# Auditoría, Seguridad y Vulnerabilidad

en el uso de las Tecnologías de Información y Comunicación

**Por: Víctor V. López Chávez, MSe**
Master of Science in Engineering
lopezvictor01@gmail.com
serendipiadas.jimdo.com
63470927

## I. RESUMEN

El propósito principal de este artículo, que comparto hoy con ustedes, es el de fomentar una cultura en donde se valore y se le brinde la debida importancia a la auditoría, la seguridad, la vulnerabilidad, la pérdida y recuperación de los datos, en en el uso de las Tecnologías de Información y Comunicación; elementos necesarios para la generación de alternativas y mejor toma de decisiones en las organizaciones. También está el diseñar, estructurar e implementar una estrategia oportuna, pertinente con una política de procedimientos que obedezca a las normas ISO 27001: 2013 y a los procedimientos de auditoría que requiera la organización. Además el planificar una auditoría de sistemas que nos permita monitorear y dar seguimiento a las normas y procedimientos establecidos en la organización. Por otro lado está el capacitar a los usuarios, expertos de sistemas en las estrategias y planes de seguridad para evitar situaciones críticas. Igualmente debemos simular pruebas y experimentos con diversos escenarios de misión crítica en donde se vulneren servidores de datos, aplicaciones en desarrollo y producción, correo e impresión para estar preparados ante cualquier situación adversa que se presente. Finalmente y no menos importante debemos fomentar el trabajo colaborativo entre los usuarios y los especialistas de sistemas para que coadyuven a la actualización, aplicación y al seguimiento de las normas, políticas y procedimientos para crear un ambiente en donde reine la seguridad, la estabilidad y la confianza en el uso de las TIC.

## II. PALABRAS CLAVES

Actualización, Innovación, Cambio, Seguimiento, Control, Estabilidad, Confianza, Riegos, Respaldos, Recuperación, Datos, Información, Comunicación, Normas, Políticas, Procedimientos, Usuarios, Equipos, Programas, Tecnologías, Redes, Servidores, Switches, Routers.

## III. SITUACIÓN ACTUAL

### 1. ¿Qué está sucediendo con la Seguridad de la Información en nuestras organizaciones?

La información se define como un conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. El esquema completo de la comunicación, consiste en un emisor que transmite un mensaje a través de un canal con ruido en un contexto que tiene como destino un receptor; en donde los usuarios hacen uso de las Tecnologías de Información y Comunicación para compartir, transmitir, almacenar, recuperar y manipular datos, para uso personal, en nuestros hogares, en nuestros negocios y en las organizaciones dónde laboramos a diario.

En la actualidad, las organizaciones o empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. El activo más importante en una organización después del recurso humano es la información. Esta última se encuentra ligada o asociada a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

Estamos frente a un mundo nuevo. Menos tiempo. Menos presupuesto. Menos recursos. Más dispositivos. Más amenazas. Más cosas en riesgo. Los switches, routers y soluciones inalámbricas, están desarrollados para una arquitectura de red digital, que fortalecen el estado de su seguridad a través de estar Constantemente aprendiendo. Constantemente adaptándose. Constantemente protegiendo. Estamos en busca de una red evolucionada, una red intuitiva, que nos brinde soluciones sometidas a una constante, que es el cambio.

El concepto seguridad se refiere a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia en la seguridad. En términos generales, la seguridad se define como "el estado de bienestar que percibe y disfruta el ser humano". Lo que traducido al ámbito de las Tecnologías de Información y Comunicación, hace referencia a la reducción de la posibilidad de la pérdida y/o recuperación de datos por parte de los usuarios y especialistas que coadyuvan a la implementación de normas y procedimientos para crear entornos de alta confiabilidad y seguridad de la información de la organización.

## IV. PROBLEMA

### 2. ¿Por qué se afecta la Seguridad de la Información y cómo están distribuidos los usuarios de internet en Panamá?

Una red de computadoras es un conjunto de equipos informáticos y programas conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos y tiene como finalidad el compartir información, recursos y ofrecer servicios. Precisamente es este último punto el causante de toda esta polémica.

Panamá es un país que por su posición geográfica se dedica a la compra y venta de bienes y servicios. La población estimada de Panamá al 3 de noviembre de 2016, totaliza 4,058, 372 habitantes, con una tasa de crecimiento anual de 1.55%, según información del Instituto Nacional de Estadística y Censo (INEC) de la Contraloría General de la República.

Según las estimaciones del INEC, la provincia de Panamá tiene 1,552,343 habitantes y una tasa de crecimiento de 1.81%; Panamá Oeste es la segunda provincia con mayor población, tiene 567,886 habitantes y cuenta con una de las tasas de crecimiento más altas con 2.16% por año.

Las diferencias sociales que la tecnología puede provocar se hacen más notorias cuando de acceso a Internet se trata. Del total de hogares en el país, sólo 20.2% contaban con conexión a Internet. Fue la provincia de Panamá (28.8%) la única en superar la media nacional de los hogares con conexión a Internet, situación esperada y que se presentó al ser la provincia con más acceso a este servicio, territorialmente.

Le siguieron las provincias de Colón (18.3%), Chiriquí (13.5%), Herrera (13.2%), Los Santos (9.3%), Coclé (8.5%), Veraguas (8.2%), Bocas del Toro (7.7%) y Darién (1.2%). Orden atribuible a la magnitud urbanística de cada una de las provincias. En las comarcas Kuna Yala, Emberá y Ngöbe Buglé contaron con 0.2%, 0.1% y menos de 0.05% de hogares con Internet, respectivamente, situación provocada en parte por la escasez de fluido eléctrico, el acceso limitado al servicio en estas zonas muy apartadas y por lo costoso que puede ser obtenerlo, incluso en términos de los accesorios.

Como podemos observar, estamos ante un proceso en que se está produciendo modificaciones, por lo que el término Seguridad de la Información está tomando una traducción más acertada. Aunque aún hay muchos especialistas que siguen nombrándolo según el enfoque técnico que hemos comentado anteriormente; la Seguridad de la Información es muy extensa, por lo que no es sólo una cuestión técnica, sino que supone una responsabilidad de la alta dirección de la organización o empresa, así como de sus directivos.

Los riesgos operacionales son hoy en día más cruciales en lo referente a Seguridad de la Información. Las vulnerabilidades de este tipo de riesgo se expanden durante una amplia gama de grises, en conexión con el comportamiento humano y los juicios subjetivos de las personas, la resistencia al cambio, la cultura organizacional, la forma de comunicarse, entre otros.

Se tiene que considerar los sujetos, los procesos y las funciones de negocio, además de la protección de todos los activos/recursos de la entidad impulsora, propietaria y beneficiaria de la Seguridad de la Información, dentro de un marco de responsabilidades compartidas.

Se tienen que considerar la totalidad de los riesgos técnicos de las TIC, además de que la seguridad se desarrolle por toda la organización, es decir, son riesgos administrativos, operacionales y físicos.

Tenemos que tomar en cuenta que el ambiente de las TIC está orientado al servicio y a la actuación en función de los procesos de negocio. Se diferencia de los procesos centrales en que constituyen el núcleo de los negocios de la organización.

En el caso de no involucrarse las unidades activas y los líderes de negocio, como podrían ser, ejecutivos, directivos, entre otros. de las entidades, no podrá existir un plan de Seguridad de la Información, a partir de todos los riesgos determinados. Todo ello se lleva a cabo en el seno del sistema de dirección y control propio del gobierno de la organización.

## V. SOLUCIÓN

### 3. ¿Cuál es la solución para compartir información, recursos y ofrecer servicios en el uso de las TIC?

La solución está en gestionar las vulnerabilidades de los sistemas de información que se hayan mitigado al identificar, remediar y verificar que las diferentes debilidades. Se pueden realizar escaneos constantes por medio de una aplicación a todos los dispositivos, aplicaciones, servicios, criterios de evaluación y servidores de la red de la compañía.

La solución está en ser proactivos. Configurando correctamente mi perfil de usuario en las aplicaciones en el uso de las TIC, antes de compartir_información, recursos y ofrecer servicios. De esta forma evitamos ser vulnerables a los ataques cibernéticos disminuyendo la probabilidad de ser víctimas de un fraude o de la pérdida de datos e información al momento de hacer uso de las TIC.

La solución está en realizar una auditoría informática que es un proceso llevado a cabo por profesionales especialmente capacitados para tal efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas. Permiten detectar de Forma Sistemática el uso de los recursos y los flujos de información dentro de una Organización y determinar qué Información es crítica para el cumplimiento de su Misión y Objetivos, identificando necesidades, falsedades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

En sí, la auditoría informática está definida por 2 tipos:

**Auditoría Interna:** Es aquella que se hace desde dentro de la empresa; sin contratar a personas ajena, en el cual los empleados realizan esta auditoría trabajan ya sea para la empresa que fueron contratados o simplemente algún afiliado a esta.

**Auditoria Externa:** Como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoría en su empresa. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Otra de las soluciones eficientes para auditar la seguridad y la vulnerabilidad en el uso de las TIC, es contratar a un proveedor de seguridad de la información administrable o Managed Security Service Provider, que ofrecen servicios de coberturas que se ajustan a las necesidades particulares de su organización.

## VI. CARACTERÍSTICAS Y BENEFICIOS

### 4. ¿En qué consiste y cuáles son los beneficios de la Auditoría de Seguridad y Vulnerabilidad en el uso de las TIC?

La gestión consiste en identificar, remediar y verificar que las diferentes vulnerabilidades de los sistemas de información se hayan mitigado. Se pueden realizar escaneos constantes por medio de una aplicación a todos los dispositivos, aplicaciones, servicios, criterios de evaluación y servidores de la red de la compañía.

La totalidad de los especialistas en seguridad basan sus conocimientos y experticias sobre el aspecto técnico tradicional de la seguridad, esto es en las áreas TI (tecnologías de información), aunque bastantes de ellos consideran las cuestiones propias como el nuevo aspecto en las comunicaciones y que hace que actualmente se hable de las TIC (tecnologías de información y comunicación).

Además de tener un enfoque técnico prácticamente, los especialistas únicamente se manejan con las vulnerabilidades y en parte con amenazas en forma de ataques, todo lo dicho no se considera suficiente para hablar de los riesgos correspondientes.

Cuando los servicios de seguridad se adquieren de manera externa, una de las principales ventajas que se considera es la experiencia y conocimiento del personal que participa, ya que si mantiene una capacitación constante, puede contar con un

mayor panorama sobre amenazas informáticas y vulnerabilidades. Además, se obtiene una perspectiva objetiva e imparcial sobre lo que sucede en las organizaciones.

Los objetivos de la auditoría Informática son:

- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Desempeño, Fiabilidad, Eficacia, Rentabilidad, Seguridad, Privacidad.

Por otro lado la seguridad de la información genera o produce estabilidad, fortaleza y sobre todo confianza en la generación de alternativas para la mejor toma de decisiones en la organización o empresa.

**También existen otros tipos de auditoría:**

- Auditoría operacional: Se refiere a la revisión de la operación de una empresa y juzga la eficiencia de la misma.
- Auditoría administrativa: Se refiere a la organización y eficiencia de la estructura del personal con la que cuenta el personal y los procesos administrativos en que actúa dicho personal.
- Auditoría social: Se refiere a la revisión del entorno social en que se ubica y desarrolla una empresa, con el fin de valorar aspectos externos e internos que interfieren en la productividad de la misma.

**Sus beneficios son:**

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (re-procesos, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

## VII. CONCLUSIONES

### 5. ¿Qué observaciones hemos encontrado durante la realización de este estudio?

El avance que experimentó la población con respecto al acceso y uso de internet en torno a diferencias que han provocado el nivel de ingresos, conectividad, ubicación y área geográfica, entre otras situaciones sociales, permite conocer el estado de la brecha digital entre los que efectivamente forman parte de esta nueva forma de comunicarse y los que no.

Actualmente existe una la ley de propiedad intelectual, que regulan los aspectos relacionados a la piratería informática y una ley de comercio electrónico que establece cuales son los procedimientos y normas al registrar una tienda virtual para realizar compra y venta de bienes y servicios a través de internet.

En Panamá existe una alta incidencia de delitos cibernéticos, o que se comenten por internet, informó a TVN el fiscal superior especializado de delitos contra la propiedad intelectual y seguridad informática, Ricaute González Torres el 14 de diciembre de 2016.

Existe también un marco teórico, más no así, un marco jurídico en donde se establezca una ley que regule una cultura de Auditoría que regule la Seguridad y Vulnerabilidad en el uso de las TIC, como medida preventiva a los delitos Cibernéticos.

Una auditoría de sistemas nos permite establecer las distintas vulnerabilidades de la empresa por medio de un proceso muy distinto a las mediciones o lecturas tomadas con las computadoras, servidores, switches, routers, entre otros. Como normalmente no se disponen de datos históricos suficientes, realizar un análisis exacto se hace muy complicado. Por lo que un verdadero análisis se complementa con la información que se puede recabar por medio de Apps especializados y finalmente se debe realizar entrevistas que establecen el valor de los activos de la institución que están en riesgo.

Entre los Servicios Especializados que una empresa proveedora de servicios de seguridad de la información ofrece están los siguientes:

- Buscador de Seguridad: (Blindar Portales y Aplicaciones Web, Asegurar la Red Interna, Seguridad Perimetral, Filtrado de Contenidos, Aseguramiento de Datos, Asegurar Redes Wirless, Prevenir Fuga de Información, Administración de Seguridad, Protección a PC's & Servidores).
- Servicios Administrados: (MSSP Ciberseguridad, MSSP Continuity Partner, MSSP Antivirus HandsOn, MSSP Antivirus HandsOn PLUS, MSSP Next Generation Firewall, MSSP AntiSpam HandsOn, MSSP Optimized Network, MSSP Guarantee Backup).

- **Cumplimiento Normativo:** (Sistema de Gestión 27001, Análisis y Gestión de Riesgos, Estudio de Seguridad TI, Cyber Security Audit Controls).
- **Análisis de Seguridad:** (Pruebas de Penetración, Análisis de Vulnerabilidades, Gestión de Vulnerabilidades, Wireless Security Assessment, Pruebas de Ingeniería Social, Análisis de Código Fuente, Cómputo Forense, Recuperación de Datos).
- **Pólizas de Soporte Técnico:** (Póliza de Servicio Básica, Póliza de Servicio Avanzada).

# VIII. RECOMENDACIONES

## 6. ¿Cuáles deben ser ahora los pasos a seguir?

- Promover una ley que regule una cultura de Auditoría que regule la Seguridad y Vulnerabilidad en el uso de las TIC, como medida preventiva a los delitos Cibernéticos.
- Realizar un FODA (Fortalezas, oportunidades, debilidades y amenazas) sobre Auditoría, Seguridad y Vulnerabilidad en el uso de las TIC.
- Crear un POA en donde aparezcan los rubros a invertir durante este Plan Operativo Anual.
- Presentar y Aprobar un presupuesto en donde se muestre un cronograma de actividades a corto, mediano y largo plazo donde se de la cultura de la Seguridad de la Información.
- Crear una estrategia oportuna, pertinente con una política de procedimientos que obedezca a las normas ISO 27001: 2013 y a los procedimientos de auditoría que requiera la organización.
- Planificar una auditoría de sistemas que nos permita monitorear y dar seguimiento a estas normas y procedimientos de la pérdida y recuperación de los datos de la organización.
- Capacitar y dar seguimiento a los usuarios y especialistas en cuanto a las normas y procedimientos oportunos y pertinentes basados en la Norma ISO: 27001: 2013.
- Fomentar el trabajo colaborativo entre los los usuarios y especialistas.
- Crear un ambiente en donde reine la seguridad, la estabilidad y la confianza en el uso de las TIC.
- Innovar, Implementar y Auditar las políticas, normas y procedimientos que sean necesarios y luego realizar una auditoría que garantice la seguridad, estabilidad y confianza en el uso de las TIC: (Norma ISO 27001: 2013, seguridad Informática, evaluación de riesgos, medidas de seguridad, seguridad de la Información, riesgos técnicos de TIC, vulnerabilidades de una empresa, evaluación de activos, seguridad informática, sistema de gestión de seguridad de la información).
- Establecer cuáles son los roles, papeles o funciones específicas de los usuarios y especialistas durante la ejecución de la cultura de Auditoría, Seguridad y Vulnerabilidad en el uso de las TIC.
- Adicionalmente les recomiendo seguir los siguientes consejos a los usuarios y especialistas: (siempre piensa, no compartas tu contraseña, siempre finaliza tu sesión antes de apagar tu computadora, mantén tus datos en privado como dirección y teléfono, respeta a los demás, sé responsable con tus comentarios y opiniones, utiliza un apodo o un alias que sólo conozca tus amigos y familia, no aceptes solicitudes de desconocidos, tampoco establezcas contacto con ellos, ni compartas tus datos, siempre se consiente de su huella digital, revisa siempre las cláusulas de privacidad de sitios donde te registres. Tú también tienes voz, denuncia si encuentras algo inadecuado).

# IX. CIBERGRAFÍA

## 7. ¿Cuáles fueron las fuentes de información consultadas durante esta investigación?


**Enlaces**

- Auditoría de sistemas
  http://tic01sv-14rigoberto.blogspot.com/
- Gestión de vulnerabilidades
  https://protektnet.com/servicios/analisis-de-seguridad/gestion-de-vulnerabilidades/
- Gestión de vulnerabilidades
  http://www.gb-advisors.com/es/gestion-de-vulnerabilidades/
- La red intuitiva – basada en cisco DNA (digital network architecture)
  http://www.cisco.com/c/es_mx/solutions/enterprise-networks/index.html?stickynav=1
- ISO 27001:2013 AWARENESS TRAINING
  http://www.oeconsulting.com.sg/ppt-iso-27001-isms-awareness
- Soluciones de seguridad ti
  https://protektnet.com/soluciones/#soluciones
- Estadísticas según INEC (Instituto Nacional de Estadística y Censo)
  http://laestrella.com.pa/economia/poblacion-estimada-panama-4058372-segun-inec/23968996
- Atlas Social de Panamá, Ministerio de Economía y Finanzas, Acceso y uso de las Tecnologías de Información y Comunicación
  http://www.mef.gob.pa/es/informes/Documents/11%20-%20Acceso%20y%20uso%20de%20las%20tecnologias%20de%20informacion%20y%20comunicacion.pdf
- Panamá con alta incidencia de delitos cibernéticos, https://www.tvn-2.com/nacionales/Panama-incidencia-delitos-ciberneticos-fiscal_0_4643535619.html

**Videos**

- Seguridad de la Información - "Arquitectura de seguridad en la red de datos"
  https://www.youtube.com/watch?v=BdSaeX8Srak&feature=youtu.be
- The Network. Define.
  https://youtu.be/ZuJjncuptz0
- The Network. Intuitive.
  https://youtu.be/NJF1Em5IMlU


**X. ANEXO**

- Nuevas Versiones ISO27001 e ISO27002
  https://www.dropbox.com/s/04yyldno27tsnyr/NuevasVersionesISO27001eISO27002-FODA.pdf?dl=0