exclusivamente para el desarrollo de las actividades laborales establecidas a los servidores públicos, contratistas y terceros, y así mismo su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

d. Autorización de usuarios

Todos los usuarios deben ser identificados independientemente, con permisos de acceso específicamente e individualmente autorizados por razones básicas de sus funciones. Los mecanismos de acceso de usuarios deben exigir un proceso robusto de autenticación (por ejemplo: identificación del usuario única y contraseña), autorización apropiada y auditoría confiable.

e. Responsabilidad

Los usuarios y custodios de los activos de información de la Contaduría General de la Nación son responsables por el uso apropiado, la protección y privacidad de estos activos. Los sistemas informáticos de la Contaduría General de la Nación generarán y mantendrán pistas apropiadas de auditoría para identificar usuarios y para documentar las situaciones relacionadas con eventos de seguridad.

f. Disponibilidad

Los activos de información deben estar disponibles para soportar los objetivos de la Contaduría General de la Nación. Deben tomarse medidas adecuadas para asegurar el tiempo de recuperación de toda la información y el acceso por individuos autorizados.

g. Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

h. Confianza

Los servidores públicos, contratistas y terceros deben demostrar capacidad para reunir o exceder los requerimientos de seguridad de la Contaduría General de la Nación, y deben justificar la confianza en sus capacidades para asegurar los activos de información de la organización. La confianza empieza a incrementar su importancia cuando los activos de información de la Contaduría General de la Nación son compartidos con terceros.

i. Esfuerzo de equipo

Para que logre ser efectiva, la seguridad de información debe ser un esfuerzo de equipo donde debe participar en forma activa cualquier funcionario que tenga interacción con la información o los sistemas de información de la organización. Todos los servidores públicos y contratistas de la organización deben cumplir con las políticas de seguridad de información y desempeñar un papel proactivo para la protección y divulgación de estas políticas.

j. Soporte primario para la seguridad de información

El GIT de Apoyo Informático debe facilitar la administración y desarrollo de iniciativas sobre seguridad de información. El GIT de Apoyo Informático deberá proveer dirección y experiencia técnica para asegurar que la información de la Contaduría General de la Nación se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan. Los usuarios son responsables de familiarizarse, observar y cumplir las políticas de seguridad de información, las dudas que puedan surgir alrededor de éstas deben ser consultadas al GIT de Apoyo Informático de la entidad directamente con el encargado de la seguridad informática al correo seguridadinformatica@contaduría.gov.co.

k. Revisiones de seguridad en sistemas de información

Al menos una vez al año la Contaduría General de la Nación debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad, lo mismo que para verificar el cumplimiento de los estándares de configuración en las diferentes plataformas técnicas e instalaciones de tecnología de información. Anualmente se realizará la revisión y actualización de las políticas establecidas, con el fin de asegurar la suficiencia, conveniencia y eficacia.

l. Compromiso de la dirección con la seguridad de la información

Es deber del Contador General de la Nación participar de manera activa en la seguridad de la información mediante la revisión y aprobación de la presente política, la delegación de funciones y responsabilidades, y la iniciación de planes y programas para mantener la concientización sobre la seguridad de la información.

m. Clasificación de la Información

El sistema de clasificación definido para la CGN debe tener en cuenta las propiedades de seguridad de la información: confidencialidad, integridad y disponibilidad; definiendo tres niveles de clasificación para estas propiedades.

Este sistema de clasificación de información debe ser utilizado por la Contaduría General de la Nación para asignar clasificaciones sensitivas con requerimientos independientes.

V. DESARROLLO DE POLÍTICAS

a. Las estrategias de seguridad de información de la Contaduría General de la Nación son directrices globales de largo plazo, que sirven como base para la planeación adecuada y la definición de soluciones de seguridad para ajustarse a las necesidades de la entidad, tanto actuales como futuras y se apoyaran en el equipo de comunicaciones de la entidad.

b. Las decisiones y disposiciones de seguridad de información estarán basadas en análisis de riesgo y métodos de evaluación. Éstas incluirán métricas que consideren el valor para las entidades de las alternativas a corto y largo plazo.

c. La seguridad de información considera revisiones continuas del valor para la institución de las medidas de seguridad en uso.

d. La administración de la seguridad de información se desarrollará sobre métodos y estándares globales.

e. Las políticas de seguridad deberán ser revisadas cada vez que se cumpla un ciclo de gestión de seguridad de la información.

f. Las políticas de Seguridad, deberán ser aprobadas por el Contador General de la Nación, y estar acorde a los lineamientos de la CGN.

VI. POLÍTICAS APLICABLES A USUARIOS

Acceso a los recursos de información:

a. Se debe custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar su sustracción, destrucción, ocultamiento o utilización indebida.

b. Se debe vigilar y salvaguardar los útiles, equipos, muebles y bienes que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a los que han sido destinados.

c. El acceso a los sistemas y recursos de información solamente se debe permitir si existe autorización formal y escrita por parte del jefe inmediato, teniendo en cuenta los siguientes parámetros:

"El jefe inmediato solo puede autorizar acceso a información propia del área que coordina y solo podrá asignar privilegios de acceso a los servidores públicos, contratistas y terceros que están bajo su supervisión. En caso de su ausencia o vacancia, el cargo inmediatamente superior en la jerarquía podrá evaluar y autorizar acceso a la información."

d. El acceso a los recursos de información de la organización presupone la aceptación de este documento de Políticas de Seguridad Informática, así como las respectivas sanciones por su incumplimiento de acuerdo a lo establecido en el Código Único Disciplinario (Ley 734 de 2002). Esto se confirmará (para el caso de los servidores públicos) a través de la firma de un acuerdo de responsabilidad y/o confidencialidad que hará parte de la resolución y del manual de funciones, y (para el caso de los contratistas y terceros) los contratos.

e. Los servidores públicos, contratistas, terceros y público en general deben garantizar que el acceso a la información y la utilización de la misma sea exclusivamente para actividades relacionadas con funciones propias de la entidad, y que ésta sea utilizada de acuerdo a los criterios de confidencialidad definidos por la Contaduría General de la Nación.

f. El establecimiento de conexiones directas entre los sistemas de cómputo y comunicaciones de la Contaduría General de la Nación con cualquier otra organización, a través de Internet o cualquier otro tipo de red, debe contar con una evaluación y autorización formal previa, basada en un análisis de riesgos de seguridad por parte del administrador de red o el encargado de la seguridad informática.

g. Módem, Cable-módem o dispositivos de índole similar no deben ser utilizados para las comunicaciones de la Contaduría General de la Nación, a menos que un firewall y una red privada virtual sea establecida entre los equipos de cómputo involucrados en dicha comunicación.

h. Una vez se dé por terminada la relación laboral de un servidor público, contratista o tercero, se deben retirar todos los

derechos de acceso a los recursos a los cuales estuvo autorizado y se debe realizar también una devolución de activos.

i. La devolución o retiro de equipos, información o software solo debe realizarla el personal autorizado.

VII. USO DE LOS RECURSOS DE INFORMACIÓN

a. Se deben utilizar los bienes y recursos informáticos asignados única y exclusivamente para el desempeño de su empleo, cargo y/o función. De la misma forma las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, debe ser utilizada en forma exclusiva para fines institucionales de la entidad.

b. Los sistemas de cómputo entregados por la Contaduría General de la Nación deben ser utilizados únicamente para propósitos propios de la entidad y son propiedad del Estado, por esta razón se recuerda que el uso que se le dé a los mismos es de carácter oficial.

c. No se pueden almacenar, instalar o utilizar juegos en los equipos de cómputo de la Contaduría General de la Nación.

d. Las únicas personas autorizadas por la Contaduría para instalar software en los equipos son los funcionarios del GIT de Apoyo Informático y los técnicos de soporte con previa autorización del Coordinador del GIT de Apoyo Informático, motivo por el cual se prohíbe a los funcionarios instalar algún software sin previa autorización del GIT de Apoyo Informático, con el fin de constatar la seguridad y legalidad del mismo.

e. A menos que sean específicamente autorizados por el Coordinador del GIT de Apoyo Informático los servidores públicos de la Contaduría General de la Nación no deben utilizar herramientas de hardware o software que puedan ser empleadas para evaluar vulnerabilidades o comprometer la seguridad de los sistemas de información o la información de otros usuarios. Incidentes que involucren este tipo de herramientas y el intento no autorizado de comprometer las medidas de seguridad de los sistemas de información, serán considerados como violaciones serias de las políticas de la Contaduría General de la Nación y podrán ser denunciados legalmente.

f. El GIT de apoyo informático, debe realizar un Análisis de Riesgos para el software (aplicativo, sistema operativo) y hardware nuevo, que llegue a la Contaduría General de la Nación.

g. La Contaduría General de la Nación se reserva el derecho de examinar toda la información almacenada en, o transmitida por sus sistemas de cómputo y de comunicación, y debe informar a los servidores públicos, contratistas y terceras partes que no deben esperar privacidad asociada con la información que almacenan o envían a través de estos sistemas.

h. No se permitirá la navegación en sitios Web de uso social, que no generan valor a la entidad: sitios como youtube, myspace, facebook, hi5, entre otros. Tampoco se permitirá el uso de herramientas en línea y directas de chat, video chat, etc., tipo messenger, yahoo, skype, solamente serán utilizadas por el grupo de comunicaciones.

i. Está prohibido el uso de emisoras de radio por Internet, debido al incremento en el uso de ancho de banda, que afecta la velocidad de navegación de los usuarios de la entidad. Se exceptúa para los equipos del Contador General de la Nación, los Subcontadores, el Secretario General y la oficina de Comunicaciones de la entidad.

j. No se permite la descarga por Internet de archivos de video, música, etc., por afectar el rendimiento de la red y uso del enlace de Internet.

k. El GIT de Apoyo Informático garantizará que todos los usuarios cuenten con una configuración estándar en el uso de los recursos de la entidad, y acceso Internet, con el propósito de asegurar que lo establecido en ésta política se cumpla.

l. El envío de información a través de cualquier medio electrónico, servicio o aplicación (como por ejemplo: orfeo o correo electrónico) y que requiera un proceso de autenticación, es decir, usuario y contraseña, será responsabilidad de cada usuario. Lo anterior sustentado en el artículo 55 de la Ley 1437 de 2011 que establece: "Los documentos públicos autorizados o suscritos por medios electrónicos tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código de Procedimiento Civil".

VIII.CUMPLIMIENTO ANTE REQUERIMIENTOS LEGALES Y CONTRACTUALES – DERECHOS DE AUTOR

a. Es política de la Contaduría General de la Nación, el cumplimiento de todas las obligaciones legales, adquiriendo el material patentado de la empresa propietaria o duplicándolo bajo expresa autorización de la misma. Todo el software operativo y aplicativo es de propiedad de la Contaduría General de la Nación y solo el GIT de Apoyo Informático está autorizado para instalarlo en las estaciones de trabajo de la entidad.

b. Si se requiere utilizar software patentado, éste debe tener las respectivas licencias de uso y se debe pedir autorización para instalación al GIT de Apoyo Informático. Solo dicha área está autorizada para instalar software en las estaciones de trabajo de la entidad.

c. El software patentado es generalmente suministrado bajo un acuerdo de licencia, el cual limita el uso de dichos productos en equipos específicos, y puede limitar las copias únicamente a aquellas con el objetivo de mantener un respaldo de los medios. Por lo tanto, los servidores públicos, contratistas y terceros que trabajan para la Contaduría General de la Nación no deben copiar el software suministrado por la entidad en medios de almacenamiento, transferir dicho software a otros computadores o suministrar dicho software a terceras partes sin la autorización escrita del Coordinador del GIT de Apoyo. Lo anterior aplica para el software desarrollado por la entidad. La trasgresión de

derechos en cierto software, bajo la Ley de derechos de autor, constituye un delito criminal.

d. La Contaduría General de la Nación cuenta con la autoridad y autonomía para realizar auditorías periódicas sobre las estaciones de trabajo, previa autorización del jefe inmediato, para verificar el apropiado uso de software. Se mantendrán los registros de los hallazgos identificados.

e. No está permitido distribuir copias de esta política a personas externas a la entidad, sin la autorización respectiva por parte del personal encargado de la seguridad informática.

f. Se debe cumplir a cabalidad con todas las leyes, normas, decretos, sentencias y demás que sean aplicables.

IX.CONFIDENCIALIDAD DE LA INFORMACIÓN

a. Los siguientes elementos deben ser considerados por los Propietarios de la Información y el GIT de Apoyo Informático independientemente de la clasificación del nivel de sensibilidad de la información, con el objeto de que toda la información (medio físico y electrónico) de la Contaduría General de la Nación quede protegida en forma predeterminada.

b. La Contaduría General de la Nación ha adoptado un sistema de clasificación de la información que categoriza la información en tres grupos de acuerdo a su grado de confidencialidad. Toda la información bajo control de la Contaduría General de la Nación, sea ésta generada interna o externamente, se encuentra en una de estas categorías: Dominio Público, Uso Interno y Confidencial. Todos los servidores públicos deben familiarizarse con las definiciones para estas categorías y cumplir con las medidas de protección establecidas para ellas.

c. Si la información no está clasificada como pública, ésta no podrá ser proporcionada a ninguna entidad externa sin un acuerdo de confidencialidad.

d. Los servidores públicos, contratistas y terceros que trabajan para la Contaduría General de la Nación, en ausencia de instrucciones claras o precisas, considerarán la información como de uso interno exclusivamente. Esta política aplica especialmente cuando, por algún motivo, no se ha realizado una clasificación de la información.

e. Los servidores públicos, contratistas y terceros que trabajan para la Contaduría General de la Nación no deben enviar información de carácter diferente a Dominio Público por correo electrónico, a menos que se tengan medidas adicionales de protección.

f. Toda la información de la Contaduría General de la Nación (Dominio Público, Uso Interno y Confidencial) debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento a terceras partes (servidores públicos, prestadores de servicios, entidades externas y personal que realiza alguna actividad dentro de la entidad). Estas entidades tendrán acceso a la información de la Contaduría General de la Nación únicamente cuando se demuestre la necesidad de conocer su existencia y cuando se haga a través de una cláusula o contrato de confidencialidad.

g. Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a entidades no autorizadas, el Propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad informática de la entidad, con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.

h. Ningún servidor público, contratista o tercero que tenga alguna relación laboral con la Contaduría General de la Nación revelará los controles de seguridad de los sistemas de información y la forma en que están implementados, a menos que se obtenga una autorización previa del Coordinador del GIT de Apoyo Informático. Esto incluye: información que se proporciona en presentaciones, discusiones, o es tratada en diferentes foros que incluya aspectos técnicos de infraestructura.

i. La información específica de debilidades en sistemas de Información (como pueden ser la caída de un sistema, falta de un control, etc.), no debe ser distribuida a personas que no demuestren la necesidad de conocer esta información. Es decir, las personas de la Contaduría General de la Nación que tengan acceso a este tipo de información, deben saber que es estrictamente controlada, y evitar que sea conocida por entidades que puedan representar un riesgo o comprometer los sistemas de información de la entidad.

j. Toda la información clasificada como confidencial y para uso interno, debe ser etiquetada (marcada) con base en estándares definidos. Se buscará que estas etiquetas sean mantenidas en buen estado y visibles de tal forma que se puede identificar la clasificación de la información de la entidad en cualquier momento.

k. Cualquier medio de almacenamiento de cómputo que contenga información confidencial o de uso interno (tales como cintas, discos, y otros), debe ser etiquetado de acuerdo con la clasificación.

l. Toda la documentación impresa, escrita a mano o documento legible que contenga información clasificada como confidencial o de uso interno, debe tener una etiqueta que indique el nivel apropiado de sensibilidad con base en la clasificación.

X. MONITOREO Y EVALUACIÓN DEL CUMPLIMIENTO

a. Todos los servidores públicos, contratistas y terceras partes, en primera instancia, tienen la responsabilidad de monitorear sus estaciones de trabajo en forma permanente con el fin de identificar material que pueda ser considerado.

Como ofensivo o potencialmente ilegal, así como las situaciones que afecten la seguridad informática de la entidad, y deben reportar este tipo de situaciones.

b. La Contaduría General de la Nación se reserva el derecho de monitorear o inspeccionar todos los sistemas de información de la entidad. Esta evaluación puede tener lugar con el consentimiento, presencia o conocimiento del jefe inmediato de los servidores públicos involucrados. Los sistemas de información sujetos a tal examen incluyen, pero no están limitados a, sistemas de archivo de correo electrónico, archivos en discos duros de computadores personales, archivos de correo de voz, archivos en colas de impresión y salidas de máquinas de fax.

c. Debido a que los sistemas de cómputo y comunicaciones suministrados por la Contaduría General de la Nación se emplean únicamente para propósitos de la entidad, los servidores públicos, contratistas y terceras partes no deben tener expectativas de privacidad asociadas con la información que ellos almacenan o envían a través de estos sistemas de información.

d. La Contaduría General de la Nación conserva el derecho de retirar de los sistemas de información cualquier material que pueda ser considerado ofensivo o potencialmente ilegal.

e. El administrador del sistema o el GIT de Apoyo Informático no leerá o facilitará a otra persona que lea el contenido de ningún archivo de correo electrónico del personal sin obtener el permiso del usuario o, en su defecto, del jefe inmediato, cuando exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (tal como la eliminación de virus), cumplir obligaciones legales (tal como citaciones judiciales) y efectuar ciertas funciones de administración del sistema (tal como remitir los mensajes con direcciones erróneas).

f. No obstante, lo anterior, la Contaduría General de la Nación puede obtener acceso a la información de los servidores públicos, contratistas y terceros, en caso que se requiera dicha información para investigaciones o en caso de emergencia. Por ejemplo, si el servidor público, contratista o tercera parte está ausente durante un período prolongado de tiempo debido a enfermedad u otro motivo (previa autorización escrita del jefe inmediato), se podrá tener acceso a la información para suplir necesidades del servicio y para las investigaciones de la Secretaría General.

g. La Contaduría General de la Nación se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través del sistema de la entidad como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoría o seguridad del desempeño del sistema. Todo el personal debe estar consciente de esto cuando use los sistemas de tecnologías de información de la entidad.

XI. REPORTES DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN

Se entiende por incidente en la plataforma informática, cualquier evento que ponga en riesgo la integridad, disponibilidad, confiabilidad, veracidad y consistencia de la información de la CGN.

Todo el personal de la Contaduría General de la Nación debe estar vigilante respecto a los incidentes o debilidades de seguridad (incluyendo fallas en el sistema, pérdida del servicio, errores resultado de datos del negocio incompletos o inadecuados, rompimiento de la confidencialidad). Si se detectan estos incidentes o debilidades de seguridad, deben ser reportados en forma inmediata al encargado de la seguridad informática al correo electrónico seguridadinformatica@contaduria.gov.co.

XII. PANTALLA DESPEJADA Y ESCRITORIO DESPEJADO

a. Todos los servidores públicos, contratistas y terceros deben tener conocimiento de los requerimientos de seguridad y de los procedimientos para proteger equipos sin atención. También deben conocer su responsabilidad, y la implementación de dicha protección.

b. Los servidores públicos, contratistas y terceros deben adoptar como mínimo las siguientes prácticas al dejar desatendido su equipo:

c. Terminar la sesión activa al finalizar, a menos que se pueda asegurar por medio de un software que proporcione protección: ej: "Protector de Pantalla" o "bloqueo del equipo" con Windows XP o Windows 7. Se pueden asegurar los PC (o terminales) por medio de una llave o control equivalente. (ej: contraseña de acceso).

d. En equipos servidores se debe desactivar (log off) la sesión si se pretende apagar el equipo o si simplemente se va a dejar desatendido por un periodo de tiempo considerable. Para computadoras mainframe se debe finalizar la sesión – en vez de simplemente apagar la terminal o PC.

e. Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarlo bajo llave y/o utilizar una guaya de seguridad.

f. Se deben utilizar restricciones en los tiempos desconexión para brindar seguridad adicional.

g. Por fuera del horario regular de trabajo, cuando los funcionarios no se encuentren en su puesto de trabajo, deben limpiar sus escritorios y áreas de trabajo de cualquier información que utilicen para el desarrollo de sus labores y sea considerada ―Confidencial" de acuerdo a la clasificación. Así mismo, deben asegurar en forma apropiada dicha información.

h. La información considerada como sensitiva o crítica debe siempre permanecer bajo llave y no debe dejarse desatendida en ningún sitio durante otros turnos de trabajo o el fin de los mismos.

XIII. RESPALDO DE DATOS

a. Los servidores públicos, contratistas y terceras partes que trabajan para la Contaduría General de la Nación deben establecer con el GIT de Apoyo Informático los lineamientos

para el respaldo, almacenamiento y destrucción de la información sensible, valiosa o crítica de la entidad, minimizando el riesgo de pérdidas de información o el mal uso de ésta.

b. Los procedimientos de almacenamiento en medios magnéticos y ópticos (dispositivos de almacenamiento USB, CD, cintas magnéticas, etc.), deben asegurar que la información sensible, crítica o valiosa almacenada por periodos prolongados de tiempo, no se pierda por deterioro. Por ejemplo, el GIT de apoyo informático debe efectuar copias de los datos en medios de almacenamiento diferentes, si el medio de almacenamiento original muestra señas de deterioro.

c. Si se otorga a los usuarios finales la capacidad de restaurar sus archivos propios, no deben tener los privilegios para restaurar los archivos de otros usuarios o examinar qué archivos han sido respaldados por otros usuarios.

d. Toda la información sensible, valiosa o crítica residente en los sistemas de cómputo de la Contaduría General de la Nación debe respaldarse periódicamente.

e. Para prevenir que la información almacenada fuera de la Contaduría General de la Nación, considerada como sensible, valiosa o crítica, sea revelada o utilizada por partes no autorizadas, se buscará que ésta sea debidamente protegida. De la misma forma un acuerdo de confidencialidad de información debe ser firmado por la empresa que hace la custodia de la misma.

f. Los usuarios deberán estar conscientes de que la información Confidencial o sensible almacenada en sus computadoras puede ser recuperada con métodos avanzados aun cuando haya sido normalmente borrada. Por esta razón se deberán tener las precauciones para el manejo de información Confidencial en las computadoras y memorias USB que hayan tenido esta información y que se pretendan prestar o compartir.

g. Los datos críticos que hayan sido respaldados no deben utilizarse directamente para restaurar datos, a menos que exista otra copia de respaldo de los mismos en un medio de almacenamiento diferente (cinta, disco, memorias USB, smart-card, CD-ROM, etc.). Si se sospecha la existencia de virus u otro problema de software, la copia de respaldo adicional debe realizarse en una computadora diferente. Esta política previene que la única copia de respaldo de datos críticos sea dañada inadvertidamente en el proceso de restauración.

h. Deberá existir un lugar de almacenamiento de medios (anteriormente llamado cintoteca) interno y externo fuera del edificio con información crítica de la entidad para propósitos de recuperación contra desastres. De la misma forma un acuerdo de confidencialidad de información debe ser firmado por la empresa que hace la custodia de la información.

i. Los respaldos de información sensible, crítica y valiosa deben almacenarse en un sitio protegido contra inclemencias del medio ambiente y con controles estrictos de acceso que se encuentre a una distancia razonablemente fuera del alcance de un evento en la zona original.

j. Toda la información de la Contaduría General de la Nación debe almacenarse de forma segura, de acuerdo a unos requerimientos de tiempo determinados por el GIT de Jurídica, y de conformidad a las normas expedidas por el Archivo General de la Nación para tal fin. (Ley 594 de 2000 y acuerdo 07 de 1994- según tablas de retención documental).

XIV. LA SEGURIDAD DEL ACCESO DE TERCEROS

El acceso físico o lógico (conexión a la red) de un contratista o tercero puede introducir un número de riesgos a la seguridad – tales como daño o pérdida de datos en las instalaciones de la Contaduría General de la Nación. Estos riesgos deben ser identificados y evaluados por GIT de Apoyo Informático, y las medidas de seguridad apropiadas se deben acordar con el contratista o tercero y se deben incluir en el contrato.

Las situaciones particulares que se necesiten señalar, especialmente en el acceso lógico, deben incluir lo siguiente:

a. La documentación del acceso en donde se describa, como mínimo, información referente a: responsable de la conexión, fecha de instalación, fecha de desconexión, persona que autoriza, justificación para instalar dicha conexión, personal que usa la conexión, periodos de conexión.

b. La necesidad de identificar y evaluar los riesgos para la Contaduría General de la Nación.

c. Las implicaciones en los planes para la continuidad de la entidad.

d. Los estándares de seguridad a especificarse y el proceso para medir el grado de cumplimiento.

e. Los procedimientos y responsabilidades para reportar y manejar incidentes de seguridad.

f. Las pautas sobre contratos con terceros que estén involucradas en el acceso a instalaciones de la Contaduría General de la Nación.

XV. ACCESO LÓGICO

La Contaduría General de la Nación debe contar con un control efectivo para el cuidado de la información que reside en los sistemas informáticos de la entidad, que tenga lineamientos y políticas que restrinjan el acceso de los usuarios a las aplicaciones y sistemas de la entidad.

XVI. ACCESO FÍSICO

El centro de cómputo de la CGN es una zona restringida y deberá contar con un control de acceso físico apropiado para asegurar que sólo se permita el acceso a personal autorizado.

XVII. CONTROL DE ACCESO

a. Todos los sistemas conectados a la red de la Contaduría General de la Nación deben solicitar el usuario de acceso a la red y contraseña máximo en diez (10) oportunidades. Se debe buscar que información específica como el nombre de la entidad, el sistema operativo, el nombre de la aplicación y otros aspectos relevantes no aparezcan hasta que el usuario tenga acceso exitosamente al sistema.

b. Toda computadora personal deberá contar con una contraseña de protector de pantalla.

c. Todos los usuarios deben ser identificados previamente con un usuario de acceso a la red, que será único en el sistema, y una contraseña secreta para poder usar cualquier computadora multi-usuario, servidores, o recursos de sistemas y aplicaciones en producción.

d. A menos que se hayan otorgado los permisos adecuados por el GIT de apoyo informático, los sistemas no deben permitir sesiones simultáneas con el mismo user-id desde diferentes terminales o PC.

e. Si el usuario está utilizando información sensible clasificada como confidencial, no podrá abandonar su PC, terminal o estación de trabajo sin antes salirse de los sistemas o aplicaciones pertinentes o bloquear la estación de trabajo con el comando Windows + L.

h. Toda computadora personal debe estar desconectada de la red cuando no sea utilizada por periodos prolongados de tiempo (vacaciones, enfermedades, viajes largos, entre otros).

i. Los usuarios deben tener acceso sólo a la información que sea necesaria para el desarrollo de sus actividades y para la cual tengan autorización.

XVIII. CONFLICTOS LEGALES

Las políticas de seguridad de información de la Contaduría General de la Nación fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones. Si algún servidor público y/o tercero de la Contaduría General de la Nación considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al personal encargado de la seguridad informática de la entidad al correo seguridadinformatica@contaduria.gov.co.

XIX. CONCLUSIONES

En la búsqueda de mejorar la seguridad en la entidad, encontramos que los procesos de comunicación y de integración entre las personas no responden a sus necesidades, lo anterior afecta íntegramente a la entidad, tanto internamente como externamente por no dirigir la planeación hacia el modelo de sistema de gestión para su calidad y permanencia. Necesitamos tratar a las personas como afectan nuestros procesos en seguridad, sino reportamos y contribuimos al cambio, jamás tratar a las personas como una unidad.

Si en la entidad, se genera un incremento en el apoyo y reporte de los incidentes de seguridad a la alta dirección, se enfocaría mejor en sus procesos y no habría un alto impacto en el cambio de tecnología. Si los procesos que se definieron con anterioridad son claros y justificados, podríamos brindar mejor protección a la información de los usuarios externos e internos, sin dejar de lado el proceso de negocio, por eso se hace necesario el diseño de un SGSI, que finalmente va a brindar mayor protección para la Contaduría General de Nación y para todos los procesos críticos de la entidad lo cual busca la protección efectiva de la información.

REFERENCIAS

[1] Colombia, el primer país que penaliza los delitos informáticos. La patria. Marzo 2012. :http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980

[2] Advisera, ¿Qué es norma ISO 27001?. http://advisera.com/27001academy/es/que-es-iso-27001/

Antonio Andrés Osorio Sánchez.
Ingeniero de Sistemas Corporación Universitaria Unitec.
Aspirante a Especialista en Seguridad Informática Universidad Piloto de Colombia.
Ingeniero de Soporte en Mesa de Ayuda, en la Contaduría General de la Nación.