

Universidad CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de una guía para la revisión de la seguridad de las bases de datos que deben ser reguladas por la Agencia de Protección de Datos de los Habitantes (PRODHAB)

Estudiante:

Ing. Yahaira Rocio Sosa Arias

Agosto 2018

Declaratoria de Derechos de autor

©2018, Guía para la revisión de la seguridad de las bases de datos que deben ser reguladas por la Agencia de Protección de Datos de los Habitantes (PRODHAB), Sosa Arias, Yahaira Rocio

La presentación de este documento está sometida a procesos de confidencialidad. La vigencia de esta cláusula es por un periodo de: 5 año(s), a partir de la fecha de realizado el documento. Una vez pasado dicho periodo, el trabajo se pondrá a disposición de estudiantes, personal docente o administrativo, en la biblioteca de la Universidad, tanto para estudio, consulta o ejemplificación en clases relacionadas con el tema.

DEDICATORIA

Dedico este trabajo con todo mi amor y cariño a mi amada hija Victoria por ser mi fuente de motivación e inspiración para superarme cada día, a mi esposo José Joaquín quien fue incondicional todo este tiempo y a mis padres Rocío y Alcides, que han sido el equipo detrás de las cámaras ocupándose de temas y situaciones en las que yo no podía participar, han sabido comprender el sacrificio y esfuerzo de trabajar, estudiar y sobre todo el aceptar de forma comprensiva mi relativa ausencia en sus vidas durante estos últimos dos años, a Dios y a la Virgen María que me han guiado y acompañado, sin soltar mi mano todo el camino.

Gracias a todos

AGRADECIMIENTO

A Dios y la Virgen, por permitirme cumplir esta meta y haberme dado salud y recursos para lograr mis objetivos, además de su infinita bondad y amor.

A mi familia, por haberme apoyado en todo momento, por sus consejos, su acompañamiento y su colaboración incondicional, además de su amor.

A CENFOTEC por darme la oportunidad de estudiar y ser una profesional en Seguridad de la Información.

A mi tutor Miguel Pérez por su esfuerzo y dedicación, quien, con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

Son muchas las personas que han intervenido en este proyecto amigos y amigas del alma, de esos que son parte del corazón, me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida.

Para ellos mis más sinceros deseos de bendición y prosperidad, no es igual llegar a la meta solo que llegar con un equipo de trabajo que tuvo fe en mí y en mis capacidades. Dios los bendiga enormemente.

Tabla de Contenido

Declaratoria de Derechos de autor 2

DEDICATORIA 3

AGRADECIMIENTO 4

Lista figuras 8

Resumen ejecutivo 9

Capítulo 1. Introducción 10

Descripción del proyecto 10

1.1 Generalidades 10

1.2 Marco filosófico 11

1.3 Objetivos de la Agencia 11

1.4 Antecedentes del problema 13

1.5 Definición y descripción del problema 15

1.6 Justificación 16

1.7 Viabilidad 17

1.7.1 Punto de vista técnico 17

1.7.2 Punto de vista operativo 17

1.7.3 Punto de vista económico 17

1.8 Objetivos 18

1.8.1 Objetivo general 18

1.8.2 Objetivos específicos 18

1.9 Alcances y Limitaciones 18

1.9.1 Alcances 18

1.9.2 Limitaciones 19

Capítulo 2. Marco teórico 20

2.1. Introducción 20

2.2. Orígenes del termino seguridad 20

2.3. ¿Qué es la seguridad de la información? 21

2.3.1. Resguardo de la información 22

2.3.2. Respaldo de la información 22

2.3.3. Recuperación de la información 22

2.4. Objetivo de la seguridad informática 23
2.5 Por qué es importante proteger sistemas, equipos y bases de datos? 26
2.6 Seguridad física 27
2.7 Elementos claves para la gestión de seguridad de la información 28
2.8 Seguridad lógica 30
2.9 Algunas consideraciones sobre protección de datos personales y delitos informáticos..... 30
Capítulo 3. Marco metodológico..... 42
3.1 Tipo de investigación..... 42
3.2 Alcance investigativo..... 43
3.3 Enfoque 43
3.4 Diseño..... 44
3.6 Instrumentos de Recolección de Datos..... 45
3.7 Técnicas de análisis de la información 45
Capítulo 4. Desarrollo de la solución..... 46
Capítulo 6. Recomendaciones..... 50
Capítulo 7. Reflexiones finales 51
Capítulo 8. Trabajos a futuro..... 52
Referencias Bibliográficas 54
ANEXOS 57
Anexo 1. Normas Generales de Inspecciones de Oficio/ Auditorías..... 58
CONSIDERANDO 59
PRESENTACIÓN..... 63
INTRODUCCIÓN 63
CAPÍTULO I 65
NORMAS PERSONALES..... 65
1. Independencia y objetividad..... 65
2. Naturaleza confidencial y discreción sobre el trabajo 65
3. Ética profesional..... 65
4. Competencia y pericia profesional..... 66
5. Debido cuidado profesional 66
6. Educación profesional continua 67
CAPÍTULO II 67

NORMAS GENERALES RELATIVAS AL TRABAJO DE INSPECCIÓN/AUDITORÍA EN EL SECTOR PÚBLICO/PRIVADO Y PRIVADO 67
1. Administración de la inspección/auditoría 67
2. Actividades del proceso de inspección/auditoría 67
3. Planificación 67
4. Examen 69
5. Comunicación de resultados 69
6. Seguimiento 71
7. Evidencia de inspección/auditoría 72
8. Documentación de la inspección/auditoría 72
9. Archivo permanente 73
Capítulo III 75
NORMAS GENERALES SOBRE INSPECCIÓN/AUDITORÍA DE CUMPLIMIENTO 75
1. Planificación 75
2. Criterios de inspección/auditoría 75
3. Evidencia 75
4. Comunicación de resultados 75
Anexo 2. Descripción General de la Auditoría 76
Anexo 3. Planificación de la Auditoría 81
Anexo 4. Ejecución de la Auditoría 94
Anexo 5. Planificación de la Auditoría 107
RESUMEN 108
1. INTRODUCCIÓN 108
2. OBSERVACIONES 110
3. CONCLUSIONES 110
4. ATRIBUCIONES/REQUERIR 111
ANEXOS 111

Lista figuras

Figura 1. *Organigrama de la Agencia de Protección de Datos* 12
Figura 2. *Diagrama de Ishikawa: Análisis causa-efecto de los problemas* 46

Resumen ejecutivo

El propósito fundamental de la presente investigación es crear una guía para auditar la seguridad de las bases de datos que deben ser reguladas por la Agencia de Protección de Datos de los Habitantes (PRODHAB) en Costa Rica.

Esto con el fin de iniciar con el cumplimiento de su función asociada a las inspecciones de oficio, al proveer un instrumento que facilite el chequeo a realizar cuando exista la necesidad de auditar una base de datos que contenga información sensible de los habitantes de Costa Rica.

La incorporación del área de auditoría de tecnologías de información propiamente en seguridad es un reto para la PRODHAB que se visualiza y debe ser realizado en los próximos 2 años.

Por otro lado, se necesita personal capacitado en temas de auditoría que pueda comprender e implementar la guía que se planea desarrollar en este proyecto.

Capítulo 1. Introducción

Descripción del proyecto

1.1 Generalidades

La Agencia de Protección de Datos de los Habitantes (PRODHAB) es una institución adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de las funciones y en la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones.

Su principal objetivo es garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto al derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de la libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Asimismo, orienta al ciudadano a ejercer sus derechos y a las entidades públicas y privadas que manejan bases de datos, a cumplir las obligaciones que establece la Ley creada el 7 de julio del 2011, publicada en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011 bajo el No. 8968.

La PRODHAB fue creada mediante la Ley N° 8968 del 7 de julio del 2011, publicada en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011.

Sus funciones y procedimientos son especificados mediante el Reglamento a la Ley (en adelante RPDP) el Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012 y publicado en el Alcance No. 42 de Diario Oficial La Gaceta, No. 45 del 05 de marzo del 2013.

El 06 de diciembre del 2016, entró en vigor el Decreto Ejecutivo No. 40008-JP, a fin de realizar una serie de nuevas reformas al Reglamento de la Ley 8968.

Con lo anterior, se pretende actualizar la normativa costarricense sobre protección de datos personales a la corriente de tendencias internacionales en la materia, a través de la aclaración de aspectos que en su momento suscitaron inquietudes respecto a la Ley y su aplicación, así como coadyuvar a las instituciones públicas y privadas a cumplir con las garantías, derechos otorgados y la simplificación de los trámites que corresponden, garantizando mayor fluidez en la transferencia y comercialización de datos y mejor control y competencia en la protección de datos personales.

1.2 Marco filosófico

Misión

La Agencia de Protección de Datos de la República de Costa Rica es una entidad pública, que garantiza a toda persona su derecho fundamental a la autodeterminación informativa y demás derechos de la personalidad, la defensa de su libertad e igualdad con respecto al tratamiento de la información correspondiente a sus datos y al de sus bienes.

Visión

Ser una organización pública reconocida a nivel nacional e internacional, con una cultura de transparencia, y de buenas prácticas en la protección de datos de la persona y los de sus bienes.

1.3 Objetivos de la Agencia

- Garantizar el respeto al derecho fundamental de la autodeterminación informativa en la sociedad para salvaguardar la vida o actividad privada de las personas.
- Impulsar el intercambio científico tecnológico en materia de protección de datos personales. (PRODHAB, 2017).

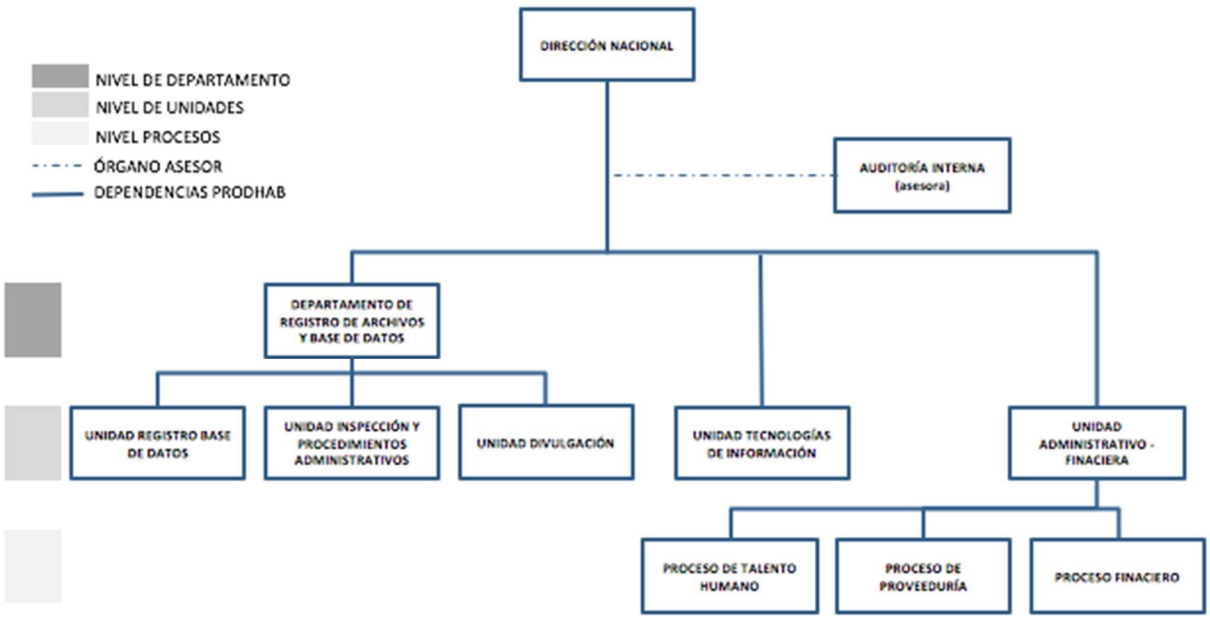


Figura 1. ***Organigrama de la Agencia de Protección de Datos***

Fuente: *MIDEPLAN, Resolución N 104-2013-PLAN*

1.4 Antecedentes del problema

La institución se encuentra adscrita al Ministerio de Justicia y Paz y su objeto es garantizar la protección de la persona frente al tratamiento de sus datos personales.

Sus dos principales funciones son las siguientes:

1. La inscripción de las bases de datos conforme a la Ley 8968 de Protección de Datos que establece que toda base de datos pública o privada administrada con fines de distribución, difusión o comercialización, debe inscribirse en la PRODHAB.

2. Trámite de denuncias ya que las personas tienen derecho al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos en cualquier base de datos.

Para ejercer sus funciones la PRODHAB cuenta con una unidad financiera, una unidad de recursos humanos, una unidad de proveeduría, una unidad legal, una unidad de tecnologías de información y finalmente con un director nacional.

A pesar de que se estableciera su creación en el año 2011, inicia operaciones a partir del año 2013 con 3 personas tramitando denuncias de 11 que son la totalidad de los colaboradores; 8 personas se integraron a la PRODHAB a partir del mes de julio del año 2015. Se puede entender que, debido al poco tiempo que tiene de operar, la madurez de sus procesos se encuentra en desarrollo y la mayoría se realizan de forma manual; sin embargo, se espera que en el segundo semestre del año 2018 se esté tramitando la contratación de equipo tecnológico (de hardware y software) que permita automatizar algunos de los procesos de la entidad.

Siendo que se está avanzando con la automatización de los procesos, se vuelve necesario el tema de la seguridad informática, porque la tecnología permite la posibilidad de interconectarse a través de redes, abriendo nuevos horizontes para

explorar más allá de las fronteras nacionales, lo que resulta en nuevas amenazas en las tecnologías de información.

Esto ha provocado que muchas organizaciones gubernamentales y no gubernamentales, alrededor del mundo, hayan desarrollado documentos y directrices que orientan a sus usuarios en el uso adecuado de herramientas tecnológicas y recomendaciones para obtener el mayor provecho de éstas y evitar el uso indebido de la mismas, lo que puede ocasionar serios problemas en los bienes y en los servicios que prestan las instituciones.

Las políticas institucionales de seguridad informática surgen como un lineamiento organizacional para concientizar a cada uno de sus miembros sobre la importancia y sensibilidad de la información y servicios críticos que existen en la organización.

Las estrategias y recomendaciones que se puedan dar en esta área contribuirán a que se generen nuevos conocimientos que permitan aplicar mejores prácticas en los procesos y acciones que se realizan en los diferentes lugares en donde existan instalaciones que cuenten con equipo tecnológico computacional y programas para operarlos, las estrategias ofrecen recomendaciones en la gestión de la seguridad informática y permiten la preservación de la confidencialidad, integridad y disponibilidad de los datos.

Es por ello que en los siguientes apartados se presenta una propuesta que permita a la PRODHAB la creación de una guía de auditoría para verificar la seguridad de la información de las bases de datos que deben ser reguladas con base a la Ley 8968 por la PRODHAB.

1.5 Definición y descripción del problema

Debido a la creciente utilización de las tecnologías de la información y comunicaciones en las empresas en el mundo, además de la importante cantidad de información que está en formato electrónico, nace la problemática de la seguridad de la información, misma que busca proteger la confidencialidad, integridad y disponibilidad de los datos.

Considerando que es a mediados del 2015 cuando se integra la mayoría de personal a formar parte de sus diversas unidades funcionales, entre ellas a la Unidad de Tecnologías de Información, se puede entender que los procesos y la gestión específica de tecnologías de información tienen poco tiempo de existir.

Por ser una institución gubernamental, debe cumplir con las Normas que emitan entidades como la Contraloría General de la Republica, así como las buenas prácticas y estándares internacionales en materia de gestión de las tecnologías de información.

Adicionalmente una de las aristas fundamentales de la Ley 8968 es que la PRODHAB puede hacer inspecciones de oficio que permitan verificar que existe un adecuado tratamiento de los datos personales, es decir, revisar los protocolos mínimos de actuación implementados por la empresa/entidad con la finalidad de garantizar una adecuada seguridad de la información en el tratamiento de los datos personales.

Se ve la necesidad de que se atienda de manera prioritaria y pronta lo referente a crear un instrumento que facilite el proceso de realizar inspecciones de oficio, propuesta que se desarrolla en el capítulo 4, y se adjunta en los anexos.

1.6 Justificación

La información es un recurso clave para todas las empresas y desde el momento en que la información es creada hasta el momento que es destruida, la tecnología tiene una función significativa. En la actualidad la computación y la informática son una parte importante del desarrollo de la sociedad, debido a que estas tecnologías son en gran medida las que han permitido mejorar en sectores sociales, económicos, en la calidad de la educación y una mejor calidad de vida para las personas.

Pero al igual que cualquier otra tecnología de innovación que se haya diseñado en el pasado, necesita de procesos y estrategias que le ayuden a desarrollarse y que le permitan un mejor cumplimiento de los objetivos por la que se diseñó y creó.

Es ahí donde radica la importancia de brindarle mecanismos de seguridad a estos equipos y programas informáticos que a diario se utilizan y que propician el desarrollo en muchos de los entornos en los que interactúan y participan.

Es por ello que surge la necesidad de contar con una Guía de Auditoría que le permitiría a la PRODHAB fortalecer el proceso de inspecciones de oficio, mediante el establecimiento de criterios básicos de control que deben ser observados durante la auditoría de una base de datos, ya sea de carácter privado o pública, y poder profundizar en el tipo de tecnologías involucradas en la infraestructura que de alguna forma son parte de la gestión de la base de datos y que a su vez coadyuven en el control y fiscalización de los recursos que posee la institución auditada.

La seguridad de la información, según la norma ISO/IEC 27001:2014 (Norma que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información - SGSI)), consiste en la

preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Además, como institución gubernamental debe acatar lo establecido en el Manual denominado “Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE)” desarrollado por la Contraloría General de la República de Costa Rica. Tomando en cuenta que estas normas son de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, adicionalmente se debe cumplir con la Ley de Control Interno y sus normas para garantizar su eficacia y eficiencia en cuanto a los procedimientos de tecnologías de información.

Razón por la que resulta prioritario que se analicen estas normativas para esta investigación y que se complementen e integren con la Ley 8968 que se propondrá para la realización del trabajo en mención.

1.7 Viabilidad

1.7.1 Punto de vista técnico

La PRODHAB cuenta con hardware y software disponibles, para cubrir las necesidades incluso de almacenamiento de esta investigación. Se cuenta con el acceso a la Ley de Protección de Datos y su reglamento y a la legislación costarricense a través de internet.

1.7.2 Punto de vista operativo

A nivel operativo se cuenta con la aprobación y el apoyo de la Directora de la Agencia y del encargado de la Unidad de Tecnologías de Información.

1.7.3 Punto de vista económico

Se refiere a que se dispone del capital en efectivo o de los créditos de financiamiento necesarios para invertir en el desarrollo del proyecto, mismo que deberá haber probado que sus beneficios a obtener son superiores a sus costos en que incurrirá al desarrollar e implementar el proyecto o sistema.

El proyecto necesita recurso a nivel humano para realizar la investigación y sus diferentes etapas como el análisis, desarrollo e implementación, por lo que no es necesario realizar una inversión monetaria ni contemplar inversión por parte de la Agencia y/o un tercero.

El proyecto tendrá así una viabilidad económica asegurada para su pleno desarrollo.

1.8 Objetivos

1.8.1 Objetivo general

Preparar una guía que ayude a verificar la seguridad de la información de las bases de datos que deben ser reguladas de acuerdo a la Ley 8968 por la Agencia de Protección de Datos de los Habitantes (PRODHAB).

1.8.2 Objetivos específicos

1. Identificar las necesidades de documentación que tiene la PRODHAB asociadas al cumplimiento de la Ley 8968, en el Unidad de Auditoría.
2. Determinar las especificaciones de seguridad de la información establecidas en la Ley 8968.
3. Investigar buenas prácticas de gestión de Tecnologías de Información, que complementen el cumplimiento de la Ley 8968 en materia de seguridad de la información.
4. Construir la Normativa y protocolos que permitan auditar y verificar la seguridad de la información en las bases de datos reguladas por la Ley 8968.

1.9 Alcances y Limitaciones

1.9.1 Alcances

1. Se capacitarán a los colaboradores de la PRODHAB con el fin de que puedan utilizar el instrumento que va a ser desarrollado en esta investigación para realizar inspecciones y/o auditorías revisando aspectos relacionados con la

seguridad de las bases de datos y la protección de datos personales, con la finalidad de generar conciencia y ser un punto de partida en esta área.

2. Lo que se busca es formar las bases y puede considerarse la importancia de éstas para las futuras inspecciones y/o auditorías.

3. Se intenta concienciar sobre esta área de la informática que tiene gran auge y/o importancia en la actualidad para todas las empresas e instituciones a nivel mundial y considerando que el instrumento a desarrollar va a marcar un antes y un después en la percepción de la gestión de auditoría en la Agencia.

4. El desarrollo del proyecto permitirá tomar las bases de esta área, permitiendo que se empiecen a considerar aspectos a los que posiblemente no se les daba el nivel de importancia que debería e incluso la creación de la Unidad de Auditoría con asignación de personal que se dedique a esta labor.

5. Podrá servir como referencia a otras instituciones que deseen conocer acerca de la seguridad en las bases de datos y la protección de datos personales.

6. El futuro encargado de la Unidad de Auditoría podría generar estrategias que propicien y mejoren los conocimientos en este campo.

7. Conocer más sobre las legislaciones, normas, marcos de referencia que le aporten valor a la guía propuesta en este proyecto.

1.9.2 Limitaciones

1. Este proyecto pretende ser un punto de partida para concientizar a la PRODHAB sobre la necesidad de utilizar una guía que permita revisar controles asociados a la seguridad de las bases de datos y a su vez tome en cuenta la protección de los datos personales.

2. El desarrollo y el logro de toda la investigación dependerá del interés que se le dé por parte de los actores que participan en él.

3. Falta de personal, actualmente la PRODHAB cuenta solo con 3 colaboradores en TI, por lo que se vuelve fundamental la creación y el equipo de trabajo que pueda realizar las inspecciones y/o auditorías, utilizando la guía que se pretende crear en este proyecto.

Capítulo 2. Marco teórico

2.1. Introducción

El motivo del presente capítulo es dar a conocer los aspectos teóricos más importantes, como marco referencial del tema de estudio, que aparte de las definiciones, tiene una clara inclinación hacia la seguridad informática y describe la manera en que se relacionan con el estudio realizado.

2.2. Orígenes del termino seguridad

La seguridad es una necesidad básica y como tal desde épocas anteriores ya se iniciaban a contextualizar estos conceptos.

Como cita Borghello (2001), *"los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, Cesar"* (p.2) han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Como todo concepto, la seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

Según Borghello (2001), *"La primera evidencia de una cultura y organización en seguridad madura aparece en los documentos de la República (estado) de Roma imperial y republicana"* (p. 2). Además, indica que:

El próximo paso de la seguridad fue la especialización. Así nace la seguridad externa (aquella que se preocupa por la amenaza de entes externos hacia la organización) y la seguridad interna (aquella preocupada por las amenazas de nuestra organización con la organización misma) (p. 3).

Desde el punto de vista técnico, la seguridad es un tema considerado integral en toda la empresa, que se contempla de forma holística lo que implica que la alta dirección esté anuente a participar en la gestión de la seguridad, además en cada uno de los usuarios y en el grado de concientización respecto a la importancia de la información y el conocimiento, que se maneja y al que se tiene acceso.

2.3. ¿Qué es la seguridad de la información?

La información es uno de los activos más importantes y esenciales en una organización, imprescindible para la toma de decisiones y en consecuencia necesita ser protegida adecuadamente.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar protegida de forma adecuada.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio y el cumplimiento de las obligaciones legales, minimizar los riesgos asociados a una vulnerabilidad, especialmente en cuanto a los datos personales almacenados en las bases de datos, lo que se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware; para ello se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumpla con los objetivos que permitan mitigar la materialización del riesgo.

2.3.1. Resguardo de la información

El resguardo de información es proteger la información de las computadoras y respaldarla en caso de una falla. Hacer una copia de seguridad o copia de respaldo se refiere a la copia de datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información, ya sea por un virus, accidentes en los equipos, fallo y/o daños en los discos duros, o eliminación accidental de la información.

2.3.2. Respaldo de la información

El respaldo de la información es a partir de la obtención de una copia de los datos en otro medio diferente al que fueron creados, de tal modo que a partir de la copia sea posible restaurar el sistema al momento de haber realizado el respaldo. Por lo tanto, los respaldos deben hacerse con regularidad, con la frecuencia preestablecida y de la manera indicada, a efectos de hacerlos correctamente, principalmente utilizando las políticas y/o procedimientos de la entidad referentes al Respaldo de la Información que a su vez van a estar referenciados en alguna buena práctica para la gestión de tecnologías de la información. Estos respaldos también deben de contar con la seguridad necesaria para que no puedan ser utilizados por personas no autorizadas.

2.3.3. Recuperación de la información

La recuperación de la información es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo. A partir de los datos de la última copia realizada, se hace una copia en sentido nuevo, recuperando la aplicación.

La recuperación es una tarea eventual. Solo se hace si se han perdido datos, en magnitud tal que justifique utilizar el respaldo. Puede hacerse en forma parcial por ejemplo solo un archivo o de forma completa. Si se hace una recuperación parcial, debe asegurarse que no se altere la integridad de los datos.

2.4. Objetivo de la seguridad informática

Para comenzar el análisis de la Seguridad Informática se deberán conocer las características con las que se pretende proteger la Información.

2.4.1. Datos

Son los almacenados en un computador. Se puede constituir en un activo cualitativo de una organización y se deben salvaguardar, pues a través del procesamiento de los datos se obtiene información que sirve de base para la toma de decisiones.

Algunos mecanismos contribuyentes a la protección de los datos son los controles que se establecen previos al registro de esos datos, dentro del computador empleado para el procesamiento, durante su proceso de transformación y posterior a este.

2.4.2. Información

En términos generales, se habla de información como un conjunto de datos que están organizados y que tienen un significado. La información es un elemento fundamental en el proceso de la comunicación, ya que tiene un significado para quien la recibe, que la va a comprender si comparte el mismo código que quien la envía. Esto no sólo ocurre en un proceso social sino también en el mundo de la informática.

Existe información que debe o puede ser pública y otra que debe ser privada y es por estas razones que es necesario maximizar los esfuerzos para preservarla de ese modo, reconociendo los siguientes aspectos importantes en la Información:

- Es crítica: es indispensable para garantizar la continuidad operativa.
- Es valiosa: es un activo con valor en sí misma.

- Es sensible: debe ser conocida por las personas que la procesan y sólo por ellas.

También resulta necesario considerar los siguientes aspectos que la identifican y le generan el valor y la importancia que tiene.

- **La integridad de la información:** consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

- **La disponibilidad u operatividad de la información:** el objetivo de la disponibilidad es garantizar el acceso a un servicio y/o recurso.

- **La privacidad o confidencialidad de la información:** consiste en hacer que la información sea inaccesible para aquellos individuos que no estén involucrados en la operación.

- **El control sobre la información:** garantizar el acceso a recursos únicamente a las personas autorizadas.

- **La autenticidad de la información:** es el acto de establecimiento o confirmación de algo (o alguien) como auténtico.

2.4.3. Riesgo

Riesgo es la combinación de la probabilidad de un evento y sus consecuencias. Los riesgos del negocio pueden tener un impacto negativo sobre los activos, procesos u objetivos de un negocio u organización específicos.

2.4.4. Daño

Es el resultado causado por la amenaza.

2.4.5. Amenazas

Representa el tipo de acción que tiende a ser dañina y podría comprometer un sistema y/o servicio.

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operación de una entidad. Las amenazas pueden ser de carácter físico o lógico, como una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema y/o base de datos.

- La Prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo, el cifrado de información para su posterior transmisión.

- La Detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

- La Recuperación (después): mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo, recuperación desde las copias de seguridad (backup) realizadas.

2.4.6. Vulnerabilidades

Son ciertas condiciones inherentes a los activos o presentes en un entorno Informático que facilitan que las amenazas se materialicen y llevan a esos activos a ser vulnerables.

Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

2.4.7. Contramedidas (técnicas de protección) adecuadas.

La Seguridad indicará el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo.

Luego para garantizar que un sistema este seguro e íntegro, se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer “qué es lo que queremos proteger”, “de quién lo queremos proteger”, “cómo se puede lograr esto legislativa y técnicamente”; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución (¿anulación?) de los riesgos.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades y Amenazas con el propósito de implementar controles y contramedidas; evaluar las ventajas o desventajas de la situación; para con esto tener en cuenta el nivel de seguridad que se tiene, el esperado y el deseable. Además, se debería tratar de disminuir cualquier circunstancia negativa que intente minimizar la operación normal de un sistema, equipo o centro de cómputo.

2.5 Por qué es importante proteger sistemas, equipos y bases de datos?

Porque existen Intrusos o Atacantes que acceden (o intentan acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

2.5.1. ¿Qué se debería proteger?

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos.

- Hardware: corresponde a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

- Software: es equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

- Datos: se pueden mencionar los siguientes:

    - Datos personales: cualquier dato relativo a una persona física identificada o identificable.
    - Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.
    - Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.
    - Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.
    - Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

2.6 Seguridad física

Consiste en la implementación de barreras físicas, controles lógicos y administrativos que contemplen procedimientos de control, como medidas de prevención ante amenazas a las bases de datos y su información. Las exposiciones físicas podrían tener como consecuencia perdida financiera, repercusiones legales, la pérdida de la credibilidad o la perdida de la ventaja competitiva. Las mismas se originan principalmente en peligros naturales y artificiales y pueden exponer el

negocio a accesos no autorizados y falta de disponibilidad de la información del negocio.

2.6.1 Objetivo de la seguridad física

Es evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

2.7 Elementos claves para la gestión de seguridad de la información

2.7.1 Políticas y procedimientos

Se debe establecer el marco de una política proporcionando una declaración concisa de directivas de la alta gerencia que trata el valor de los activos de información, la necesidad de seguridad y la importancia de definir una jerarquía de clases de activos confidenciales y críticos. Seguidamente de contar con una política aprobada, desarrollar los siguientes documentos:

- Estándares para desarrollar niveles de seguridad mínimos
- Criterios y métodos de medición
- Directrices, prácticas y procedimientos específicos

La política debe asegurar que se cumplan las leyes y regulaciones. Las políticas y procedimientos de seguridad deben estar actualizados y deben reflejar los objetivos del negocio, los estándares y las prácticas de seguridad generalmente aceptados.

2.7.2 Adecuada concientización y formación en toda la entidad

Todos los empleados de una entidad y, cuando corresponda, los usuarios externos, deben recibir capacitación apropiada y actualizaciones periódicas para promover la concienciación y el cumplimiento de las políticas y los procedimientos de seguridad que están por escrito. Para los nuevos empleados, esta capacitación debe ocurrir antes de que se le otorgue acceso a la información, bases de datos y/o a los servicios. Los diferentes mecanismos disponibles para elevar la concienciación de seguridad incluyen los siguientes:

- Actualizaciones periódicas escritas de las políticas y procedimientos de seguridad que están por escrito
- Capacitación formal sobre seguridad de la información
- Programa interno de certificación para el personal relevante
- Declaraciones firmadas por los empleados comprometiéndose a acatar la política y los procedimientos de seguridad documentados, incluyendo la obligación de no divulgación.
- Uso de diferentes medios para la distribución de material relacionado con la seguridad (por ejemplo, boletín de noticias de la compañía, pagina web, videos, etc.)
- Cumplimiento visible de las reglas sobre seguridad y auditorías periódicas
- Ejercicios e incidentes simulados de seguridad

2.7.3 Tratamiento y respuesta de incidentes

Un incidente de seguridad de computadoras es un evento que afecta adversamente el procesamiento del uso de computadoras. Esto incluye pérdida de confidencialidad de la información, causar inestabilidad de la integridad de la información, negación de servicio, acceso no autorizado a los sistemas, mal uso de los sistemas de información, robo y daño a los sistemas. Otros incidentes incluyen ataques de virus e intrusiones por personas dentro o fuera de la empresa.

2.8 Seguridad lógica

La seguridad lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a personas autorizadas para hacerlo." (p. 11).

Según Borgghello (2001) los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.9 Algunas consideraciones sobre protección de datos personales y delitos informáticos

2.9.1. Generalidades

La sección de delitos informáticos del Organismo de Investigación Judiciales (OIJ) es la encargada de realizar las investigaciones tanto de delitos informáticos

como de otros delitos donde la informática es parte de la comisión del delito o sirve como prueba para comprobar quién realizó un acto delictivo. Fue creada en 1997, por la necesidad de procesar información contenida en computadoras y servidores decomisados en casos importantes. Se realizan investigaciones de delitos informáticos y de otros delitos donde la informática es utilizada para el acto delictivo o como medio de prueba.

En el 2004 se constituye como Sección de Delitos Informáticos. Se utilizan técnicas de Computación Forense en la recolección, preservación y análisis de indicios para garantizar la cadena de custodia de los indicios en computadoras, discos duros, llaves USB, dispositivos móviles, entre otros dispositivos de procesamiento y almacenamiento de datos. (Poder Judicial, 2017).

2.9.2 Legislación costarricense

En lo que respecta a legislación en esta área, a continuación, se enlista lo que en la actualidad se encuentra en vigencia.

- **Constitución Política de la República de Costa Rica**

Artículo 23. - “"El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante, pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley”."

Artículo 24. - “"Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.

Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados

de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos.

Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.

No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación. (Constitución Política, 2017).

(Así reformado por el artículo 1° de la ley N° 7607 de 29 de mayo de 1996)".

- **Directriz 046-H-MICITT – La Presidenta de la República y los Ministros de Hacienda y el de Ciencia, Tecnología y telecomunicaciones.**

Artículo 1. A partir de esta publicación de esta directriz las instituciones del sector público privilegiarán, cuando sea posible y conveniente, la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura. Esto aplica para equipos, licencias y sistemas informáticos, servidores de hospedaje de páginas web, servidores de aplicaciones, correo electrónico, muros de fuego, sistemas operativos, sistemas ofimáticos, bases de datos u otras tecnologías informáticas ya sea para el usuario final o para el centro de datos en sí, o cualquier otro tipo de desarrollo tecnológico. Se busca con esta directriz facilitar el acceso a plataformas tecnológicas en concordancia con los planes de modernización del Estado y garantizar su disponibilidad independientemente de ubicación física, respetando criterios de uso racional de recursos públicos.

Artículo 8. La información que se capture en los instrumentos que se implementen y en cumplimiento de esta directriz, no deberá incluir detalles que pudieran comprometer la seguridad de la información y de la infraestructura tecnológica de las instituciones relacionadas. Asimismo, no debe arriesgar o comprometer información confidencial de los particulares a la que tuviera acceso la institución que se trate.

Dada en la Presidencia de la Republica, a los nueve días del mes de abril del año dos mil trece.

- **Legislación sobre delitos informáticos en Costa Rica**

Código Penal de Costa Rica

Artículo 196. Violación de correspondencia o comunicaciones.

Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona.

La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.
La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.
La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este articulo son realizadas por:
a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.
b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 196 bis. Violación de datos personales.

Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.
La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:
a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
b) La información vulnerada corresponda a un menor de edad o incapaz.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la SUGEF (Superintendencia General de Entidades Financieras) de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley.

Artículo 217 bis. Estafa informática.

Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 229 bis. Daño informático.

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.
La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Artículo 229 ter Sabotaje informático.

Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

Artículo 230. Suplantación de identidad.

Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.

Artículo 231. Espionaje informático.

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

Artículo 232. Instalación o propagación de programas informáticos maliciosos.

Será sancionado con prisión de uno a seis años quien, sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.
b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.
c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.
d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.
e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.
La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.

ii) Afecte el funcionamiento de servicios públicos.

iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.

iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

Artículo 233. Suplantación de páginas electrónicas.

Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Artículo 234. Facilitación del delito informático.

Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

Artículo 236. Difusión de información falsa

Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

- **Ley General de Aduanas**

CAPITULO II

DELITOS INFORMATICOS

ARTÍCULO 221.- Delitos informáticos

Será reprimido con prisión de uno a tres años quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.

d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

ARTÍCULO 222.- Agravante

La pena será de tres a cinco años cuando, en alguna de las causales del artículo anterior, concurra una de las siguientes circunstancias:

a) Intervengan en el hecho tres o más personas, en calidad de autoras.

b) Intervenga, en calidad de autor, instigador o cómplice, un funcionario público en ejercicio de sus funciones, con ocasión de ellas o con abuso de su cargo. (Ministerio de Hacienda., 2017)

- **Ley de protección de la persona frente al tratamiento de sus datos personales**

La ley 8968, fue publicada en el diario oficial La Gaceta número 170, del 5 de setiembre del 2011.

ARTÍCULO 1.- Objetivo y fin

Esta ley es de orden público y tiene como objetivo garantizara cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. (p. 2)

ARTÍCULO 2.- Ámbito de aplicación

Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.
El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas. (p. 2)

- **Estándares Iberoamericanos**

Los estándares de protección de datos personales para los estados iberoamericanos fueron publicados en junio del 2017 y tiene como objeto:

a. Establecer un conjunto de principios y derechos de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.

b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como entre los Estados Iberoamericanos, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

c. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

d. Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento social y económico de la región. e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.

Capítulo 3. Marco metodológico

El proyecto incluye componentes de investigación los que requieren una base formal para constituir la herramienta y dejar claro el enfoque investigativo utilizado. Esta base incluye describir el tipo de investigación realizado, el diseño y el alcance del proyecto. También se detalla la población involucrada, así como los instrumentos de recolección de datos y las estrategias de desarrollo.

3.1 Tipo de investigación

Investigar es conocer, transformar la tradición y el rutinario quehacer hacia nuevas visiones de mundo contextualmente realistas.

El tipo de investigación en este proyecto es investigación aplicada; según artículo de Vargas Cordero (2009) recibe el nombre de “investigación práctica o empírica”, que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. Es el uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad, tal como lo define Padrón (citado en Vargas Cordero, 2009) haciendo dos distinciones:

a. La que incluye cualquier esfuerzo sistemático y socializado por resolver problemas o intervenir situaciones. En ese sentido, se concibe como investigación aplicada tanto la innovación técnica, artesanal e industrial como la propiamente científica.
b. La que sólo considera los estudios que explotan teorías científicas previamente validadas, para la solución de problemas prácticos y el control de situaciones de la vida cotidiana.

En este proyecto el problema se establece en la falta de una guía de auditoría para verificar la seguridad de la información en las bases de datos que deben ser reguladas, guía que a su vez se convierte en un modelo específico para realizar

auditorías y/o inspecciones de oficio en un entorno dentro de protección de datos personales, en donde sus características particulares dificultan la aplicación de modelos construidos con un enfoque empresarial de seguridad de la información.

En este contexto y a partir de casos particulares de estudio obtenidos de las fuentes primarias, investigación sobre metodologías de auditoría aplicados en otros campos y trabajos teóricos sobre generación de guías de sobre protección de datos, el producto final será un instrumento/guía que permita colaborar con la Unidad de Auditoría, para realizar auditorías y/o inspecciones de oficio, con bases sólidas que permitan validar y revisar la seguridad de la información en la infraestructura y/o bases de datos que contienen datos personales de costarricenses.

3.2 Alcance investigativo

El alcance investigativo de este proyecto es de carácter exploratorio. La investigación exploratoria se efectúa sobre un tema poco estudiado, en donde los alcances se limitan a la observación y al registro objetivo de lo encontrado (Barrantes, 1999, p. 131). Este proyecto considera las fuentes primarias, los casos aplicados de guías de auditoría y los estudios teóricos sobre auditoría y protección de datos para crear una herramienta que permita auditar cualquier institución pública o privada que realice tratamiento de datos personales en Costa Rica.

Por otra parte, y de acuerdo con lo establecido en el tipo de investigación, se propone una solución aplicada, en donde los modelos observados y documentados, serán utilizados para generar una guía de auditoría con las características específicas requeridas para la PRODHAB.

3.3 Enfoque

El enfoque de la investigación será mixto, cualitativo y cuantitativo. Cuantitativo porque según Hernandez Sampieri (2014) consiste “en utilizar la recolección y el análisis de datos para contestar preguntas de investigación y probar

hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población". Pero también cualitativo porque según Hernandez Sampieri "consiste en utilizar la recolección de datos sin medición numérica para descubrir o afinar preguntar de investigación en el proceso de interpretación".

3.4 Diseño

El diseño de la investigación define las estrategias básicas para generar información confiable e interpretable (Bautista, 2011, p. 150). La investigación-acción permite el diagnóstico de problemáticas sociales, políticas, laborales, económicas, etc., de naturaleza colectiva. Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones, algunas de sus características según Hernandez Sampieri "Cuando una problemática de una comunidad necesita resolverse y se pretende lograr el cambio." (2014, p. 471) y además es relevante mencionar que las personas tomen conciencia de su papel en ese proceso de transformación. Por ello, implica la total colaboración de los participantes en: la detección de necesidades, el involucramiento con la estructura a modificar, el proceso a mejorar.

Las estrategias estarán dirigidas a resolver un problema puntual, en este caso, generar una guía de auditoría de seguridad de la información enfocada a la protección de datos que además contenga con las características específicas requeridas para la PRODHAB.

3.6 Instrumentos de Recolección de Datos

Para efectos de esta investigación se utilizaron diversos medios, físicos y lógicos, mediante la revisión de la documentación de políticas y procedimientos existentes, así como el uso de entrevistas para recopilar los datos, además se cuenta con conocimiento del negocio y su estrategia para asegurar el desarrollo del mismo.

3.7 Técnicas de análisis de la información

La gestión de problemas apunta a resolver problemas a través de la investigación y un análisis en profundidad de incidentes. Una de las metodologías estándar es realizar un diagrama Ishikawa (o diagrama de causa-efecto) a través de una tormenta de ideas de las partes afectadas. Ya que en este caso conocemos a profundidad el problema, la condición se convierte en un "error conocido". Entonces se puede desarrollar un proceso para resolver el problema en cuestión.

El diagrama de Ishikawa, conocido también como causa-efecto o diagrama de espina de pez, es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema. Permite, por tanto, representar gráficamente el conjunto de causas que dan lugar a una consecuencia o bien el conjunto de factores y sub-factores (en las “espinas”) que contribuyen a generar un efecto común (en la “cabeza” del diagrama).

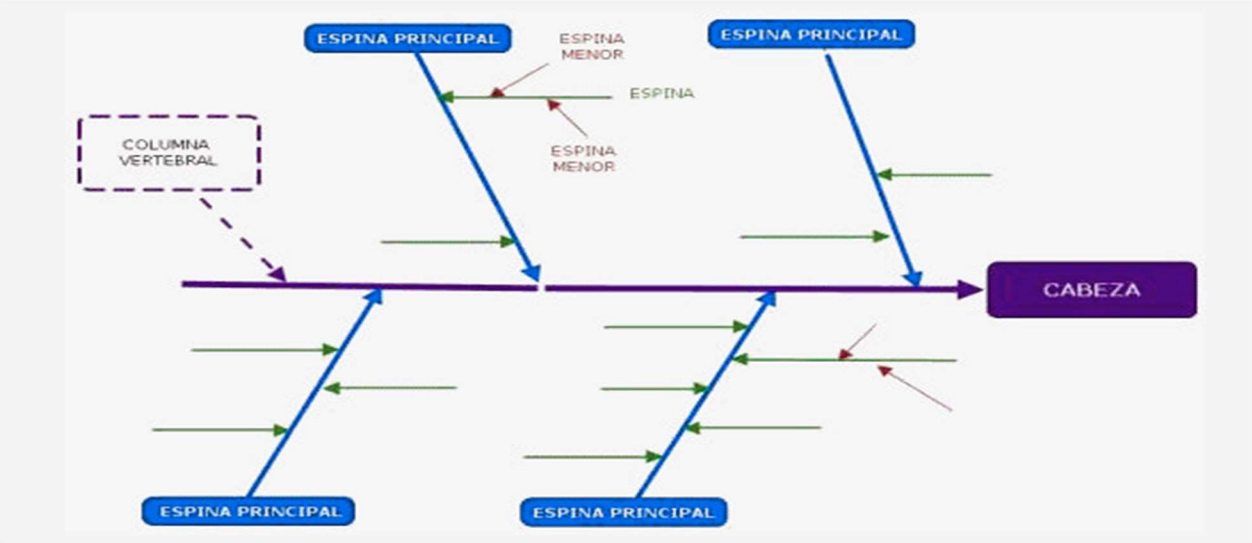


Figura 2. ***Diagrama de Ishikawa: Análisis causa-efecto de los problemas***

Fuente: http://www.pdcahome.com/diagrama-de-ishikawa-2

Capítulo 4. Desarrollo de la solución

El presente proyecto consistió en analizar, diseñar y proponer una guía para la revisión de la seguridad de la información de las bases de datos que deben ser reguladas por la Agencia de Protección de Datos de los Habitantes con un alcance de instituciones públicas y privadas y que además facilite el proceso de realizar inspecciones de oficio y/o auditorías.

La solución consistió en la creación de los siguientes documentos que permiten la elaboración sistemática de la propuesta, ya que desarrolla las fases y/o pasos para completar el proceso que colabore con las inspecciones de oficio y/o auditorías, estos documentos se encuentran en los anexos de este proyecto:

1. *Anexo #1.* Documento sobre las **Normas Generales de Inspecciones de Oficio/Auditorías** porque era necesario crear el marco normativo de las inspecciones de oficio y/o auditorías de las bases de datos con datos personales, en el sector público y privado, documento donde se describe la autoridad y razonabilidad de las futuras inspecciones/auditorías; también se

definen las normas generales al trabajo de inspección/auditoría; finalmente la descripción de las fases y/o pasos a seguir para realizar las inspecciones de oficio/auditorías.

2. *Anexo #2.* Documento denominado **Descripción General de la Auditoría,** define objetivo general, objetivos específicos, efectos, justificación, institución auditada, alcance, asignación de roles, asignación de horas, fechas de realización y un cronograma que divide las etapas de la inspección de oficio/auditoría y que debe ser elaborado por el auditor de la PRODHAB, revisado por la jefatura de Auditoría. Sin embargo, si no ha sido creada la Unidad de Auditoría será revisado por la jefatura de TI.

3. *Anexo #3.* Denominado **Planificación de la Auditoría**, define el objetivo general, objetivos específicos, objetivos de la actividad, asuntos objetivos del estudio, periodo del estudio, normativa aplicable para la auditoría y sus respectivos criterios tomando en cuenta cada norma y pasos a seguir para el procedimiento de auditoría a aplicar, fuentes de información, recursos requeridos. Debe ser elaborado por el auditor de la PRODHAB, revisado por la jefatura de Auditoría y si no ha sido creada la Unidad de Auditoría será revisado por la jefatura de TI.

4. *Anexo #4. Do*cumento designado para la **Ejecución de la Auditoría**, define el objetivo general, objetivos específicos, objetivos de la actividad, asuntos objetivos del estudio, periodo del estudio, normativa aplicable para la auditoría, y sus respectivos criterios tomando en cuenta cada norma, donde se especifica qué documentos se van a solicitar, es decir, este documento hace referencia a los requerimientos de evidencia solicitados a la entidad auditada, además de la revisión de software de la base de datos y documentación, incluye fuentes de información, recursos requeridos. Debe ser elaborado por el auditor de la PRODHAB, revisado por la jefatura de Auditoría y si no ha sido creada la Unidad de Auditoría será revisado por la jefatura de TI.

5. *Anexo #5. Do*cumento designado para documentar el **Informe de la Inspección/Auditoría**. Luego de realizados los pasos de la auditoría es necesario generar un documento donde se indique lo que se examinó, los hallazgos, responsables y recomendaciones acorde la Ley 8968 y las normas utilizadas. Incluye descripción del origen, objetivo, alcance, aspectos positivos que favorecieron la inspección/auditoría, generalidades, metodología aplicada, observaciones, conclusiones y disposiciones. debe ser elaborado por el auditor de la PRODHAB, revisado por la jefatura de Auditoría y si no ha sido creada la Unidad de Auditoría será revisado por la jefatura de TI.

Capítulo 5. Conclusiones

- La documentación que tiene la PRODHAB como parte de sus controles administrativos no ha contemplado las inspecciones de oficio y/o auditorías, además no cuenta con una Unidad y/o Departamento de Auditoría, ni con un procedimiento que facilite la posibilidad de realizar inspecciones y/o auditoría.
- Es importante que exista un mayor compromiso por parte de la Dirección Nacional para crear la Unidad y/o Departamento de Auditoría y además involucrar a los colaboradores que tengan habilidades para coadyuvar con la realización de las inspecciones/auditorías.
- Existen profesionales capaces y con conocimientos en el área de seguridad informática y auditoría de los sistemas de información, que pueden participar y generar recomendaciones, además de utilizar los documentos creados en este proyecto.

- El producto de esta investigación pretende constituirse en una herramienta estratégica, que permita la realización de inspecciones de oficio y/o

auditorías colaborando con la madurez de esta área, permitiendo el desarrollo de mejores prácticas, en el ámbito de auditoría para la futura Unidad y/o Departamento de Auditoría, se determinaron las especificaciones de seguridad de la información establecidas en la Ley 8968.

- Se investigó sobre buenas prácticas de gestión de Tecnologías de Información, que complementan el cumplimiento de la Ley 8968 en materia de seguridad de la información y de protección de datos.

- Se construyó una Normativa y formularios que funcionarán como protocolos que permitan auditar y verificar el cumplimiento en cuanto a la seguridad de la información y protección de datos de las bases de datos reguladas por la Ley 8968.

- Las estrategias y buenas prácticas utilizadas en este proyecto y que se pretenden implementar y utilizar en la Unidad de Auditoría serán efectivas si se adopta el proyecto como respuesta a la necesidad de cumplir con los objetivos estratégicos, y atribuciones de la PRODHAB.

- El proyecto contó con los recursos necesarios para su desarrollo e implementación, en el aspecto económico tuvo el apoyo de la Dirección Nacional con la asignación de horas para el desarrollo del mismo, pero además cabe destacar la colaboración de los colaboradores de la Unidad Legal y de Tecnologías de la Información para aclarar dudas, reuniones y aportar información valiosa en cualquier momento durante los meses del desarrollo del mismo.

Capítulo 6. Recomendaciones

- Es necesario que se analice la posibilidad de aprobar las herramientas elaboradas en este proyecto por parte de la Dirección Nacional, porque es insumo fundamental para cumplir con la atribución establecida en la Ley 8968 sobre realizar inspecciones de oficio a nivel nacional.

- La institución cuenta con profesionales titulados y capacitados en auditoría de la información, seguridad de la información, riesgos de tecnologías de la información en la Unidad de Tecnologías de Información, que serían de valiosa colaboración si se involucraran generando recomendaciones para las herramientas creadas durante este proyecto y generen experiencias académicas y operacionales, que permitan un nivel de seguridad mejor en el acceso y utilización de los equipos computacionales.

- Se debe revisar, aprobar y aplicar la Norma creada durante este proyecto, acorde a las buenas prácticas internacionales de gestión de tecnologías de la información, esta Norma debe actualizarse al menos una vez al año y es el documento que se debe de compartir con las instituciones que serán auditadas. El documento debe ser publicado en el diario oficial La Gaceta, para brindar garantía jurídica. Debe ser utilizado por los profesionales de PRODHAB quienes participen en la inspección y/o auditoría y debe ser conocido por las entidades auditadas.

- Tanto los colaboradores de la Unidad de Tecnologías de la Información, como los colaboradores de la futura Unidad de Auditoría deberían informarse, investigar y profundizar los conocimientos en esta área, como parte de su desarrollo profesional y personal porque a diario se dan a conocer nuevas técnicas, métodos y estrategias que se utilizan para vulnerar equipos, produciendo amenazas y/o riesgos a los lugares donde utilicen equipos computacionales y de esta forma poder enriquecer las herramientas creadas en este proyecto, fundamentalmente ampliando la percepción y alcance

cuando se necesite evaluar una base de datos y verificar si cumple con adecuados controles que garanticen la protección de datos y la seguridad, para complementar la investigación sobre las actuales buenas prácticas de gestión de Tecnologías de Información plasmadas en las herramientas creadas.

- El tema de la protección de datos personales se debería exponer y presentar en cualquier entidad a nivel de Costa Rica porque en la actualidad y a nivel mundial ya es catalogado como una problemática de carácter social, que se acrecienta con el paso del tiempo y a un ritmo acelerado.
- Ejecutar una auditoría piloto para validar los formularios y el procedimiento utilizando como muestra las bases de datos de bajo riesgo.

Capítulo 7. Reflexiones finales

Hoy en día las organizaciones tienen un porcentaje alto de dependencia de la tecnología, para procesar su información, almacenarla, enviarla a través de la red, por ende, desde el acopio de la información, su almacenamiento y eliminación debe garantizar un adecuado tratamiento de los datos personales, cuando en sus procesos y/o sistemas utilizan datos personales como parte de sus productos y/o servicios.

El pasado 25 de mayo 2018 se publicó el nuevo Reglamento General de Protección de Datos de la Agencia Española que afecta a todos los países y ciudadanos del mundo, es bastante extenso en cuanto al derecho de las personas a saber quién, cómo y por qué se están utilizando o almacenando sus datos y establece criterios sobre los casos en los que se puede exigir borrar o transferir esos datos, suspender su tratamiento o rectificarlos si son incorrectos. Los Estados miembros del Parlamento Europeo tienen que adecuarse y también el sector público y las empresas.

Las repercusiones son de alcance a nivel mundial, además prevé un riguroso régimen sancionatorio ante las infracciones, dependiendo de las multas administrativas se podría alcanzar el 4% de la facturación anual de la compañía, reconoce el derecho a la indemnización a las víctimas por daños y perjuicios y la protección de datos se está volviendo parte de los acuerdos comerciales de las empresas. Por ejemplo, empresas como Facebook y Google invirtieron recursos para revisar y actualizar las políticas y configuraciones de privacidad.

Por lo anterior, estamos frente a una regulación compleja y de mucha relevancia para Costa Rica y un reto para la PRODHAB. En cuanto al nivel legislativo debe actualizarse la Ley y el Reglamento 8968 y a la vez el nuevo Reglamento Europeo que exige mejores controles y mayores responsabilidades asociadas a la protección de datos personales, por lo que las herramientas elaboradas en este proyecto son de vital importancia para las revisiones futuras de bases de datos, recomendaciones de seguridad y colaborar con la madurez de los procesos realizados en la PRODHAB.

Capítulo 8. Trabajos a futuro

La PRODHAB está realizando de momento un importante trabajo de concienciación sobre la Ley y el Reglamento de Protección de Datos personales, al menos 2 veces por semana se dan charlas sobre la Ley y el Reglamento, por otro lado, a nivel de Costa Rica hay un alto porcentaje de la población que desconoce la existencia y alcance de la PRODHAB. Además, existe poco personal que debe de abarcar todos los procesos operativos de la PRODHAB que a su vez atender a todo el país.

Parte de los retos que tiene la PRODHAB actualmente es realizar inspecciones de oficio y/o auditorías a las bases de datos que contengan información sobre datos personales, sin ser relevante si esa base de datos está inscrita o no ante la PRODHAB y si pertenece al sector público o privado; actualmente solo se cuentan con 90 bases de datos inscritas, por lo que podemos

prever que existe una gran cantidad de bases de datos que aún no han sido inscritas y que existen empresas responsables que aún no conocen sobre la Ley el Reglamento y los criterios establecidos para cumplir con la misma y desconoce por completo que la PRODHAB tiene la atribución de ir a revisar la base de datos, controles administrativos, físicos y lógicos, además de un protocolo mínimo de actuación indicado en el Reglamento de la Ley 8968.

Se espera que la PRODHAB adopte los documentos creados en este proyecto como parte de sus controles administrativos y que sirvan de base para iniciar con las inspecciones de oficio y/o auditorías y ser pioneros en este tipo de investigaciones que buscan garantizar una adecuada protección de los datos personales de los ciudadanos de Costa Rica.

Referencias Bibliográficas

Barrantes, R. (1999). Investigación: un camino al conocimiento, un enfoque cualitativo y cuantitativo. San José, Costa Rica: EUNED.

Bautista, N. (2011). Proceso de la investigación cualitativa: epistemología, metodología y aplicaciones. Bogotá: Manual Moderno.

Borghello, Cristian. (2001) Seguridad Informática - Implicancias e Implementación. Recopilado el martes 21 de noviembre del 2017 de, http://www.segu-info.com.ar/tesis/

La gaceta N93. (2013). Directriz N 46-H-MICITT.Directriz. Recuperado el 27 de noviembre del 2017, URL: http://www.digeca.go.cr/sites/default/files/directriz_46-h-micitt-la_gaceta_93-16_mayo_2013_tecnologias_de_informacion.pdf

Ministerio de Hacienda. (2017). Ley General de Aduanas. Disposiciones Generales. Recuperado el 11 de diciembre del 2017, URL: http://www.hacienda.go.cr/docs/51c9baa1b805f_LEYGENERALDEADUANASACTUALIZADAAOCTUBRE2012.pdf

Poder Judicial. (2017). Departamento de Investigaciones Criminales. Sección de delitos informáticos. Recuperado el 11 de diciembre del 2017, URL: https://www.poder-judicial.go.cr/oij/index.php/ofi/departamento-de-investigaciones-criminales/delitos-informaticos

PRODHAB. (2017). ¿Quiénes Somos?. Agencia de Protección de datos de los Habitantes. Recuperado el 26 de octubre del 2017, URL: http://prodhab.go.cr/quienesomos/

PRODHAB. (2017). Misión y Visión. Agencia de Protección de datos de los Habitantes. Recuperado el 27 de octubre del 2017, URL: http://prodhab.go.cr/mision/

Red Iberoamericana de Protección de Datos. (2017). Documentos Generales. Estándares de protección de datos personales para los estados Iberoamericanos. Recuperado el 27 de noviembre del 2017, URL: http://www.redipd.es/documentacion/index-ides-idphp.php

Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio, Metodología de la Investigación, 6ta Edición, México D.F, 2014.

SCIJ. (2011). Ley 8968 Protección de la Persona frente al tratamiento de sus datos personales. Recuperado el 26 de octubre del 2017, URL: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=70975&nValor3=85989&strTipM=FN

SCIJ. (2017). Sistema Costarricense de Información Jurídica. Código Penal. Recuperado el 12 de diciembre del 2017, URL: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=108691&strTipM=TC}

SCIJ. (2017). Sistema Costarricense de Información Jurídica. Constitución Política. Recuperado el 11 de diciembre del 2017, URL: http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=871&strTipM=TC

Universidad de Costa Rica. (2017). Normas técnicas para la gestión y el control de las Tecnologías de Información. Recuperado el 28 de octubre del 2017, URL: http://ocu.ucr.ac.cr/images/ArchivosOCU/CapacitacionRIDS/N-2-2007-CO-DFOENormasGestionControlTI-CGR.pdf

Vargas Cordero, Z. (2009). La Investigación aplicada: Una forma de conocer las realidades con evidencia científica. Rev. Educación, 33(1), 155-165.

Contraloría General de la República. (2014). Normas Generales de Auditoría para el Sector Público. Recuperado el 15 de enero del 2018, URL:

http://ocu.ucr.ac.cr/images/ArchivosOCU/Normativa/NormativaExterna/NormasGeneralesAuditoriaSectorPublico.pdf

ANEXOS

Anexo 1. Normas Generales de Inspecciones de Oficio/ Auditorías

Normas Generales de Inspecciones de Oficio /Auditorías

Agencia de Protección de Datos de los Habitantes

UNIDAD DE TECNOLOGIAS DE INFORMACIÓN

PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

CONSIDERANDO

1º— Que la PRODHAB fue creada mediante la Ley N° 8968 del 7 de julio del 2011, publicada en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011, órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz.

2º— Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.

Por tanto,

RESUELVE

Artículo 1°—Aprobar y promulgar el documento denominado “Normas Generales de Inspecciones de Oficio/auditorías” con la siguiente estructura:

Presentación

Introducción

Capítulo I. Normas Personales

1. Independencia y objetividad
2. Naturaleza confidencial y discreción sobre el trabajo
3. Ética Profesional
4. Competencia y pericia profesional
5. Debido cuidado profesional
6. Educación profesional continua

Capitulo II. Normas generales relativas al trabajo de inspección/auditoría en el sector público y privado

1. Administracion de la inspección/auditoría
2. Actividades del proceso de inspección/auditoría
3. Planificación
4. Examen
5. Comunicación de resultados

6. Seguimiento
7. Evidencia de inspección/auditoría
8. Documentación de la inspección/auditoría
9. Archivo permanente

Capítulo III. Normas generales sobre inspección/auditoría de cumplimiento

1. Planificación
2. Criterios de inspección/auditoría
3. Evidencia
4. Comunicación de resultados

Glosario

Artículo 2°_ Las “Normas Generales de Inspecciones de Oficio/auditorías”, serán aplicables para la Agencia de Protección de Datos de los Habitantes, las inspecciones/auditorías internas del sector público/privado, y los profesionales autorizados —de forma unipersonal u organizados por medio de despachos o firmas de inspección/auditoría— cuando actúan en labores de inspección/auditoría en el sector público y privado.

Artículo 3°— Las “Normas Generales de Inspecciones de Oficio/auditorías” son de carácter vinculante para los sujetos señalados en el artículo anterior, por lo que estas Normas deberán prevalecer sobre cualquier disposición en contrario que emitan las inspecciones/auditorías internas y la administración activa en su ámbito de aplicación.

Artículo 4°— El incumplimiento de cualquiera de las regulaciones contenidas en las presentes Normas podrá generar la aplicación de los regímenes de responsabilidad establecidos en el ordenamiento jurídico.

Artículo 5°—La Agencia de Protección de Datos de los Habitantes deberá en su sitio oficial en Internet http://www.prodhab.go.cr.

Artículo 6°—Las administraciones deberán diseñar e implantar las medidas y los mecanismos necesarios para poner en práctica lo regulado en esta normativa a partir de su entrada en vigencia.

Artículo 7°—Comunicar que las “Normas Generales de Inspecciones de Oficio/auditorías” entrarán a regir a partir del x de x de x.

Publíquese.

Nombre del Director (a)

DIRECTORA AGENCIA DE PROTECCION DE LOS HABITANTES

Normas Generales de Inspecciones de Oficio/Auditorías

NGIOA

Fecha de publicación en la Gaceta

Contenido

CONSIDERANDO ..... **¡Error! Marcador no definido.**

PRESENTACIÓN ..... **¡Error! Marcador no definido.**

INTRODUCCIÓN ..... **¡Error! Marcador no definido.**

CAPÍTULO I ..... **¡Error! Marcador no definido.**

NORMAS PERSONALES ..... **¡Error! Marcador no definido.**

1. Independencia y objetividad ..... **¡Error! Marcador no definido.**
2. Naturaleza confidencial y discreción sobre el trabajo..... **¡Error! Marcador no definido.**
3. Ética profesional ..... **¡Error! Marcador no definido.**
4. Competencia y pericia profesional..... **¡Error! Marcador no definido.**
5. Debido cuidado profesional ..... **¡Error! Marcador no definido.**

6. Educación profesional continua..... **¡Error! Marcador no definido.**

CAPÍTULO II..... **¡Error! Marcador no definido.**

NORMAS GENERALES RELATIVAS AL TRABAJO DE INSPECCIÓN/AUDITORÍA EN EL SECTOR PÚBLICO/PRIVADO Y PRIVADO..... **¡Error! Marcador no definido.**

1. Administración de la inspección/auditoría ..... **¡Error! Marcador no definido.**
2. Actividades del proceso de inspección/auditoría ..... **¡Error! Marcador no definido.**
3. Planificación ..... **¡Error! Marcador no definido.**
4. Examen ..... **¡Error! Marcador no definido.**
5. Comunicación de resultados ..... **¡Error! Marcador no definido.**
6. Seguimiento..... **¡Error! Marcador no definido.**
7. Evidencia de inspección/auditoría..... **¡Error! Marcador no definido.**
8. Documentación de la inspección/auditoría..... **¡Error! Marcador no definido.**
9. Archivo permanente..... **¡Error! Marcador no definido.**

Capítulo III ..... **¡Error! Marcador no definido.**

NORMAS GENERALES SOBRE INSPECCIÓN/AUDITORÍA DE CUMPLIMIENTO..... **¡Error! Marcador no definido.**

1. Planificación ..... **¡Error! Marcador no definido.**
2. Criterios de inspección/auditoría..... **¡Error! Marcador no definido.**
3. Evidencia..... **¡Error! Marcador no definido.**
4. Comunicación de resultados ..... **¡Error! Marcador no definido.**

Normas Generales de Inspecciones de Oficio/auditorías

PRESENTACIÓN

Necesidad de crear el marco normativo de las inspecciones de oficio y/o auditorías de bases de datos con datos personales, en el sector público y privado

Ante la creación de la Ley 8968 sobre la Protección de la persona frente al tratamiento de sus datos personales y su reglamento, y la respectiva creación de la Agencia de Protección de Datos de los Habitantes, dicha Ley indica sobre la atribución de la PRODHAB de:

a) Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
b) Llevar un registro de las bases de datos reguladas por esta ley.
c) Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados.
d) Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.

e) Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales.
f) Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.
g) Imponer las sanciones establecidas, en el artículo 28 de esta ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito.
h) Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.

i) Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.
j) Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

Resulta necesario que la PRODHAB dicte medidas para realizar el proceso de inspecciones de oficio y/o auditoría en el sector público y privado.
Con fundamento en lo anterior, las presentes Normas establecen una base normativa común y actualizada para el ejercicio de las inspecciones de oficio y/o inspección/auditoría en el sector público y privado costarricense.

Estructura

Las presentes Normas están estructuradas en tres capítulos de normas generales. Los dos primeros capítulos comprenden normas que aplican para todos los tipos de inspección/auditoría que se detallan en este documento, específicamente el primer capítulo agrupa las normas que se refieren a los atributos que deben caracterizar al personal que interviene en el proceso de inspección/auditoría y el segundo comprende las normas relativas al trabajo de inspección/auditoría. El tercer capítulo incorpora las normas de carácter general que son propias para el desarrollo de las inspecciones/auditorías de cumplimiento.

Fuentes normativas de referencia

Para el desarrollo de estas Normas Generales de Inspecciones de Oficio/Auditorías se utilizaron como referencia, principalmente, los marcos normativos internacionales relacionados con la inspección/auditoría y los estándares emitidos por entidades como la ISACA, la ISO (International Organization for Standarization), y la NIST National Institute of Standards and Technology, COBIT5 del ámbito nacional documentación creada por la Contraloría General de la República.

INTRODUCCIÓN

Propósito de las normas

Las presentes “Normas Generales de Inspecciones de Oficio y/o Auditorías” se emiten con el propósito de promover un poner en práctica el proceso de inspecciones de oficio / Auditorías y garantizar un adecuado tratamiento de los datos personales.

Inspección/auditoría en el sector público/privado

La inspección/auditoría en el sector público/privado, según el sujeto que la ejecute, se clasifica en externa e interna. La inspección/auditoría es externa cuando la lleva a cabo la PRODHAB, así como cuando la realizan los entes y órganos de control,

respecto al ámbito externo de su competencia, y los profesionales autorizados que laboran de forma unipersonal u organizados por medio de despachos o firmas de inspección/auditoría. La inspección/auditoría es interna cuando la realizan unidades de inspección/auditoría que pertenecen al ente u órgano que auditan.

Tipos de inspección/auditoría según el sujeto que la realiza

Las inspecciones de oficio/inspección/auditoría es un proceso sistemático, independiente y profesional para obtener y evaluar objetivamente evidencia en relación con hechos y eventos de diversa naturaleza, comprobar su grado de correspondencia con un marco de referencia de criterios aplicables y comunicar los asuntos determinados, así como las conclusiones y disposiciones o recomendaciones a la respectiva Administración/Dirección, con el fin de mejorar la gestión y la toma de decisiones y fortalecer el marco de responsabilidades asociado a la protección de datos personales.

Tipos de inspección/auditoría según sus objetivos

Auditorías de cumplimiento

Las auditorías de cumplimiento incluyen pruebas específicas de los controles para demostrar el cumplimiento de normas regulatorias o de la industria. Estas inspecciones/auditorías a menudo coinciden con las auditorías tradicionales, pero pueden concentrarse en datos o sistemas particulares.

Las inspecciones/auditorías de carácter especial se llevan a cabo para evaluar si las actividades, operaciones financieras e información, cumplen en todos los aspectos relevantes, con las regulaciones o mandatos que rigen a la entidad auditada.

CAPÍTULO I

NORMAS PERSONALES

1. Independencia y objetividad

El personal que ejecuta el proceso de inspección/auditoría en el sector público/privado debe mantener un criterio independiente en el desarrollo de su trabajo, y actuar de manera objetiva, profesional e imparcial.

2. Naturaleza confidencial y discreción sobre el trabajo

Durante la ejecución de la inspección/auditoría los papeles de trabajo son de acceso restringido, por lo que el personal que participa en el proceso de inspección/auditoría en el sector público/privado debe mantener reserva y la discreción debidas respecto de la información obtenida durante el proceso de inspección/auditoría, y no deberá revelarla a terceros, salvo para los efectos de cumplir con requerimientos de las instancias públicas autorizadas legalmente.

3. Ética profesional

La organización de inspección/auditoría debe establecer y poner en práctica principios y valores que orienten la actuación diaria de su personal.

Los participantes en el proceso de inspección/auditoría en el sector público/privado deben observar las normas éticas que rigen su profesión, que se caracterizan por valores como integridad, probidad, objetividad, confidencialidad, imparcialidad, justicia, respeto, transparencia y excelencia, sin perjuicio de otros valores que la organización a la que pertenecen promueva para guiar su actuación.

4. Competencia y pericia profesional

El personal que participa en el proceso de inspección/auditoría en el sector público/privado debe tener formación, conocimientos, destrezas, experiencia, credenciales, aptitudes y otras cualidades y competencias propias del tipo específico de inspección/auditoría a realizar y que lo faculten para el ejercicio de sus funciones.

5. Debido cuidado profesional

El personal que participa en el proceso de inspección/auditoría en el sector público/privado debe ejecutar siempre sus funciones con el debido cuidado, pericia y juicio profesional, con apego a la normativa legal y técnica aplicable y a los procedimientos e instrucciones pertinentes de su organización de inspección/auditoría.

El equipo de inspección/auditoría debe aplicar su juicio profesional para tomar las decisiones de inspección/auditoría, debidamente razonadas y documentadas, durante las distintas actividades del proceso; (planificación, examen, comunicación de resultados y seguimiento), por lo que debe valorar aspectos como el costo beneficio de las acciones, el riesgo de inspección/auditoría, la importancia relativa, la materialidad y la evidencia disponible al momento de tomar la decisión.

El juicio profesional debe ser aplicado a las circunstancias de la inspección/auditoría, de acuerdo con el conocimiento, competencia profesional y experticia de los auditores. La aplicación del juicio profesional debe estar enmarcada dentro de los siguientes parámetros:

a) Ajustarse a la debida diligencia profesional.

b) Alinearse con el ordenamiento jurídico y técnico aplicable.

c) Tener en consideración los objetivos de la inspección/auditoría.

6. Educación profesional continua

El personal de inspección/auditoría debe mantener y perfeccionar sus capacidades y competencias profesionales mediante la participación en programas de educación y capacitación profesional continua.

CAPÍTULO II

NORMAS GENERALES RELATIVAS AL TRABAJO DE INSPECCIÓN/AUDITORÍA EN EL SECTOR PÚBLICO/PRIVADO Y PRIVADO

1. Administración de la inspección/auditoría

La organización de inspección/auditoría debe establecer e implementar políticas y procedimientos para el manejo de la inspección/auditoría.

2. Actividades del proceso de inspección/auditoría

El proceso de inspección/auditoría en el sector público/privado debe comprender las actividades de planificación, examen, comunicación de resultados y seguimiento de disposiciones o recomendaciones.

3. Planificación

Toda inspección/auditoría en el sector público/privado debe ser planificada de manera que garantice la realización de una labor de alta calidad de un modo económico, eficiente y eficaz y de manera oportuna (momento) y de acuerdo con los principios de la buena gestión de proyectos.

La planificación de la inspección/auditoría debe permitir un normal desarrollo del proceso, de manera que se facilite su administración, se haga un uso eficiente de

los recursos involucrados y se puedan incorporar los ajustes que correspondan durante su desarrollo.
El auditor debe elaborar el programa para la actividad de planificación, en el que se definan los procedimientos de inspección/auditoría que se requiere aplicar para cumplir con los objetivos correspondientes a esta actividad; así como el objetivo, naturaleza, alcance, oportunidad, plazo y responsables de los mismos.

Los procedimientos de inspección/auditoría en la actividad de planificación deben elaborarse para obtener un conocimiento de la entidad, vinculado con el objetivo y alcance de la inspección/auditoría, la comprensión del sistema de control interno relacionado con el asunto objeto de inspección/auditoría, así como la identificación de los criterios de inspección/auditoría que serán aplicados. Con estos insumos de información y conocimiento, se realizará una evaluación del riesgo, que conduzca a seleccionar las áreas a auditar en la actividad de examen y permitirá la elaboración del Plan General de Inspección/auditoría.

El auditor debe preparar y documentar un Plan General de Inspección/auditoría para guiar el desarrollo de la actividad de examen. El Plan General de Inspección/auditoría debe contener al menos, los siguientes asuntos:

a) Marco de referencia de la Inspección/auditoría.
b) Viabilidad de la inspección/auditoría.
c) Relevancia de la inspección/auditoría.
d) Objetivo de la inspección/auditoría.
e) Alcance y período objeto de examen
f) Resumen de los resultados y selección de áreas de examen.
g) Recursos requeridos para el desarrollo del trabajo
h) Cronograma de trabajo.

La organización de inspección/auditoría, según sus objetivos, debe valorar oportunamente la posibilidad de utilizar especialistas internos o externos, que sean

requeridos para apoyar la realización de una inspección/auditoría, según estas normas, deben ser calificados y tener competencia profesional demostrada en sus áreas de especialización y no tener impedimentos que afecten su independencia y objetividad.

En la actividad de planificación se deben depurar, validar, desarrollar o ajustar los criterios de inspección/auditoría, así como el título, objetivo y alcance del examen a realizar. En ese sentido, al final de dicha actividad de planificación se deberá comunicar a la administración la viabilidad de la inspección/auditoría, así como el nombre, objetivo y alcance de la inspección/auditoría, y los criterios de inspección/auditoría a aplicar.

En la actividad de planificación se debe preparar y aprobar el programa específico que el equipo de trabajo elaboró, para ser ejecutado durante la actividad de examen de cada uno de los temas, áreas o cuentas seleccionadas.

4. Examen

Durante la actividad de examen se debe ejecutar el programa específico para alcanzar los objetivos de la inspección/auditoría, ejecutar en forma ordenada las actividades dispuestas, lo cual conlleva a realizar pruebas, evaluar controles y recolectar la evidencia necesaria mediante la utilización de técnicas y prácticas de inspección/auditoría para determinar, justificar y presentar apropiadamente los hallazgos de inspección/auditoría, con sus atributos de criterio, condición, causa y efecto.

El auditor debe utilizar los métodos estadísticos que correspondan para la selección y análisis de muestras, dependiendo del objetivo y el alcance de la inspección/auditoría.

5. Comunicación de resultados

01. La organización de inspección/auditoría debe establecer e implementar políticas y procedimientos sobre las formas de comunicación y el trámite de documentos que origine el proceso de inspección/auditoría.

02. El auditor debe mantener una comunicación proactiva y efectiva con la Administración de la entidad u órgano, con el fin de facilitar el normal desarrollo de todo el proceso de la inspección/auditoría, sin perder de vista ni comprometer en ningún momento la objetividad e independencia que le rige.
03. Las instancias correspondientes de la administración auditada deben ser informadas, sobre los principales resultados, las conclusiones y las disposiciones o recomendaciones según corresponda, producto de la inspección/auditoría que se lleve a cabo, lo que constituirá la base para el mejoramiento de los asuntos examinados.
04. La comunicación del auditor con la Administración se debe realizar, según su juicio profesional, al considerar la relevancia de los resultados obtenidos, en forma paralela a la actividad de examen, mediante informes parciales y un informe final, o bien, por medio de un solo informe final una vez concluida esa actividad.
05. Los informes de inspección/auditoría deben elaborarse en un lenguaje sencillo, ser objetivos, concisos, claros, completos, exactos e imparciales, basados en hechos y respaldados con evidencia suficiente, competente y pertinente y con una estructura predeterminada de conformidad con las políticas que al respecto emita la organización de inspección/auditoría y en atención a los requerimientos técnicos.
06. En los informes de inspección/auditoría se debe revelar que la inspección/auditoría fue realizada de conformidad con el NGIOA dictado por la Agencia de Protección de Datos de los Habitantes, así como señalar cualquier otra normativa que resulte aplicable.
07. En la declaración de cumplimiento del NGIOA, incorporada en los informes de inspección/auditoría, se revelará si no se siguió alguna norma, lo que debe quedar justificado en los papeles de trabajo con la debida aprobación de quien corresponda, conforme a lo que se establezca a lo interno de la organización de inspección/auditoría.

08. El auditor debe efectuar una conferencia final con la Administración de la entidad u órgano auditado y con los responsables de las bases de datos de poner en práctica las recomendaciones o disposiciones, antes de emitir el Informe Definitivo, con el fin de exponer los resultados, conclusiones y disposiciones o recomendaciones de la inspección/auditoría, de conformidad con lo establecido por las políticas y procedimientos de la organización de inspección/auditoría.
09. Los informes de inspección/auditoría deben incorporar, en su cuerpo o en un anexo, el análisis realizado de las observaciones recibidas de la Administración.
10. Los informes de inspección/auditoría deben contener un resumen ejecutivo de los principales resultados obtenidos, así como de las conclusiones, disposiciones o recomendaciones emitidas.
11. Las disposiciones o recomendaciones se redactarán cuando el equipo de inspección/auditoría haya establecido que existen acciones correctivas u oportunidades de mejora, admisibles y viables, que puedan ser aplicadas por la entidad u órgano auditado, para atender las debilidades encontradas. Deben contemplar al menos lo siguiente:

a) Generar valor
b) Fundamentadas en la calidad
c) Atacar las causas del problema o condición identificada.
d) Dirigidas al nivel responsable de solventar la deficiencia.
e) Ser claras, específicas, convincentes y relevantes

6. Seguimiento

Cada organización de inspección/auditoría del sector público/privado debe establecer e implementar los mecanismos necesarios para verificar oportunamente el cumplimiento efectivo de las disposiciones o recomendaciones emitidas.

La Administración es responsable tanto de la acción correctiva como de implementar y dar seguimiento a las disposiciones y recomendaciones de manera oportuna y efectiva, por lo que deberá establecer políticas, procedimientos y

sistemas para comprobar las acciones llevadas a cabo para asegurar el correcto y oportuno cumplimiento. Las inspecciones/auditorías internas deberán verificar el cumplimiento de las disposiciones o recomendaciones que otras organizaciones de inspección/auditoría hayan dirigido a la entidad u órgano de su competencia institucional.

La organización de inspección/auditoría del sector público/privado, de conformidad con el marco legal que la regula, debe establecer con claridad las acciones que proceden en caso de que las disposiciones o recomendaciones emitidas sean incumplidas injustificadamente por la entidad auditada.

7. Evidencia de inspección/auditoría

Los hallazgos de inspección/auditoría contenidos en los informes deben estar sustentados en evidencia suficiente, competente y pertinente, obtenida por los medios legales y técnicos aplicables.

El Auditor debe seleccionar, con base en su juicio profesional, las técnicas de recopilación de información que sean válidas y fiables para obtener la evidencia.

El juicio profesional de los auditores determinará la cantidad y el tipo de evidencia necesaria para respaldar sus hallazgos.

8. Documentación de la inspección/auditoría

Cada organización de inspección/auditoría debe establecer las políticas y procedimientos relativos al diseño, revisión, codificación, manejo, custodia y conservación de los papeles de trabajo (documental y electrónico), de conformidad con la normativa jurídica y técnica aplicable.

La organización de inspección/auditoría debe considerar en sus políticas y procedimientos relacionados con los papeles de trabajo, la inclusión de regulaciones que propicien y faciliten la utilización de soportes electrónicos en su totalidad para la documentación de las inspecciones/auditorías, según las posibilidades de la institución y valorando aquella normativa institucional interna definida sobre políticas de reducción de papel o de uso eficiente de los recursos.

Las inspecciones/auditorías se deben documentar por medio de papeles de trabajo, los que deberán contener información que respalden los hallazgos contenidos en el informe.

En los papeles de trabajo se deben consignar los procedimientos de Inspección/auditoría realizados, la evidencia relevante recopilada y las conclusiones del equipo de inspección/auditoría durante la actividad.

Los papeles de trabajo deben ser suficientes, oportunos, claros, concisos, redactados en tono constructivo, completo y detallado de acuerdo con los objetivos de la inspección/auditoría.

9. Archivo permanente

La organización de inspección/auditoría debe mantener un archivo permanente actualizado, ya sea en forma impresa, digital u otro medio electrónico, que contenga la información relevante sobre la entidad u órgano sujeto de inspección/auditoría.

10. Calidad en la inspección/auditoría

El aseguramiento de la calidad de la inspección/auditoría es una labor que debe ejecutarse durante cada una de las actividades del proceso de inspección/auditoría, con el propósito de asegurar que los insumos, las tareas realizadas y los productos generados cumplan oportunamente con los estándares profesionales y con los requerimientos establecidos en la normativa bajo un enfoque de efectividad y mejoramiento continuo.

La organización de inspección/auditoría debe asumir su compromiso y responsabilidad con el aseguramiento de la calidad en la inspección/auditoría en el sector público/privado mediante el establecimiento de un sistema de control de calidad que considere y de respuesta a los riesgos asociados con la calidad del trabajo desarrollado. Este sistema de control de calidad debe incluir:

a) Políticas y procedimientos que promuevan internamente, una cultura de importancia de la calidad en el desempeño de las inspecciones/auditorías.

b) Políticas y procedimientos que garanticen razonablemente el cumplimiento de los valores y requerimientos éticos relevantes.

c) Políticas y procedimientos que le den garantía al ente auditado sobre la competencia, capacidad y compromiso del personal en el desarrollo de las inspecciones/auditorías.

d) Políticas y procedimientos sobre la observancia y el cumplimiento de estándares profesionales y de aquellos elementos legales y regulatorios particulares en la institución durante el desarrollo de las inspecciones/auditorías.

e) Un proceso de monitoreo del sistema de control de calidad, que garantice la relevancia, la idoneidad y la operación correcta del sistema conforme a su objetivo de creación.

El sistema de control de calidad debe complementarse con una adecuada divulgación al personal de la entidad que desarrolla las inspecciones/auditorías. Para ello debe implementar las siguientes acciones:

a) Diseñar, desarrollar y mantener actualizadas las políticas y metodologías de trabajo que se deben aplicar en los diferentes tipos de inspección/auditoría, que permitan un control apropiado de la calidad. Dicha normativa debe estar alineada con el flujo de trabajo definido para cada actividad de la inspección/auditoría, de manera que el auditor tenga disponible los lineamientos, plantillas, modelos y herramientas que debe o puede aplicar en cada parte de la inspección/auditoría.

b) Establecer mecanismos oportunos de divulgación y capacitación de la normativa técnica y jurídica

relacionada con la inspección/auditoría en el sector público/privado. Dicha capacitación debe ir dirigida a todo el personal que realiza labores de inspección/auditoría.

c) Establecer mecanismos de supervisión continua y documentada en cada una de las actividades del proceso de inspección/auditoría en el sector público/privado, para asegurar el cumplimiento de la normativa que sobre el particular se haya emitido y resulte aplicable.

La organización de inspección/auditoría debe realizar procesos continuos de revisión interna de la calidad de la inspección/auditoría en el sector público/privado, con el fin de verificar si las políticas y metodologías están diseñadas de conformidad con la normativa técnica y jurídica relacionada y determinar si efectivamente se

están aplicando. Esas revisiones deben ser efectuadas por personal independiente del que ejecutó las inspecciones/auditorías, el cual debe contar con la competencia y experiencia necesarias.

Capítulo III

NORMAS GENERALES SOBRE INSPECCIÓN/AUDITORÍA DE CUMPLIMIENTO

1. Planificación

01. El objetivo, alcance y los procedimientos diseñados deben responder a un enfoque de cumplimiento.
02. El auditor, según los objetivos de inspección/auditoría y el criterio profesional debidamente documentado, debe obtener un conocimiento razonable del asunto objeto de inspección/auditoría y comprender el sistema de control interno relacionado con ese asunto.
03. El auditor, según los objetivos de inspección/auditoría, deberá realizar una evaluación del riesgo de inspección/auditoría, con fundamento en el conocimiento adquirido y la comprensión del ambiente de control del ente u órgano objeto de inspección/auditoría.
04. Los procedimientos que se definan para el desarrollo de una inspección/auditoría de carácter especial, deben circunscribirse al asunto objeto de inspección/auditoría.

2. Criterios de inspección/auditoría

En las inspecciones/auditorías de carácter especial, el auditor debe discutir y comunicar a la Administración los criterios de inspección/auditoría que aplicará, una vez que hayan sido identificados.

3. Evidencia

El auditor debe definir la naturaleza, alcance y oportunidad de los procedimientos de inspección/auditoría que se aplicarán, a efecto de obtener la evidencia suficiente, pertinente y competente para respaldar los resultados de la inspección/auditoría.

4. Comunicación de resultados

El informe de inspección/auditoría de carácter especial debe incluir los hallazgos, las conclusiones, y las disposiciones o recomendaciones pertinentes.

Anexo 2. Descripción General de la Auditoría

Descripción General de la Auditoría

Nombre de la Auditoría
Auditoría para Entidades Públicas/Privadas de Costa Rica

Si la Base de datos se encuentra inscrita en PRODHAB
Revisar el expediente en caso de que la o las base (s) de datos esté (n) inscritas ante la PRODHAB, de lo contrario se debe de entrevistar a las personas auditadas para obtener información.

Objetivo General
El propósito de esta auditoría es analizar la o las base (s) de datos que contiene (n) datos personales, el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36)

Objetivos específicos
1. Analizar la implementación de los mecanismos de seguridad indicados en el Reglamento a la Ley 8968. 2. Revisar la razonabilidad de la seguridad física y lógica de los datos personales, tratados o almacenados en la(s) base(s) de datos. 3. Verificar la consistencia e integridad de los datos registrados la(s) base(s) de datos.

Producto

Informe final de Inspección de Oficio/auditoría

Efectos
• Constatar que se mantienen las medidas de seguridad administrativas, físicas y lógicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el Reglamento 8968 • Mayor apoyo a la toma de decisiones mediante el cumplimiento de la Ley de protección de datos de los Habitantes y su Reglamento 8968 • Buenas prácticas de gestión de la calidad y seguridad de la información relativa a las bases de datos.

Justificación del Proyecto
Artículo 16 de la Ley 8968 Son atribuciones de la PRODHAB, además de las otras que le impongan esta u otras normas, las siguientes: a) Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos. c) Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados. d) Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y,

excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.

Artículo 33. Facultad de verificación.

La Agencia podrá verificar, en cualquier momento, que la base de datos esté cumpliendo con los términos establecidos en el protocolo mínimo de actuación.

Institución auditada

Alcance
La auditoría se fundamenta en la evaluación de la base(s) de dato(s) y en evaluar un adecuado tratamiento de los datos personales durante un periodo de 2 meses, así como los mecanismos de control utilizados.

Vínculo del proyecto con el PETI
Las auditorías colaboran con los objetivos de la UTI, específicamente y los objetivos principales de la PRODHAB

Roles en el Proyecto (Asistente, Auditor, Coordinador, Responsable, Revisor)		
Nombre	***Rol***	***Horas***

Profesional en Auditoría	Coordinadora / Auditora	120
Profesional en Auditoría	Revisor	30
Total de Horas		**150**

Estimación del monto invertido en el proyecto
Pendiente

Fecha de inicio y de finalización de la auditoría	
Fecha Inicio	1 abril 2018
Fecha final	1 junio 2018

No	**Etapa**	**Responsable**	**Meses**												**Observaciones**
			E	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**	
1	Descripción General														
2	Planificación														
3	Ejecución														
4	Informe Final														
5	Revisión del Informe con Responsables														

	NOMBRE	CARGO	INICIALES
ELABORADO POR:	Auditor o Asistente	Profesional UTI	
REVISADO POR:	Encargado de la revisión	Jefe UTI	

Anexo 3. Planificación de la Auditoría

Planificación de la Auditoría

Nombre de la Auditoría
Auditoría para Entidades Públicas y Privadas de Costa Rica

Entidad Auditada	
Nombre de la Auditoría	Auditoría para Entidades Públicas y Privadas de Costa Rica
Tipo de Auditoría	Cumplimiento
Actividad	Planificación - Etapa 2

Equipo de Trabajo		
Nombre	***Puesto***	***Iniciales***
Auditor o Asistente	Auditor	Iniciales
Auditor	Jefatura	Iniciales

Objetivos de la Auditoría	
Objetivo General	El propósito de esta auditoría es analizar la o las base (s) de datos que contiene (n) datos personales, el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36)

Objetivos Específicos	1. Analizar la implementación de los mecanismos de seguridad indicados en el Reglamento a la Ley 8968. 2. Revisar la razonabilidad de la seguridad física y lógica de los datos personales, tratados o almacenados en la(s) base(s) de datos. 3. Verificar la consistencia e integridad de los datos registrados la(s) base(s) de datos.
Objetivos de la actividad	Lograr un conocimiento general y realizar una evaluación de aspectos relevantes asociados a la protección de datos personales, según el alcance del estudio, con el fin de determinar, si las bases de datos garantizan un adecuado tratamiento de los datos personales.

Alcance	
Asuntos objetivos de estudio	Indagar si la empresa auditada ha diseñado e implementado mecanismos de control efectivos para evidenciar un adecuado tratamiento de los datos personales de conformidad con el reglamento y la ley 8968. Indagar sobre la calidad de la información contenida en las bases de datos que son objeto de estudio. Indagar acerca del planeamiento de las TI y el cumplimiento de la Ley de Protección de la persona

	frente al tratamiento de sus datos personales 8968 y su reglamento.
Período	El periodo a analizar comprende el año 20XX

Normativa aplicable para la Auditoría	
Nombre de la norma	**Abreviatura**
Ley de Protección de la Persona frente al tratamiento de sus datos personales Nº 8968	LPDH
Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales	RLPDH
Procedimiento Interno de Auditoría	PIA
Manual de Normas técnicas para la gestión y el control de las Tecnologías de Información	N-2-2007-CO-DFOE
Objetivos de control para la información y tecnologías relacionadas (COBIT por sus siglas en inglés)	COBIT
ISO 27000 e ISO 22301	ISO
NIST - Guide to Protecting the Confidentiality of Personally Identifiable Information SP 800-122	Nist 800-122
Red Iberoamericana de Protecciones de Datos (Estándares)	RIPD

Criterios de auditoría aplicables	
Nombre	**Detalle**
Ley de Protección de la Persona frente al tratamiento de sus datos personales Nº 8968	Artículo 1.- Objetivo y fin Artículo 2.- Ámbito de aplicación Artículo 6.- Principio de calidad de la información Artículo 7.- Derechos que le asisten a la persona Artículo 10.- Seguridad de los datos Artículo 16.- Atribuciones
Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales	Artículo 32. De los protocolos mínimos de actuación Artículo 34. De las medidas de seguridad en el tratamiento de datos personales Artículo 35. Factores para determinar las medidas de seguridad Artículo 36. Acciones para la seguridad de los datos personales.
Manual de Normas técnicas para la gestión y el control de las Tecnologías de Información	1.3 Gestión de riesgos 1.4 Gestión de la seguridad de la información 1.4.1 Implementación de un marco de seguridad de la información

	1.4.2 Compromiso del personal con la seguridad de la información 1.4.3 Seguridad física y ambiental 1.4.4 Seguridad en las operaciones y comunicaciones 1.4.5 Control de acceso 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica 1.4.7 Continuidad de los servicios de TI
Objetivos de control para la información y tecnologías relacionadas (COBIT por sus siglas en inglés)	APO01 Gestionar el Marco de Gestión de TI APO02 Gestionar la Estrategia APO03 Gestionar la Arquitectura Empresarial APO07 Gestionar los Recursos Humanos APO10 Gestionar los Proveedores APO11 Gestionar la Calidad APO12 Gestionar el Riesgo BAI01 Gestionar los Programas y Proyectos BAI02 Gestionar la Definición de Requisitos

	BAI03 Gestionar la Identificación y la Construcción de Soluciones BAI04 Gestionar la Disponibilidad y la Capacidad BAI05 Gestionar la Introducción a Cambios Organizativos BAI06 Gestionar los Cambios BAI07 Gestionar la Aceptación del Cambio y del a Transición BAI08 Gestionar el Conocimiento BAI09 Gestionar los Activos BAI10 Gestionar la Configuración DSS05 Gestionar Servicios de Seguridad EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno EDM02 Asegurar la Entrega de Beneficios EDM04 Asegurar la Optimización de los Recursos EDM05 Asegurar la Transparencia hacia las Partes Interesadas

NIST - Guide to Protecting the Confidentiality of Personally Identifiable Information SP 800-122	2.1 Identificando PII 2.3 PII y practicas Justas de información 3.1 Definición de Nivel de Impacto 3.2 Factores para la determinación de niveles de impacto de confidencialidad PII 4.1 Salvaguardias operacionales 4.2 Salvaguardias específicas de privacidad 4.3 Controles de Seguridad
Red Iberoamericana de Protecciones de Datos (Estándares de Protección de Datos Personales para los Estados Iberoamericanos)	9. Tratamiento de datos personales de carácter sensible 21. Principio de seguridad 37. Reconocimiento de medidas proactivas

Procedimientos de auditoría a aplicar					
No	Procedimientos	Responsable	Periodo Estimado		Ref. Papeles de trabajo
			Fecha inicio	Fecha finalización	
1	**Comunicación de la Auditoría**				

1.1	Coordine una reunión con el superior jerárquico de la entidad y el responsable/encargado de la base de datos, con el fin de comunicarle los términos del estudio y solicitarle su colaboración para el equipo de auditoría				
2	**Conocimiento general de la Entidad**				
2.1	Indagar si existe un expediente asociado a la o las base (s) de datos esté (n) inscritas ante la PRODHAB				
2.2	Indagar si existen previas inspecciones/auditorías y recomendaciones asociadas a la base de datos en estudio				
2.3	Contrataciones realizadas por la entidad en cuanto a la base de datos y su infraestructura y/o almacenamiento				

2.4	Normativa interna emitida por la entidad sobre tecnologías de información y protección de datos personales				
3	**Conocimiento de información emitida por parte de la Auditoría Interna de la entidad sobre la protección de datos personales**				
3.1	Entreviste al Auditor Interno de la entidad para verificar la realización de estudios en los últimos cuatro años (2015-2018) o en ejecución sobre la materia de TI específicamente en la protección de datos personales. De existir informes identifique las principales recomendaciones y su grado de cumplimiento, así como la disposición de la Administración para su acatamiento				

3.2	Identifique en el plan de trabajo de la Unidad de Auditoría Interna si contempla la protección de datos personales y su tratamiento				
4	**Ambiente de control interno**				
4.1	Obtenga un conocimiento general del ambiente de control interno, asociado con el tratamiento de los datos personales				
4.2	Indague aspectos relativos a la evaluación de riesgos asociados con la protección de datos personales, su identificación, valoración y establecimiento de acciones para su administración y tratamiento.				
5	**Normativa TI, y seguridad de la información**				
5.1	Entreviste al encargado/responsable de				

	la base de datos, sobre los esfuerzos institucionales en la gestión de las TI, los planes que se tienen previstos, e incluso, sobre problemáticas que se hayan dado en relación con la protección de datos, que tengan algún tipo de impacto.				
5.2	Solicite el proceso de tecnologías, y la topología de red, y el proceso del tratamiento de datos personales				
6	**Cierre de fase**				
6.1	Analice los resultados de la aplicación de los procedimientos anteriores, a efecto de estructurar y resumir el conocimiento logrado de la entidad				
6.2	Formule los criterios de evaluación del estudio y proceda a su validación con el encargado/responsable de la base de datos				

6.3	Elabore y someta a aprobación del nivel correspondiente los resultados de los hallazgos y recomendaciones encontradas en la ejecución de la inspección/auditoría				
6.4	Reunión con Dirección Nacional de PRODHAB y a su vez traslado del informe final a la Dirección para lo que proceda en el Área Legal				

Fuentes de Información
Normativa de la PRODHAB
Normativa, sistemas, página web, e información suministrada por la entidad auditada
Entrevistas con funcionarios de la entidad auditada

Recursos Requeridos	
Humanos	Dos Auditores y una abogada
Tecnológicos	Portátiles de los funcionarios encargados del estudio
Fisicos	Espacio físico en la entidad auditada
Financieros	Ninguno

Otros	

	NOMBRE	CARGO	INICIALES
ELABORADO POR:	Auditor o Asistente	Profesional UTI	Iniciales
REVISADO POR:	Auditor	Jefe UTI	Iniciales

Anexo 4. Ejecución de la Auditoría

Ejecución de la Auditoría

Nombre de la Auditoría
Auditoría para Entidades Públicas y Privadas de Costa Rica

Entidad Auditada	
Nombre de la Auditoría	Auditoría para Entidades Públicas de Costa Rica
Tipo de Auditoría	Normal
Actividad	

Equipo de Trabajo		
Nombre	***Puesto***	***Iniciales***
Auditor o Asistente	Auditor	Iniciales
Auditor	Jefatura	Iniciales

Objetivos de la Auditoría	
Objetivo General	El propósito de esta auditoría es analizar la o las base (s) de datos que contiene (n) datos personales, el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36)
Confirmaciones a evaluar	Procesos y metodología que utiliza la entidad para garantizar un adecuado tratamiento de los datos personales, si es Entidad Pública debe cumplir con La Ley de Control Interno y sus normas para garantizar eficacia y eficiencia en lo referente a los procesos de tecnologías de información La Entidad cuenta con políticas y procedimientos que garanticen de forma razonable un adecuado tratamiento de los datos personales. La Entidad cuanta con sistema de control interno que de forma inherente colabora con el tratamiento de los datos personales.

Alcance y Periodo	
Alcance	La auditoría comprende los procesos que tomen en cuenta mecanismos de control, infraestructura asociada a la base de datos, control de accesos, control interno y evaluación de riesgos asociado a la protección de datos personales. El análisis abarca el periodo entre el 1 de abril 2018 y hasta el 1 de junio de 2018, el cual puede ser ampliado si se considera pertinente.

Período	Entre el		Y el	

Normativa aplicable para la auditoría	
Nombre de la norma	**Abreviatura**
Ley de Protección de la Persona frente al tratamiento de sus datos personales Nº 8968	LPDH
Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales	RLPDH
Normas Generales de Inspecciones de Oficio/Auditorías	NGIOA

Criterios de auditoría aplicables	
Nombre	**Detalle**
Ley de Protección de la Persona frente al tratamiento de sus datos personales Nº 8968	Artículo 1.- Objetivo y fin Artículo 2.- Ámbito de aplicación Artículo 6.- Principio de calidad de la información Artículo 7.- Derechos que le asisten a la persona Artículo 10.- Seguridad de los datos Artículo 16.- Atribuciones

Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales	Artículo 32. De los protocolos mínimos de actuación Artículo 34. De las medidas de seguridad en el tratamiento de datos personales Artículo 35. Factores para determinar las medidas de seguridad Artículo 36. Acciones para la seguridad de los datos personales.
Manual de Normas técnicas para la gestión y el control de las Tecnologías de Información	1.3 Gestión de riesgos 1.4 Gestión de la seguridad de la información 1.4.1 Implementación de un marco de seguridad de la información 1.4.2 Compromiso del personal con la seguridad de la información 1.4.3 Seguridad física y ambiental 1.4.4 Seguridad en las operaciones y comunicaciones 1.4.5 Control de acceso 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica 1.4.7 Continuidad de los servicios de TI

Objetivos de control para la información y tecnologías relacionadas (COBIT por sus siglas en inglés)	APO01 Gestionar el Marco de Gestión de TI APO02 Gestionar la Estrategia APO03 Gestionar la Arquitectura Empresarial APO07 Gestionar los Recursos Humanos APO10 Gestionar los Proveedores APO11 Gestionar la Calidad APO12 Gestionar el Riesgo BAI01 Gestionar los Programas y Proyectos BAI02 Gestionar la Definición de Requisitos BAI03 Gestionar la Identificación y la Construcción de Soluciones BAI04 Gestionar la Disponibilidad y la Capacidad BAI05 Gestionar la Introducción a Cambios Organizativos BAI06 Gestionar los Cambios BAI07 Gestionar la Aceptación del Cambio y del a Transición BAI08 Gestionar el Conocimiento BAI09 Gestionar los Activos

	BAI10 Gestionar la Configuración DSS05 Gestionar Servicios de Seguridad EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno EDM02 Asegurar la Entrega de Beneficios EDM04 Asegurar la Optimización de los Recursos EDM05 Asegurar la Transparencia hacia las Partes Interesadas
NIST - Guide to Protecting the Confidentiality of Personally Identifiable Information SP 800-122	2.1 Identificando PII 2.3 PII y practicas Justas de información 3.1 Definición de Nivel de Impacto 3.2 Factores para la determinación de niveles de impacto de confidencialidad PII 4.1 Salvaguardias operacionales 4.2 Salvaguardias específicas de privacidad 4.3 Controles de Seguridad
Red Iberoamericana de Protecciones de Datos (Estándares)	9. Tratamiento de datos personales de carácter sensible 21. Principio de seguridad

	37. Reconocimiento de medidas proactivas

Procedimientos de auditoría a aplicar					
No	Procedimientos	Responsable	Periodo Estimado		Ref. Papeles de trabajo
			Fecha inicio	Fecha finalización	
1	**Proceso de planeamiento institucional y de tecnologías de información**				
1.1	Solicite la última versión de los planes estratégicos institucional y de TI				
1.2	Revisar si en estos documentos se contempla la protección de datos personales				
2	**Seguridad de las Tecnologías de Información**				

2.1	Solicite a la Unidad de TI las políticas y procedimientos de seguridad de la información y de protección de datos; determine la completitud de estos documentos				
2.2	Realice una visita a los principales centros de datos y verifique la existencia y suficiencia de controles de seguridad física, que estén asociados a la base de datos en estudio				
2.3	Contrataciones realizadas por la entidad en cuanto a la base de datos y su infraestructura y/o almacenamiento				
2.4	Solicite y analice los planes de contingencia informática de la Unidad de Informática que contemplen la base de datos en estudio				
2.5	De presentarse brechas importantes en estos documentos y procesos, documentarlas y establecer sus causas				
3	**Calidad de la información**				

3.1	Lleve a cabo una visita al Departamento de Redes y Procesamiento de Información con el propósito de conocer las labores de control de calidad que se llevan a cabo				
3.2	Solicite los procedimientos y estándares que garantizan la calidad de la información incorporada a la base de datos de este estudio				
3.3	De considerarse necesario, verifique la calidad de la información en una muestra de los registros de la base de datos en estudio				
4	**Control Interno y Evaluación del Riesgo**				
4.1	Determine la existencia de un Sistema de Control Interno				

4.2	Consulta sobre evaluación de control interno asociada a la base de datos en estudio				
5	**Base de datos**				
5.1	Del motor de base de datos utilizado generar la siguiente información: Screenshot donde se observe el nombre y versión del Sistema Operativo. Screenshot donde se observe las versiones y archivos utilizados para desarrollar los nuevos cambios.				
5.2	Facilitar la siguiente información directamente de la base de datos en compañía de funcionarios de la PRODHAB ✓ Usuarios ✓ Grupos ✓ Permisos sobre ciertos directorios ✓ Configuraciones de contraseñas ✓ Configuraciones generales de seguridad				

	✓ o Listado de parches instalados				
5.3	• Lista de personas que pueden: ✓ autorizar creación/modificación/eliminación de usuarios y permisos, ✓ Crear/modificar/eliminar usuarios y permisos ✓ Utilizar cuentas privilegiadas de los sistemas ✓ Realizan monitoreo del proceso de administración de usuarios ✓ Realizan monitoreo de las actividades de las cuentas privilegiadas				
5.4	Matriz de perfiles de usuarios la base de datos debidamente actualizada y aprobada				
6	**Riesgos**				
6.1	Se cuenta con un análisis de riesgos en la organización, para detectar vulnerabilidades en las plataformas tecnológicas (sistemas operativos, bases de datos y a nivel de aplicación y red perimetral), indicar la frecuencia con la que se aplica, asociado a la base de datos en estudio				

6.2	De encontrarse brechas importantes en estos procesos, indagar sus causas				

Fuentes de Información
Normativa de la PRODHAB
Normativa, sistemas, pagina web, e información suministrada por la entidad auditada
Entrevistas con funcionarios de la entidad auditada

Recursos Requeridos	
Humanos	Dos Auditores y una abogada
Tecnológicos	Portátiles de los funcionarios encargados del estudio / computadoras de los funcionarios entrevistados
Físicos	Espacio físico en la entidad auditada
Financieros	Ninguno
Otros	

	NOMBRE	CARGO	INICIALES
ELABORADO POR:	Auditor o Asistente	Profesional UTI	
REVISADO POR:	Auditor	Jefe UTI	
APROBADO POR:		Directora Nacional	

Anexo 5. Planificación de la Auditoría

1 de julio, 2018

UNIDAD DE AUDITORÍA

INFORME DE LA INSPECCIÓN/AUDITORÍA

El propósito de esta inspección/auditoría es analizar la o las base (s) de datos que contiene (n) datos personales, el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36)

Tabla de contenido

RESUMEN 108

¿Qué examinamos? 108

¿Qué encontramos? 108

¿Qué sigue? 108

1. INTRODUCCIÓN 108

ORIGEN DE LA INSPECCIÓN/AUDITORÍA 108

OBJETIVO DE LA INSPECCIÓN/AUDITORÍA 109

ALCANCE DE LA INSPECCIÓN/AUDITORÍA 109

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA INSPECCIÓN/AUDITORÍA 109

GENERALIDADES ACERCA DE LA INSPECCIÓN/AUDITORÍA 109

METODOLOGÍA APLICADA 109

2. OBSERVACIONES 110

3. CONCLUSIONES 110

4. ATRIBUCIONES/REQUERIR..... 111

ANEXOS..... 111

RESUMEN

¿Qué examinamos?

Esta auditoría consistió en analizar la o las base (s) de datos que contiene (n) datos personales, a fin de determinar el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36), además verificar la aplicación de buenas prácticas de gestión de las Tecnologías de Información, en la infraestructura atinente a la base de datos de estudio. A continuación, se dará una descripción de la base de datos que se examinó.

¿Qué encontramos?

Se determinó una carencia de políticas y procedimientos de seguridad de la información que pone en riesgo la confidencialidad, integridad y disponibilidad de la información de la entidad, propiamente en el área de protección de datos personales. En consecuencia, esto amenaza la continuidad de las operaciones ante eventos que atenten contra la integridad de los equipos y su información.

¿Qué sigue?

Se requiere de las autoridades, el encargado y el responsable de la base de datos de la Entidad enviar un plan que con el plazo establecido para mitigar los riesgos encontrados asociados a los hallazgos que fueron determinados a través de este estudio.

1. INTRODUCCIÓN

ORIGEN DE LA INSPECCIÓN/AUDITORÍA

1.1. El propósito de esta auditoría es analizar la o las base (s) de datos que contiene (n) datos personales, el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36)

Determinar si la empresa auditada ha diseñado e implementado mecanismos de control efectivos para evidenciar un adecuado tratamiento de los datos personales de conformidad con el reglamento y la ley 8968. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.

OBJETIVO DE LA INSPECCIÓN/AUDITORÍA

1.2. Analizar la o las base (s) de datos que contiene (n) datos personales, el cumplimiento de los protocolos mínimos de actuación, y evidenciar las acciones para la seguridad de los datos personales (art. 36)

ALCANCE DE LA INSPECCIÓN/AUDITORÍA

1.3. La auditoría se fundamenta en la evaluación de la base(s) de dato(s) y en evaluar un adecuado tratamiento de los datos personales durante un periodo de 2 meses, así como los mecanismos de control utilizados.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA INSPECCIÓN/AUDITORÍA

1.4. La Entidad cuenta con el apoyo de la gerencia para la constitución de la documentación pendiente, además que el proceso actual cuenta con controles preventivos.

GENERALIDADES ACERCA DE LA INSPECCIÓN/AUDITORÍA

1.5 Información básica de la Entidad.

METODOLOGÍA APLICADA

1.9. Se aplicaron las Normas Generales de Inspecciones de Oficio/auditoría para Entidades Públicas y Privadas de la PRODHAB.

COMUNICACIÓN PRELIMINAR DE RESULTADOS DE LA A INSPECCIÓN/AUDITORÍA

Pendiente

2. OBSERVACIONES

Observación No. 1

POLÍTICAS DE SEGURIDAD

Evidenciamos la ausencia de políticas que regulen las Configuraciones Generales de Seguridad para Bases de Datos y Sistemas Operativos en la compañía.

Riesgo

Posibilidad de que las Configuraciones Generales de Seguridad para Sistemas Operativos y Bases de Datos no sean las mínimas requeridas.

Recomendación

Evaluar la posibilidad de elaborar un documento que regules las Configuraciones Generales de Seguridad para Bases de Datos y Sistemas Operativos.

Responsables: Pedro Pérez

Puesto: Encargado de la base de datos

Fecha probable de implementación: 30 agosto 2018

3. CONCLUSIONES

3.1. En materia de Tecnologías de Información es relevante contar con políticas dirigidas a apoyar los proyectos y procesos sustantivos de la organización, los

cuales deben estar alineados a las estrategias institucionales. Por ello, resulta una oportunidad para la entidad pública. Además de contemplar la protección de datos en la documentación pendiente de crear.

4. ATRIBUCIONES/REQUERIR

4.1. Según lo estipulado en el Artículo 16 de la Ley 8968 Son atribuciones de la PRODHAB, además de las otras que le impongan esta u otras normas, las siguientes:

a) Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.

c) Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados.

d) Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.

Artículo 33. Facultad de verificación.

La Agencia podrá verificar, en cualquier momento, que la base de datos esté cumpliendo con los términos establecidos en el protocolo mínimo de actuación.

AL LA ENTIDAD PUBLICA AUDITADA

4.2 Pendiente

ANEXOS