Universidad Técnica Nacional

Ingeniería del Software

Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente

Nivel: Licenciatura

Elaborado por:
Keylin Calvo Alfaro
Rubén Sánchez Matamoros

DECLARACIÓN JURADA

Nosotros, Rubén Alberto Sánchez Matamoros portador de la cédula número dos – cero seis seis cuatro – cero dos tres dos (206640232); Keylin Gloriana Calvo Alfaro portadora de la cédula número dos – cero seis siete nueve – cero nueve uno cuatro (206790914), conocedor de las sanciones legales con la que la Ley Penal de la República de Costa Rica castiga el falso testimonio y el Reglamento Disciplinario Estudiantil de la Universidad Técnica Nacional, UTN.

DECLARAMOS bajo la fe de juramento lo siguiente: Que somos estudiantes de la Carrera de Ingeniería del Software en el nivel de Licenciatura de la Universidad Técnica Nacional y como requisito de graduación debemos realizar una investigación aplicada descriptiva y exponerla, la cual tiene como tema de investigación: *Propuesta de Incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la Ley 8968 del 2011.*

Por lo que manifestamos que la misma ha sido elaborada siguiendo las disposiciones exigidas por la Universidad Técnica Nacional, UTN.

Además, declaramos que dicha investigación es el resultado de nuestro esfuerzo e investigación en su totalidad, que en ella no han participado personas ajenas ni otras organizaciones.

ES TODO.

Firmo en la ciudad de Alajuela a las _____horas del _____mes de ____de 2015.

Keylin Gloriana Calvo Alfaro, cédula 206790914

Rubén Alberto Sánchez Matamoros; cédula 20664023

AGRADECIMIENTOS

- Deseamos dar gracias a Dios por estar a nuestro lado a través de este proceso y permitirnos concluir una etapa más de nuestra vida universitaria.

- Agradecer al personal docente, administrativo y demás funcionarios de la Universidad Técnica Nacional que con su ayuda, apoyo y colaboración para hacer de este proyecto una realidad.

- Especial agradecimiento al PhD. Hugo Solís Sánchez por el interés, conocimiento y disponibilidad puestos a nuestra disposición, para enriquecer y ayudar a la realización de este trabajo.

- Finalmente, agradecer a nuestros padres por la confianza y el apoyo incondicional que siempre nos han dado.

Tabla de contenido

RESUMEN EJECUTIVO

La presente tesis consiste en el desarrollo de una guía técnica metodológica, mediante el análisis y aplicación de un estándar de cifrado, que permita la protección de datos confidenciales en la Universidad Técnica Nacional cumpliendo con lo establecido en la legislación vigente.

El objetivo central es entregar una guía técnica metodológica que la Universidad Técnica Nacional pueda utilizar como estándar para implementar el cifrado en las bases de datos institucionales.

Se pretende orientar al personal de la Universidad para que el proceso de cifrado sea más sencillo y rápido de implementar en el momento que decidan realizarlo. Para lograr lo anteriormente descrito, se elaboró una guía paso a paso con la información recolectada sobre el proceso del cifrado, donde explica los pasos a seguir para llevar a cabo la configuración que se requiere para cifrar la información.

La tesis consta de seis capítulos en los que se detalla la importancia de la propuesta.

El capítulo dos describe en su totalidad el cifrado en la protección de datos, los tipos de cifrado existentes y las normas de seguridad en la protección de datos.

El capítulo tres describe a la Universidad Técnica Nacional como la institución para la cual se va a desarrollar el proyecto.

El capítulo cuatro hace una descripción del análisis situacional de la Universidad Técnica Nacional y sobre las buenas prácticas a utilizar.

El capítulo cinco contiene las conclusiones y recomendaciones que se deben tomar en cuenta sobre aspectos legales, métodos de cifrado, buenas prácticas y protección de la información.

El capítulo seis contiene la guía de cifrado para las bases de datos de la Universidad Técnica Nacional.

APROBACIONES

Carrera Licenciatura en Ingeniería del Software con salida lateral al Bachillerato en Software y al Diplomado en Tecnologías Informáticas

Nota de aval inicial

Por este medio, hago constar que el documento con el nombre **Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente,** elaborado por los estudiantes Keylin Gloriana Calvo Alfaro y Rubén Alberto Sánchez Matamoros portadores de la cédula de identidad número 206790914 y 206640232 respectivamente, han cumplido con elementos propios de la especialidad, permitiendo la detección de problemas de índole teórica y práctica, el empleo de los conocimientos adquiridos en el transcurso de la preparación profesional.

Además, ha permitido el fortalecimiento y aplicación de las competencias adquiridas durante su formación universitaria, aplicando técnicas y métodos de investigación básica y aplicada conforme las políticas de investigación definidas por la Universidad Técnica Nacional en el análisis, planteamiento y resolución del problema.

El enriquecimiento de la carrera y el fortalecimiento de la universidad, mediante este tipo de aportes investigativos son fundamentales para el fortalecimiento de la Institución dentro del contexto universitario costarricense, contribuyendo con el desarrollo de la comunidad nacional.

Por lo anterior, le doy el aval a este documento para que sea trasladado al análisis y revisión exhaustiva por parte de los lectores que la dirección haya definido.

Sin más por el momento suscribo

Lic. Joaquín Artavia Chaves

Cédula: 204900534

Número colegiado: 1190

Cc.- Archivo

Universidad Técnica Nacional

Carrera Licenciatura en Ingeniería del Software con salida lateral al Bachillerato en Software y al Diplomado en Tecnologías Informáticas

Carta de Aprobación por parte del Lector del trabajo Final de Graduación

Alajuela, 7 de marzo de 2017

Estimados señores:

En mi calidad de Lector de Tesis y en cumplimiento de lo dispuesto con las directrices de Trabajos Finales de Graduación, he leído, revisado, corregido y aprobado:

Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente.

Elaborado por los postulantes: Keylin Gloriana Calvo Alfaro y Rubén Alberto Sánchez Matamoros, como requisito para optar por el grado de Licenciatura en Ingeniería de Software.
Considero que dicho trabajo cumple con los requisitos formales y de contenido exigidos por la Universidad Técnica Nacional, - Sede Central.

Suscribe

Anthony Morera V.

MRT. Anthony Morera Vásquez

Cédula de identidad: 109460089

Número de colegiado: 1145

Cc.- Archivo

Nota de aprobación del lector

Por este medio, en calidad de lector del documento **"Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente"** elaborado por los estudiantes Rubén Alberto Sánchez Matamoros portador de la cédula número 206640232; Keylin Gloriana Calvo Alfaro portadora de la cédula número 206790914, doy por finalizado el análisis y la revisión solicitados. Siempre con el afán de mejorar, me permití hacer una serie de recomendaciones y ajustes que desde mi perspectiva profesional, han de permitir contar con mejores perspectivas de desarrollo futuro.

En esta misma línea, considero que es un documento que cumple con los requerimientos fundamentales de la investigación profesional según el nivel universitario en que se ha desarrollado.

Sin más por el momento, suscribo

Ana Salazar

Nombre y firma **Ana Magali Salazar Ávila**

Cédula de identidad **205470730**

Número de colegiado **26152**

Cc.- Archivo

Nota de validación del tutor

Por este medio, en calidad de tutor del documento **Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente** doy fe de que los ajustes y variaciones propuestas por los lectores, han sido tomados en cuenta en la consistencia y redacción técnica del documento final.

Por lo anterior es que doy mi anuencia para que el documento pase a la etapa final de la defensa, previa revisión filológica.

Sin más por el momento, suscribo

Lic. Joaquín Artavia Chaves
Cédula de identidad 204900534
Número de colegiado 1190

Cc.- Archivo

Alajuela, 03 de junio de 2017

Señores
Ingeniería del Software
Sede Central
Universidad Técnica Nacional

Estimados señores:

Se comunica la revisión y corrección estilística del Trabajo Final de Graduación ***Propuesta de incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente****, para optar por el grado académico de Licenciatura en Ingeniería del Software; a petición de los sustentantes: Keylin Calvo Alfaro, portadora de la cédula de identidad 206790914 y Rubén Sánchez Matamoros, portador de la cédula de identidad 206640232, a cargo de la suscrita profesional en Filología Española.*

Cordialmente,

Isabel Cristina Solís Moreira
Filóloga y Docente
Inscripción: 94-771; 412-154

Licda. Cristina Solís M.
☎ 8312-4262
Colegiada COLYPRO 030715
✉ *csolismoreira@gmail.com*

Universidad Técnica Nacional | Licenciatura en Ingeniería del Software

Trabajo Final de Graduación

Acta No. 002

Acta de la sesión **No. 002**, del dia Viernes 11 de agosto de 2017, a partir de las 18:00 horas , en periodo del segundo cuatrimestre, y en la que el Tribunal Evaluador recibe la sustentación del proyecto de graduación, realizado por lo(a)s estudiantes: **Keylin Gloriana Calvo Alfaro,** portadora de la cédula: 206790914 y **Rubén Alberto Sánchez Matamoros;** portador de la cédula 206640232 quienes optan por el Grado Académico de Licenciatura en Ingenieria del Software, sita, en la Universidad Técnica Nacional, presentando el trabajo final de graduación con el tema:

Propuesta de Incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la Ley 8968 del 2011.

Preside el Tribunal la **Licda. Ana Cecilia Odio Ugalde**, directora de carrera de Ingeniería del Software, junto con la participación del **Lic. Joaquín Artavia Chaves** tutor del trabajo final de graduación, **MRT. Anthony Morera Vásquez**, y **Master Ana Magaly Salazar Ávila,** lectores del trabajo final de graduación.

El Señor Presidente del Tribunal manifiesta que los miembros del mismo leyeron el informe, que acogió las recomendaciones de la Dirección de Carrera, en consecuencia procede a recibir la sustentación correspondiente, en la que los estudiantes realizan su exposición, sujeto al tiempo establecido, terminada la misma, se procede a externar los comentarios pertinentes al trabajo presentado, se formulan preguntas que fueron respondidas por parte de los sustentados de manera exitosa.

Concluida la sustentación, el Tribunal, solicita a los presentes retirarse de la sala para proceder a la votación secreta. La votación da como resultado: aprobado. Con nota de 10 diez.

De nuevo en la sala, el señor(a) Presidente les comunica el resultado, por lo tanto les declara que ya son: LICENCIADOS EN INGENIERÍA DEL SOFTWARE, a la vez, indica que conforme a la reglamentación existente, deben entregar la documentación según lo que se establece en el Reglamento de Trabajos finales de Graduación vigente; también les recuerda la obligación de presentarse al ACTO DE GRADUACIÓN, al que serán convocados oportunamente. Se cierra la sesión a las: 19 horas y 00 minutos del presente.

Keylin Gloriana Calvo Alfaro
Estudiante

Rubén Alberto Sánchez
Matamoros

Lic. Joaquín Artavia Chaves
Miembro del Tribunal
Evaluador
Tutor

MRT. Anthony Morera
Vásquez
Miembro del Tribunal
Evaluador
Lector

Master Ana Magaly Salazar
Ávila
Miembro del Tribunal
Evaluador
Lectora

Licda. Ana Cecilia Odio
Ugalde
Directora de Carrera

CAPÍTULO I: INTRODUCCIÓN

1.1. Estado del Arte

Desde épocas antiguas hasta la actualidad, la necesidad de privacidad en los datos y de ocultamiento de los mensajes, se ha convertido en uno de los pilares principales para la conservación de la información, con el fin de mantenerlos a salvo de terceros que desean utilizarlos para fines que no corresponden con los establecidos.

Como solución ante esta necesidad surge la criptografía, que se utiliza como técnica para el cifrado de todo tipo de información. El origen de este término "…proviene del griego, donde [sic] se realiza la unión de los términos *kriptos* (escondido, oculto) con *logos* (discurso, estudio)" (Valenzuela, pág. 1).

La criptografía, podría considerarse como el arte de esconder el verdadero significado de un mensaje, tal y como se menciona en la siguiente cita: "la criptología entonces vendría a ser el estudio del sentido oculto o lo que se esconde en determinados mensajes" (Valenzuela, pág. 1).

El proceso criptográfico se remonta al siglo V antes de Cristo, "…es una técnica muy antigua, y durante mucho tiempo se ha relacionado con los círculos militares, religiosos y comerciales" (INTECO, pág. 1). Uno de los primeros métodos de cifrado históricamente conocidos es el llamado cifrado César que consistía en escribir el mensaje con un formato de letras del alfabeto latino desplazadas tres posiciones a la derecha.

Además de permitir ocultar el contenido de los mensajes, la criptografía también aumenta el nivel de seguridad de la información, tal y como se expresa en el siguiente párrafo:

> …un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de

> manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo (Carbajal, 2011).

En la época actual el uso del cifrado en actividades cotidianas es cada vez más común, “Actualmente, la necesidad de proteger la información ha hecho que la utilidad de la criptografía se haya extendido a actividades comunes” (INTECO, pág. 1).

No cabe duda que conservar información sensible, resguardada; es de suma importancia para mantener disponibilidad e integridad general; como consecuencia, diversas compañías han decidido hacer uso de este método de protección de datos. El robo de información por cualquier tipo de medio es una situación común, donde las personas utilizan diversas técnicas para hurtar todo tipo de datos, ya sea información personal o datos bancarios, entre otros.

En Latinoamérica, los delitos informáticos, el cibercrimen, así como el robo de información han aumentado conforme la tecnología evoluciona, la situación anterior se puede comprobar en la siguiente cita realizada específicamente para el sector latinoamericano, en donde se aprecia que dicho sector es fuertemente atacado por toda clase de delitos informáticos:

> De acuerdo [sic] con diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. La posibilidad de su comisión a través de Internet permite que, sin mayores complicaciones, el delincuente pueda estar en un determinado país, utilizar servicios de otro, para finalmente atacar a una o más víctimas de un tercer país interviniente. (Ignacio, 2013, pág. 1)

Esta situación se da también en Costa Rica, donde la incidencia de robo en todo tipo de información, se ha hecho sentir en los últimos años. “Los delitos informáticos son más frecuentes de lo que se cree en Costa Rica. Así lo considera Gabriel Macaya, director de la ANC (Academia Nacional de Ciencias)” (Rojas P. , 2014).

A raíz del aumento en la delincuencia informática, se han buscado acciones para responder a esta amenaza, como la citada a continuación.

> Es más frecuente de lo que la gente se imagina. Se promueve la creación de los Centros de Respuesta de Incidentes en Seguridad Informática, en Costa Rica el Instituto Costarricense de Electricidad tiene un centro de respuesta para la protección de la infraestructura del ICE y de sus clientes… estos incidentes de seguridad informática son mucho más complejos y hasta globales. (Rojas P. , 2014)

Las compañías de nivel nacional e internacional están informadas sobre estos problemas, conocen y están conscientes de la importancia de contar en toda organización con mecanismos que ayuden al resguardo de la información, por eso han buscado e implementado diferentes métodos para mantener su información resguardada y segura.

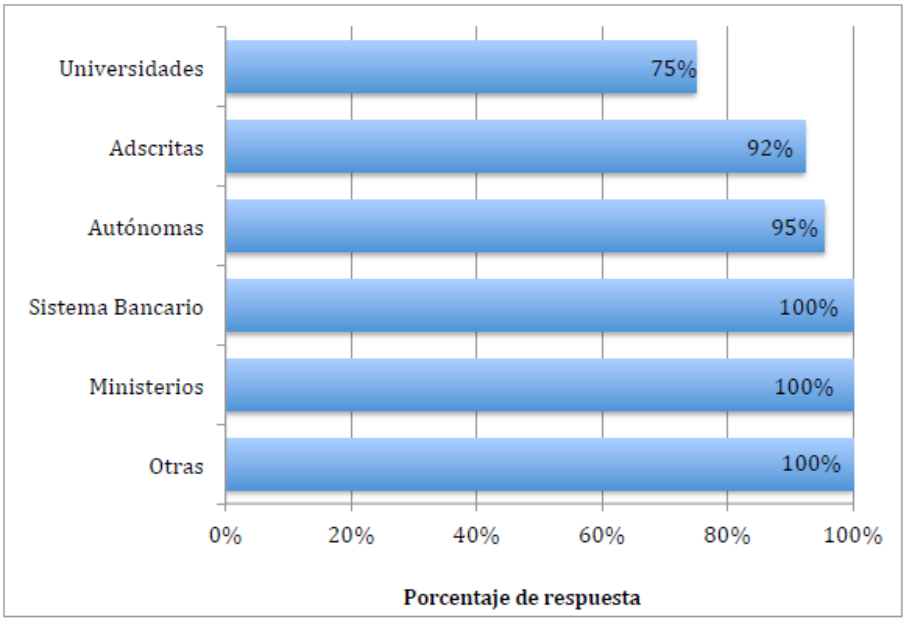
La criptografía se ha convertido en la respuesta al resguardo de la información y es el recurso que han empleado miles de empresas a nivel mundial para mantener sus bases de datos seguras, “…durante los próximos dos años, el 69% de las organizaciones encuestadas planean incrementar el uso de cifrado, lo que demuestra que las empresas se están moviendo en una dirección positiva” (Gómez, 2016).

Para Velazco, la criptografía ofrece importantes funciones, muy utilizadas en la actualidad:

> La criptografía se encarga, precisamente, de cifrar o codificar mensajes para evitar que su contenido pueda ser leído por un tercero no autorizado; es decir, la generación de códigos y algoritmos de cifrado que buscan ofuscar la información y protegerla de "ojos curiosos" es el cometido principal de esta disciplina. (Velasco, 2014, pág. 1)

Según estudios recientes, se ha encontrado que las instituciones públicas son las más vulnerables para convertirse en víctimas de algún tipo de delito informático. Como lo demuestra el siguiente gráfico tomado del Informe sobre el Estado de la Seguridad Informática en el Sector Público Costarricense (MINAET, 2011)

Gráfico 1.1. Porcentaje de Respuesta según tipo de institución



Tomado de (MINAET, 2011, pág. 16)

Como se aprecia en el gráfico, el sector de las universidades públicas de Costa Rica en comparación con las demás instituciones, son las menos preparadas ante cualquier tipo de ataque en la información que almacenan en sus bases de

datos, por lo que el uso de la criptografía para cuidar la información que conservan es sumamente necesario.

Para ayudar al resguardo de estos datos existen varios tipos de cifrado de los que se deriva una serie de clasificaciones, entre las cuales se pueden mencionar la criptografía simétrica, asimétrica e hibrida, entre ellas:

> La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad (diciéndola en alto, mandándola por correo electrónico u ordinario o haciendo una llamada telefónica) (Gutiérrez, Tipos de criptografía: simétrica, asimétrica e hibrida, 2013).

Basándose en la cita descrita se puede concluir que la criptografía simétrica tiene una vulnerabilidad a considerar si se piensa utilizar, ya que solo utiliza una clave para cifrar y descifrar los mensajes. Esto puede ser peligroso porque existe el riesgo de que otras personas la descubran o ilícitamente la descubran.

> La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca) (Gutiérrez, Tipos de criptografía: simétrica, asimétrica e hibrida, 2013).

De acuerdo con la cita, la criptografía asimétrica es un poco más segura que la simétrica, ya que al utilizar dos claves la seguridad se vuelve más robusta. El problema de este método sería la manipulación que se le dé a la clave privada, puesto que no podría ser vista o descubierta por parte de ningún usuario fuera de los asignados.

La última de las clasificaciones es la del cifrado de tipo híbrido. Se denomina de esta forma por ser una mezcla de las dos anteriores clasificaciones, se define de esta manera en la siguiente cita:

> “Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento.” (Gutiérrez, Tipos de criptografía: simétrica, asimétrica e hibrida, 2013). El sistema criptográfico hibrido es el más seguro por utilizar según lo anteriormente descrito, ya que hace uso de los dos métodos de cifrado para hacerla más resistente a ataques de terceros que deseen apoderarse de la información. Combina la seguridad con la rapidez que cada una de las anteriores ofrece, convirtiendo este método en el más seguro por utilizar.

La utilización del cifrado es útil en muchas áreas, no sólo para el cifrado de datos bancarios o de información en universidades:

> …el cifrado de los datos no sólo es útil para las comunicaciones, sino también en todo caso en que se quiera proteger información sensible. Así, es posible cifrar la información contenida en discos, carpetas o incluso archivos individuales, para evitar el acceso no permitido. Luego, además del beneficio de proteger la privacidad de los usuarios, el cifrado de datos evita otro tipo de ataques como el robo de identidad, o los fraudes bancarios, además de brindar un mecanismo de protección ante el robo o pérdida de dispositivos con información sensible (Porolli, 2013, pág. 1).

Lo anterior da margen para considerar que, hoy día, las empresas están obligadas a cifrar los datos y no lo hacen porque piensan que es un proceso complicado; sin embargo, su uso parece estar en aumento, responde a las nuevas amenazas que se presentan día con día, lo que podría mejorar las herramientas para

esta tarea y que el cifrado se vuelva más sencillo de implementar, que exista más equipo especializado para realizarlo, posiblemente bajando el costo del mismo y muestra beneficios a corto plazo.

1.2. Justificación de la Investigación

En Costa Rica, como en muchos países del mundo, se ha concebido a la seguridad informática como un área operativa dentro de las organizaciones, encargada del resguardo de la información, con el fin de mantener la seguridad, sin posibilidad de acceso a personas ajenas, así como eventos que puedan convertirse en un tipo de amenaza para la confidencialidad de la información.

> "Tener un país conectado también implica ser responsables en materia de seguridad de la información. Estar preparados significa apoyar a las instituciones para proteger el patrimonio más valioso: la información; significa aprender, prevenir y dar un énfasis en la alfabetización digital en ese conjunto de funcionarios, que con mayores o menores recursos, luchan por defender nuestro patrimonio" manifestó el Viceministro de Telecomunicaciones, Emilio Arias (MICIT, 2015).

Tal y como se mostró, el tema de seguridad de la información ha tomado mayor relevancia en Costa Rica, sumado a las alianzas del país con otras naciones como Corea del Sur. Esto ha hecho que el tema cobre fuerza, como resultado se obtuvo la firma del acuerdo en seguridad cibernética, en el año 2015 por ambos países, "…marco del II Taller de Ciberseguridad, el Viceministerio de Telecomunicaciones y la Agencia Coreana de Seguridad e Internet (KISA; por sus siglas en inglés), firmaron un Acuerdo de Entendimiento para fortalecer y promover el desarrollo de la seguridad cibernética" (MICIT, 2015).

Este nuevo rumbo que ha tomado Costa Rica, en materia de ciberseguridad ha dado como resultado que el tema se torne de suma importancia. "La seguridad

cibernética es interés nacional, ya que provee herramientas y mecanismos para la protección de los datos que circulan por la red; el Plan Nacional de Desarrollo (PND) 2014 – 2018” (MICIT, 2015)

Como consecuencia de lo anterior, los Ministerios e instituciones del Estado o aquellas reguladas por éste, deben acoplarse a este esfuerzo y establecer las medidas necesarias para proporcionar seguridad adecuada a la información que manejan en sus bases de datos. La Universidad Técnica Nacional no se exime de ello.

> La Estrategia Nacional de Ciberseguridad contempla la coordinación con aproximadamente 331 instituciones del Estado, “donde al Viceministerio de Telecomunicaciones le corresponde una labor como coordinador y facilitador de esfuerzos; pero además, se requiere de un trabajo articulado y el compromiso, que involucra al Estado, el sector empresarial, las universidades públicas y privadas y a los sectores productivos, para impactar positivamente a todo el país”, puntualizó Arias (MICIT, 2015).

El país ha planteado una serie de reglamentaciones en materia de seguridad de la información:

- Centro de Atención a Incidentes de Seguridad Informática -CSIRT-CR; creado por Decreto Ejecutivo nº 37052-MICIT.
- Ley de Protección de la Persona frente al tratamiento de sus Datos Personales (Nº 8968) y su Reglamento.
- Agencia de Protección de Datos de los Habitantes (Prodhab).
- Ley N° 9048 Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos informáticos y conexos, del Título VII del Código Penal.
- La Contraloría General de la República emite en el 2007 las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información. Publicado en la Gaceta 119 del 21 de junio del 2007.

En esta misma línea, organismos internacionales como el IGTI (Instituto de Gobernanza de Tecnologías de Información), se ha dado a la tarea de plantear una serie de regulaciones para el buen manejo de los procesos de las tecnologías de información, uno de estos estándares creados es Cobit.

“Cobit se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. Cobit ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI” (IT Governance Institute, 2007, pág. 10). Esta guía proporciona una serie de pasos detallados que las organizaciones pueden adaptar a sus procesos para mejorarlos y estandarizarlos a las normas internacionales, el proceso de seguridad de la información tiene su propio apartado en la guía de Cobit, es el dominio DS5 Garantizar la seguridad de los Sistemas.

> La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de la administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de los roles y responsabilidades de la seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad (IT Governance Institute, 2007, pág. 124).

De lo anterior, se extrae que, según Cobit, la protección de los sistemas de información es integral en la administración de una empresa; ya que previene o minimiza pérdidas o daños de los equipos o la información del negocio, que podrían

terminar en detrimentos económicos, problemas legales o daños a la imagen de la compañía.

Por lo tanto, se vuelve fundamental una adecuada administración de las llaves criptográficas con las que cuentan las instituciones para el resguardo de su información. Para dicho efecto, Cobit define lo siguiente:

> **DS5.8 Administración de Llaves Criptográficas**
>
> Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas (IT Governance Institute, 2007, pág. 125).

Con el fin de buscar formas más seguras de transmisión y almacenamiento de datos, en muchas de las empresas a nivel global han implementado varios tipos de métodos que ayudan a mantener y preservar la información. En la actualidad, una de las tecnologías más usadas es el cifrado de datos, técnica donde las compañías por medio de algoritmos criptográficos ocultan la información, logrando la protección que requieren para mantener los datos propios y de los clientes a salvo.

Por todo lo mencionado anteriormente, se pretende que esta investigación sirva para crear una guía técnica para el proceso de implementación de un estándar de cifrado, de esta manera, la Universidad Técnica Nacional cumpla con lo establecido en el artículo 10 de la sección III de la ley 8968 de protección de datos personales que se titula “Seguridad y confidencialidad del tratamiento de los datos” y que cita lo siguiente:

> “El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o

> acceso no autorizado, así como cualquier otra acción contraria a esta ley".

Es por esta razón que la propuesta para el establecimiento de un estándar de cifrado, ayudará a la Institución a mejorar sus procesos de seguridad de la información, en este caso, con un sistema de criptografía robusto y actualizado, que cumpla con las buenas prácticas y el procesamiento adecuado de los datos, así como el acceso a los mismos de forma segura.

Siguiendo con el artículo 10 de la ley, que establece:

> "No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas".

De lo anteriormente citado se desprende que como una forma de guiar en un mejor camino hacia la inclusión de dichas normas dentro de las regulaciones internas universitarias en materia de seguridad de la información, se propondrá una guía técnica metodológica que funcione como estrategia para mejorar lo existente y que además, pueda ser utilizado en investigaciones posteriores, y así plantear mejoras al sistema actual y crear otras nuevas que contribuyan con el mejoramiento procedimental informático de la Universidad.

1.3. Problema de Investigación

1.3.1. Planteamiento del Problema

Desde civilizaciones antiguas hasta la era moderna, se han desarrollado diferentes técnicas para el cifrado de la información con el fin de ocultar mensajes y verificar que realmente viene del remitente esperado; y así evitar que sean interpretados por personas ajenas, como se ejemplifica a continuación:

> El primer empleo de escritura cifrada data del siglo V A.C., cuando se utilizaba un esclavo como portador de un mensaje, fue en la guerra entre Atenas y Esparta. Recibió en una cinta una serie de letras con aparente falta de sentido, que al ser enrollada en un determinado rodillo de madera mostraba longitudinalmente los símbolos dispuestos de tal manera que podía leerse el mensaje (Díaz, 1995, pág. 75).

Todo el desarrollo y evolución que ha experimentado la criptografía a lo largo del tiempo, se entrelaza en su propósito final con el criptoanálisis, que se define como:

> …la ciencia que estudia los métodos que se utilizan para, a partir de uno o varios mensajes cifrados, recuperar los mensajes en claro en ausencia de la(s) llave(s) y/o encontrar la llave o llaves con las que fueron cifrados dichos mensajes (Paredes, 2006, pág. 6).

Debido al aumento y perfeccionamiento en los mecanismos de cifrado de datos, la criptografía, como técnica, se ha convertido en un nicho de mercado para las compañías que brindan seguridad informática, dado que la preservación y el aseguramiento de la información se han vuelto imprescindible en la sociedad actual, tal y como se menciona en el artículo “Tarjetas de crédito, Apple y robo de información corporativa, los preferidos para el ciberdelito en 2015” (Infobae, 2014), donde tres de las mayores firmas del mercado de la ciberseguridad (ESET, Kaspersky y Websense) predicen un aumento en los intentos de robo de información.

Se recuerda que, tanto el ciberdelito como la ciberseguridad son términos que se encuentran ligados con el robo de información por vía electrónica, situación que puede suceder en las entidades públicas y privadas del país y del mundo entero.

Conforme este nicho de mercado se explota y desarrolla en todo el mundo con el pasar de los años, surgen más y mejores sistemas de codificación o cifrado de datos, que ofrecen la seguridad necesaria, además se estudia la manera de decodificar mensajes contando poca información sobre el algoritmo utilizado para su cifrado, así lograr la recuperación de la información original y utilizarla para fines delictivos.

En un artículo publicado por el diario El Economista de México se relata que en el 2014 el robo de información por correo es el rubro más vulnerable para las empresas, con un 19,2%, seguido por dispositivos portátiles 13,6% y en tercer lugar, el robo de laptops con 12,8%, resultando en que según el reportaje las primeras tres vulnerabilidades de las empresas son por robo de información con un 45%, lo que es casi la mitad de vulnerabilidades totales de las empresas centradas en este rubro (El Economista, 2014).

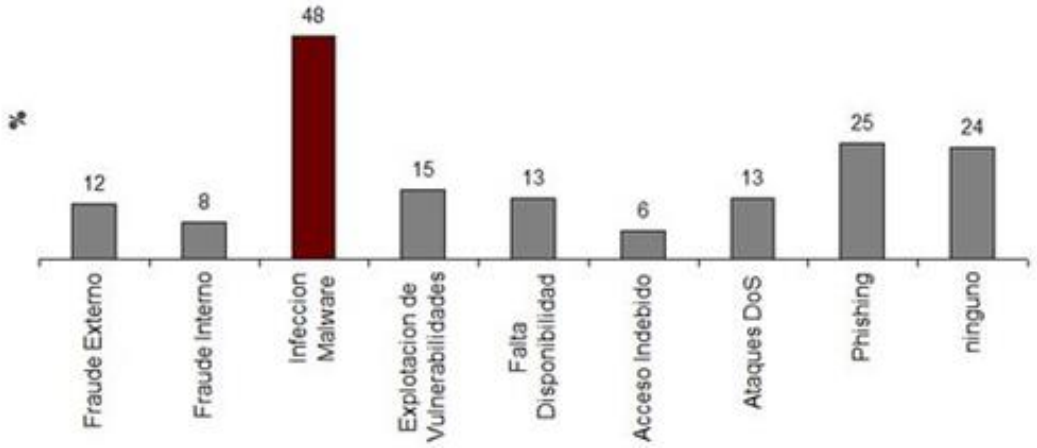
En Costa Rica la situación no escapa a esta realidad, recientemente se reveló el robo de más de 500 mil registros del sistema centralizado de recaudación (SICERE) como se menciona en el artículo "*Hackean*1" 500 mil registros del sistema de la Caja" (Rojas L. , 2015) por medio de un ataque cibernético a inicios del año 2015.

De acuerdo con el reportaje presentado por el periódico La Nación, "El 76% de las empresas en Costa Rica fue víctima de algún incidente de seguridad informática en el 2013, informó una encuesta realizada por ESET en la región" (Vega, 2014) situación a la que se debe prestar atención, ya que se revelan carencias en el área de seguridad informática del sector empresarial del país, "Las fugas de datos ponen

[1] Acción de violar la seguridad informática de un sistema.

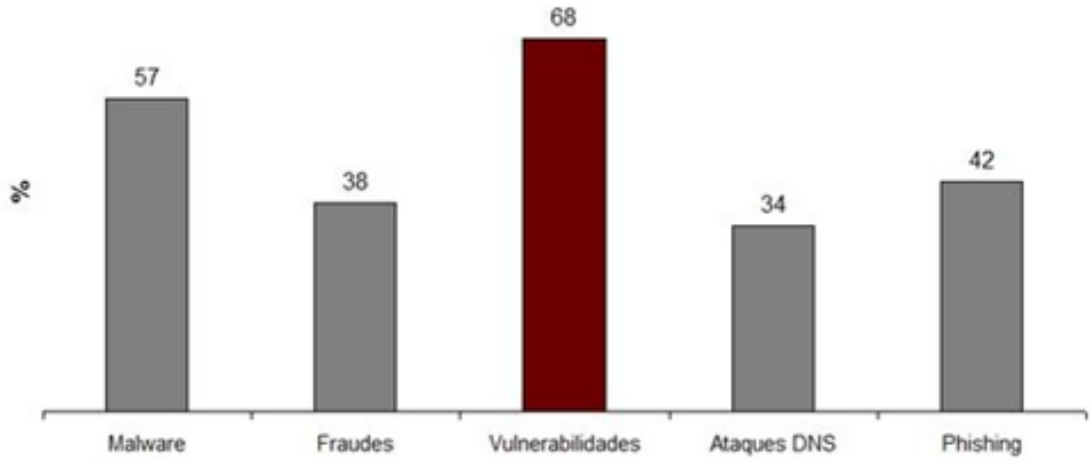
la confianza y la reputación de las compañías en riesgo y comprometen cada vez más la información personal de los consumidores" (Vega, 2014).

Gráfico 3.1. Ataques de los que han sido víctimas



Tomado de (Vega, 2014)

Gráfico 3.2. Preocupaciones que tienen en agenda



Tomado de (Vega, 2014)

Gráfico 3.3. Controles que se están implementando

Tomado de (Vega, 2014)

Según esta información, así como el incremento de este tipo de actividades en otros países y en Costa Rica, en el 2016 cabe esperar un alza significativa en este tipo de ataques, por lo que las compañías deben preocuparse por el aseguramiento de la información.

Actualmente, en Costa Rica, existe la ley 8968 “Protección de la persona frente al tratamiento de sus datos personales”, con la que se busca el aseguramiento

de la confidencialidad, integridad y disponibilidad de la información de índole personal, por lo que cobra mayor relevancia la protección de este tipo de datos.

Algunas de las razones por las cuales estas actividades delictivas están cobrando mayor importancia son:

- Las empresas han optado por tener toda su información digitalizada.
- La información personal como números de teléfono, seguro social, números de cédula y de pasaporte, tienen gran valor en el mercado.
- La facilidad para conseguir números de cuenta, tarjetas de crédito o estados financieros, es alta.
- Casi cualquier tipo de información está almacenada digitalmente.
- El uso de la modalidad de guardar la información en Internet debido a los bajos costos de mantenimiento, se ha incrementado.
- La gran cantidad de información de fácil acceso en internet sobre métodos de piratería informática, ha aumentado.

Si esto continúa igual, cada año la ciberdelincuencia irá en aumento, por lo que es preciso que las compañías costarricenses tomen medidas respecto de la seguridad informática y la protección de los datos personales.

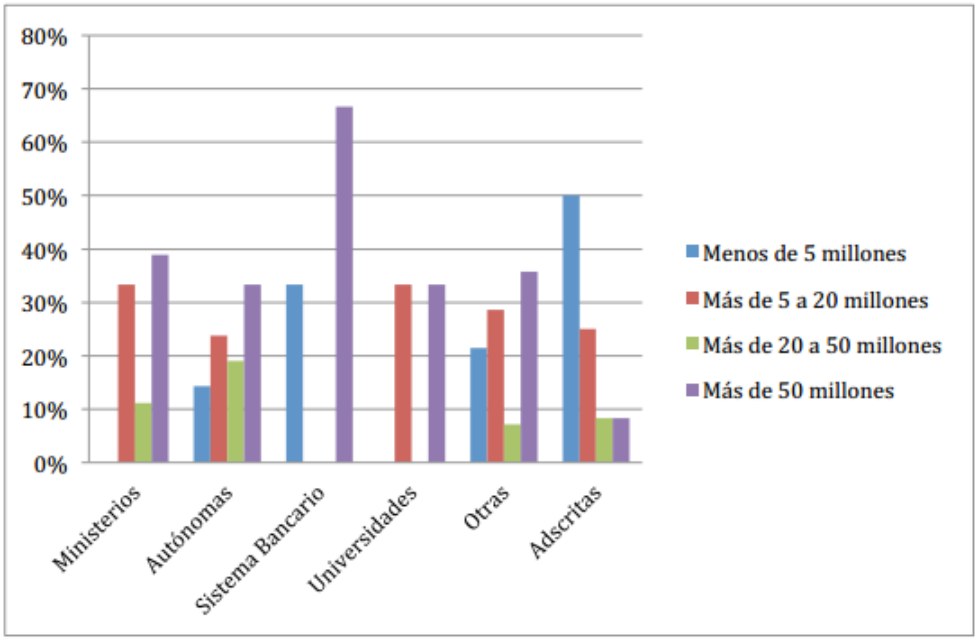
El caso de SICERE es una muestra de lo que se avecina, las grandes compañías como Apple©, Sony© y Google© son víctimas de constantes ataques cibernéticos, que buscan el robo de información de sus usuarios; una realidad en Costa Rica.

La relevancia y posibilidad de materialización exitosa de ataques de este tipo, podría llevar desde grandes pérdidas económicas y de imagen, hasta delicados procesos judiciales, dependiendo de la gravedad del caso y de la forma en como haya sido suministrada la información, sumado a esto el uso indebido que se le ha dado a los datos sustraídos.

De acuerdo con las conclusiones presentadas en el último informe de la Rectoría de Telecomunicaciones sobre el Estado de Seguridad Informática en el sector público costarricense, se detalla que el sector que más dinero invierte en seguridad es el sector financiero. “Las instituciones del sistema bancario presentan mayores porcentajes en cuanto al uso de herramientas informáticas para salvaguardar la seguridad física y lógica de sus redes de información” (MINAET, 2011, pág. 76).

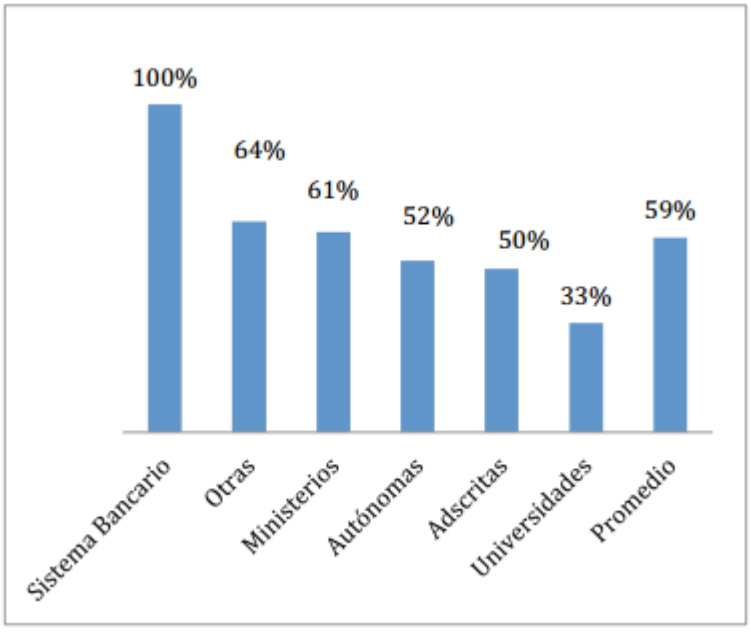
Por otra parte, las universidades son los entes que presentan menor inversión en esta área, esto se ve reflejado en el alto porcentaje de eventos de seguridad que reportaron durante el estudio, “las universidades son los entes públicos que han presentado mayores problemas de seguridad informática en el período comprendido entre enero 2010 enero 2011” (MINAET, 2011, pág. 76). Hecho que debe atenderse, ya que podría prestarse para fraudes en los títulos de carreras que ofertan, robo de información de sus estudiantes y profesores, falsificación de documentos o manipulación de datos.

Gráfico 3.4. Porcentaje de instituciones de acuerdo con el presupuesto destinado a seguridad informática (colones)



Tomado de (MINAET, 2011, pág. 63)

Gráfico 3.5. Porcentaje de Instituciones que implementaron la herramienta "Plan de continuidad de la operación" para protección de la información



Tomado de (MINAET, 2011, pág. 36)

La información mostrada indica la necesidad de propiciar cambios y mejoras en los procesos de seguridad en las instituciones costarricenses, pero especialmente

en las universidades estatales, con el fin de brindar a los usuarios protección en sus datos, ya que el objetivo principal de quienes se dedican a este tipo de estafa por medio de recursos tecnológicos es el lucro con la información sustraída.

En la actualidad, se pueden utilizar para el aseguramiento de los datos personales diversas técnicas, métodos, herramientas o estrategias y así controlar su acceso, al implementarlos como alternativas para superar la situación actual con relación a la falta de seguridad de la información. Las Universidades estatales podrían perfectamente utilizar algunos de estos como:

- Antivirus.
- Muros de Fuego.
- Sistemas de detección de intrusos.
- Roles de Acceso.
- Aplicaciones para detección de vulnerabilidades.
- Métodos confiables de criptografía que contengan un marco de referencia en donde apoyarse para que puedan ser utilizados con confianza.
- Contratos de confidencialidad robustos que garanticen fiabilidad en el proceso de cifrado de los datos.
- Controles de correo no deseado (*spam*).
- Protecciones contra software malicioso y virus (*spyware*, *malware*).
- Políticas de administración de contraseñas y nombres de usuario.
- Políticas de uso de red para los empleados.
- Formas de administración automática de la seguridad.
- Planes de continuidad de la operación.

Además de los métodos mencionados para el aseguramiento de la información, existe un estándar internacional que puede ayudar a las empresas a reducir los perfiles de riesgo en seguridad, esta herramienta se denomina COBIT, el cual en su versión 5, establece un marco que puede ser implementado para hacerle

frente a las amenazas en seguridad que pongan en riesgo los datos en las empresas,

> "el gobierno y la gestión de la información y la tecnología son temas amplios y complejos. COBIT ayuda a "simplificar" esta complejidad mediante una guía de negocios más relevante, eficiente y fácil de implementar en áreas específicas dentro de los sistemas de información. Contiene asimismo un dominio referente a seguridad de la información, desde el cual proporciona la perspectiva específica de seguridad desde esta importante herramienta de negocios y fue diseñado en respuesta a la fuerte demanda de una guía de seguridad que integra otras grandes estructuras y los patrones ", dijo Greg Grocholski, CISA, presidente internacional de ISACA y el auditor jefe de Dow Chemical (BitCompany, 2015).

Algunos de los beneficios que Cobit5 ofrece son:

- Manutención de información de alta calidad para el apoyo a las decisiones de negocios.
- Alcance de los objetivos estratégicos y obtención de los beneficios de negocio mediante el uso efectivo e innovador de las TI.
- Logro de la excelencia operativa por medio de una aplicación fiable y eficiente de la tecnología.
- Mantenimiento de los riesgos relacionados a TI bajo un nivel aceptable.
- Optimización de los servicios el coste de las TI y la tecnología.
- Apoyo para el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas.

No es posible asegurar que, lo anteriormente citado, es cien por ciento efectivos razón por la cual, la ampliación al máximo de las medidas de seguridad, es necesario, con el propósito de dificultar al máximo el trabajo del atacante.

Al ser el cifrado, la última capa de seguridad entre los datos que se quiere proteger y una persona no autorizada que desee tener acceso a ellos, al utilizar un robusto mecanismo de cifrado se asegura que en caso de que el atacante logre superar las barreras previas de seguridad, no entienda la información que ha encontrado, haciéndola inútil para sus fines.

Otro uso importante del cifrado es cuando se usa para la protección de las conexiones de internet, por medio del protocolo HTTPS[2], en el cual se cifra el canal de conexión evitando que terceros tengan acceso a los datos que se envían por este medio.

La investigación se desarrollará fundamentada en la realidad nacional en la era de la información y sus necesidades actuales en el tema de la seguridad informática. Tomando en cuenta la orientación que lleva el país en este contexto, las medidas aplicables y los estándares que debería seguir una institución universitaria, en este caso la Universidad Técnica Nacional para la implementación de seguridad en los datos.

Se procurará al final de este proceso descubrir qué tan seguro, viable y eficiente es el método de cifrado para la protección de la información ya sea personal, institucional o empresarial, almacenada en la nube o en servidores físicos; para cumplir con los requisitos que exige la Ley 8968 Protección de la persona frente al tratamiento de sus datos personales, Capitulo III, Articulo 14, Trasferencia de Datos Personales, Regla General y su reglamento, específicamente en el Capítulo V, Articulo 40, Condiciones para la Transferencia.

[2] Es un protocolo seguro de transferencia de datos de internet.

1.3.2. Formulación del Problema

Actualmente, en la Universidad Técnica Nacional, específicamente en el área de tecnologías de la información, se requiere algún tipo de sistema de cifrado sobre sus bases de datos, según información dada por personeros autorizados vía correo electrónico, dado que podrían existir carencias de seguridad en la forma de almacenamiento de los datos, que podrían provocar que se encuentren vulnerables ante un ataque o robo de información.

Además, de los riesgos a los que ya se exponen los datos de la Institución, por medio de información inicial brindada por parte del personal a cargo del área de tecnologías de la información, la Universidad podría estar incumpliendo con la ley 8968 de protección frente al tratamiento de sus datos personales. Ya que, desde su creación toda institución pública o privada de Costa Rica debería tener diversos mecanismos de protección de la información, situación que además es regulada desde la Agencia de Protección de Datos de los Habitantes (PRODHAB) que promueve la privacidad, transferencia y seguridad en los datos, el uso de la información, almacenamiento en el exterior y bases de datos anteriores a la Ley, entre otros (www.prohab.com).

En consecuencia, la exposición de la Universidad a riesgos legales, de imagen y financieros, es factible. Sea por incumplimiento o la violación a estas disposiciones, lo que inclusive podría implicar sanciones como la suspensión del uso de la base de datos e inclusive hasta la imposición de multas.

Dentro de este ámbito de análisis, esta serie de factores presentes en la Universidad, podría hacer necesaria la implementación de diversas acciones mediante políticas, procedimientos, herramientas, técnicas y métodos que aseguren el correcto funcionamiento de las bases de datos y de esta forma se garantice el uso adecuado de los datos. Por esta razón, la necesidad de contar con un estándar de cifrado en las bases de datos institucionales, podría favorecer en gran medida el

proceso de implementación de la ley y contribuir como guía para que el personal informático mejore sus acciones en torno a este proceso.

De esta manera y con base en lo descrito, surge la siguiente interrogante:

¿De qué manera la implementación de un estándar robusto de cifrado en la UTN, permitiría el aprovechamiento de factores asociados a la custodia y seguridad de la información dispuesta en la infraestructura institucional, y a la vez le traería beneficios directos en concordancia con la legislación vigente?

1.4. Objetivos de la Investigación

1.4.1. Objetivo General

Elaborar una guía técnica metodológica, mediante el análisis y aplicación de un estándar de cifrado, que permita la protección de datos confidenciales en la Universidad Técnica Nacional cumpliendo con lo establecido en la legislación vigente.

1.4.2. Objetivos Específicos

- Identificar los métodos de cifrado óptimos y las buenas prácticas del proceso de cifrado de datos mediante la revisión de los que se utilizan en la actualidad, para el desempeño de las bases de datos y su posterior aplicación en la Universidad.
- Determinar el método y la mejor práctica relacionada al cifrado de acuerdo con la información identificada, que se adapte a las necesidades de protección de datos de la Universidad.
- Examinar las ventajas de seguridad en la información y datos de los métodos escogidos, comparando la protección actual con las mejoras que se obtendrían con este nuevo procedimiento, logrando con ello un incremento en la seguridad de los datos.

- Analizar las condiciones de la infraestructura universitaria, para el aseguramiento y el resguardo de información importante, mediante el aprovechamiento del estándar sugerido.
- Proponer un estándar de cifrado para la Universidad Técnica Nacional, por medio de una guía técnica y metodológica que permita el cumplimento con lo establecido en la legislación vigente.

1.5. Hipótesis

La implementación de un estándar robusto de cifrado en la UTN, permitirá el aprovechamiento de factores asociados con la custodia y seguridad de la información dispuesta en la infraestructura institucional y a la vez, traerá beneficios directos a la Institución en concordancia con la legislación vigente.

1.6. Matriz de Congruencia

Tema	Titulo	Planteamiento del problema	Pregunta de investigación	Objetivo general y específicos
Criptografía	Propuesta de Incorporación de un estándar de cifrado a las bases de datos de la UTN según lo establecido en la legislación vigente.	¿De qué manera la implementación de un estándar robusto de cifrado en la UTN, permitiría el aprovechamiento de factores asociados a la custodia y seguridad de la información dispuesta en la infraestructura institucional, y a la vez le traería beneficios directos en concordancia con la legislación vigente?		**Objetivo General**
			¿Qué factores estructurales inciden en que la UTN no tiene ningún sistema de cifrado en sus bases de datos?	Elaborar una guía técnica metodológica, mediante el análisis y aplicación de un estándar de cifrado, que permita la protección de datos confidenciales en la Universidad Técnica Nacional cumpliendo con lo establecido en la legislación vigente.
				Objetivos Específicos

Tema	Titulo	Planteamiento del problema	Pregunta de investigación	Objetivo general y específicos
			¿Cuáles son los métodos de cifrado más recomendados para las bases de datos?	• Identificar los métodos de cifrado óptimos y las buenas prácticas del proceso de cifrado de datos mediante la revisión de los que se utilizan en la actualidad, para el desempeño de las bases de datos y su posterior aplicación en la Universidad.
			¿Cuál es la factibilidad y el impacto de implementar un método de cifrado en la base de datos?	• Determinar el método y la mejor práctica relacionada al cifrado con la información identificada, que se adapte a las necesidades de protección de datos de la Universidad.
			¿Cuáles bases de datos de la Universidad deben ser protegidas?	• Examinar las ventajas de seguridad en la información y datos de los métodos escogidos, comparando la protección actual con las mejoras que se obtendrían con este nuevo procedimiento, logrando con ello un incremento en la seguridad de los datos.

Tema	Titulo	Planteamiento del problema	Pregunta de investigación	Objetivo general y específicos
			¿Cómo ayudaría que la ley brinde los requisitos mínimos de seguridad sobre la protección de la información en lo que respecta a mecanismos de criptografía?	• Analizar las condiciones de la infraestructura universitaria, para el aseguramiento y el resguardo de información importante, mediante el aprovechamiento del estándar sugerido.
			¿Cuáles son las ventajas en que la Universidad vaya a poseer un estándar para cifrado de datos?	• Proponer un estándar de cifrado para la Universidad Técnica Nacional, por medio de una guía técnica y metodológica que permita el cumplimento con lo establecido en la legislación vigente.

CAPITULO II: MARCO TEÓRICO

2.1. El Cifrado en la Protección de los Datos

Desde épocas antiguas, el ser humano ha buscado distintas formas de comunicación y expresión que han evolucionado a través de la historia. El origen de las diferentes formas de comunicación tiene sus comienzos en las pinturas rupestres (pinturas en las cavernas), que datan de hace cuarenta mil años de antigüedad, desde los tiempos de la prehistoria, es decir, durante la última glaciación, atravesando por los tiempos de los jeroglíficos de los egipcios y otras culturas como los sumerios, hititas, chinos, entre otras. En el libro “Historia de la escritura, de la grafología y su evolución” se expresa que “los primeros signos de escritura partieron de la imitación gráfica de seres u objetos reales por medio de la pintura o los tallados” (Lages, 1994, pág. 9), continuando, posteriormente, con el surgimiento del alfabeto griego del latín, que fue el primero en separar las vocales de las consonantes, hasta los tiempos modernos con los correos electrónicos y los mensajes de texto.

2.1.1 Criptografía o Cifrado

En ocasiones la información contenida en los mensajes no debe ser entendida por nadie que no sea el destinatario de la misma, así en caso de que el mensaje llegara a manos equivocadas nadie sabría cuál es el contenido del mismo volviéndolo inútil, es aquí donde entra el uso de la criptografía. Que es la forma en que se disfraza la información para que no pueda ser entendida por personas no autorizadas.

> Este término proviene en un sentido lingüístico del griego *Kriptos*=ocultar, *Graphos*=escritura, lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje, puede ser también entendida como un medio para garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos de un sistema (Paredes, 2006, pág. 2).

De acuerdo con lo anterior, la criptografía es la ciencia de disfrazar el verdadero significado de un mensaje, de personas que no deban saberlo, es decir lo cifra.

El cifrado es la técnica o procedimiento con el cual se disfraza u oculta la información por medio de una llave, sin la cual no se puede descifrar el mensaje.

> "El cifrado de la información o criptografía es la ciencia que estudia el diseño de métodos para ocultar el significado de un mensaje, siendo éste públicamente disponible. Es decir, se oculta el contenido del mismo, pero no el mensaje" (Fuensanta, pág. 1).

Como se explica en la cita anterior, el cifrado y la criptografía van de la mano. Resumiendo, la criptografía es la ciencia que estudia los métodos o maneras de ocultar la información contenida en datos o mensajes, a este proceso se le llama cifrado.

> "Con la criptografía se puede garantizar las propiedades de integridad y confidencialidad, pero hay que saber cómo utilizarla, para ello es importante tener claros los conceptos básicos que están detrás de los sistemas criptográficos modernos. Estos conceptos van desde entender qué es la criptografía, cómo está clasificada, entender el funcionamiento básico de algunos sistemas de cifrado y conocer cómo se forman los documentos digitales como firmas y sobres digitales" (Paredes, 2006, pág. 2).

Para entender el proceso de cifrado, se deben comprender los conceptos básicos que rodean este mecanismo de ocultamiento de información.

> Al mensaje a cifrar se le suele denominar *texto en claro* y al proceso de ocultar el contenido mediante una serie de transformaciones regidas por un parámetro o valor secreto, la *clave*, se le denomina *cifrar el mensaje*, al parámetro y al mensaje cifrado se le suele denominar un *texto cifrado* o un *criptograma*. Al proceso de

obtener el texto en claro a partir de un mensaje cifrado se le denomina *descifrar el mensaje.* (Fuensanta, pág. 1)

De la cita anterior se puede entender que:

- Al mensaje original se le llama texto claro.
- Al proceso de ocultarlo por medio de alguna técnica criptográfica se le llama cifrar.
- El valor secreto o parámetro para cifrar el mensaje es la clave.
- Al proceso inverso donde se toma el mensaje cifrado y se transforma a texto claro por medio de la clave se le llama descifrar.

Dos de los puntos anteriores más importantes son el de escoger la técnica criptográfica o algoritmo para cifrado y el valor de la llave, ya que recae sobre estos el nivel de seguridad que tendrán nuestros datos. El algoritmo de cifrado se define como “transformaciones de datos que los usuarios no autorizados no pueden revertir con facilidad” (Microsoft, 2016, pág. 1); dicho de otra manera, son técnicas generalmente matemáticas donde se cambian los valores originales de los datos por otros al azar.

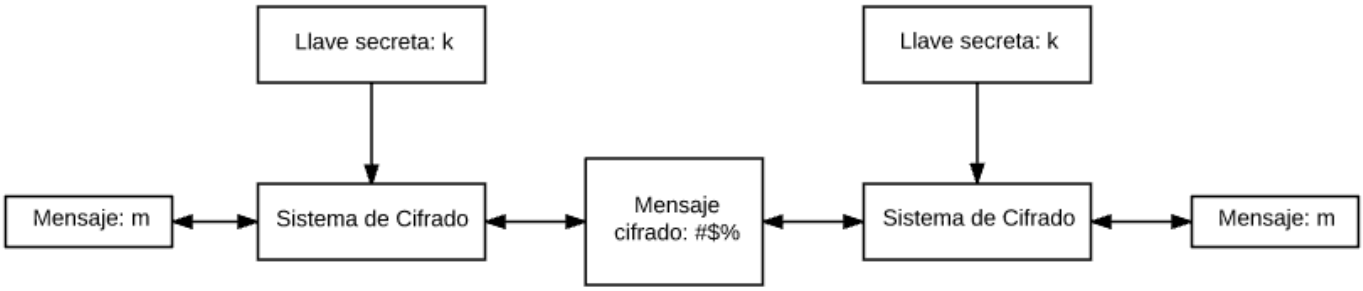
Para este proceso, se utiliza la clave como referencia, siendo esta la única que puede utilizarse para realizar la acción inversa, debido a esto la conformación y largo de la clave está directamente relacionado con la seguridad del cifrado “claves largas suelen producir un cifrado más seguro que las claves cortas” (Microsoft, 2016, pág. 2) igualmente su conformación, mientras más compleja sea la contraseña, más difícil será vulnerar la información “contraseñas largas y complejas son más seguras que las contraseñas cortas” (Microsoft, 2016, pág. 2).

Así como la criptografía se puede definir como la ciencia que estudia los mecanismos de cifrado, se debe entender los tipos y el funcionamiento de los mismos y las buenas prácticas relacionadas; los dos tipos más comunes son el cifrado simétrico, asimétrico y las funciones **hash**.

2.1.2 Cifrado Simétrico

El cifrado simétrico al ser un sistema sencillo de cifrado y descifrado con base en una sola clave, suelen ser sistemas bastante rápidos. Sin embargo, al depender únicamente de la llave secreta se corre el riesgo de que esta llegue a manos equivocadas, ya que se debe compartir con la persona a la que se le quiere hacer llegar el mensaje. El siguiente esquema, ilustra este cifrado:

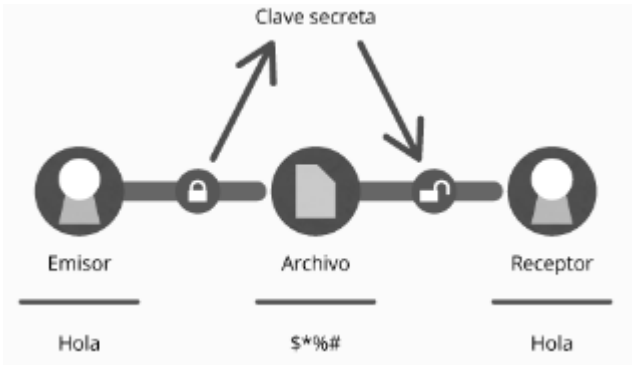
Imagen 2.1.1 Cifrado Simétrico



Tomado de (Fuensanta, pág. 10)

Con el cifrado simétrico solo se necesita conocer la clave con que se cifró el mensaje para tener acceso a la información, “la seguridad de un mensaje cifrado debe recaer sobre la clave y nunca sobre el algoritmo” (Gutiérrez, Tipos de criptografía: simétrica, asimétrica e hibrida, 2013, pág. 1) esto hace que la complejidad de la clave sea algo fundamental.

Imagen 2.1.2 Cifrado Simétrico



Tomado de (Gutiérrez, Tipos de criptografía: simétrica, asimétrica e hibrida, 2013)

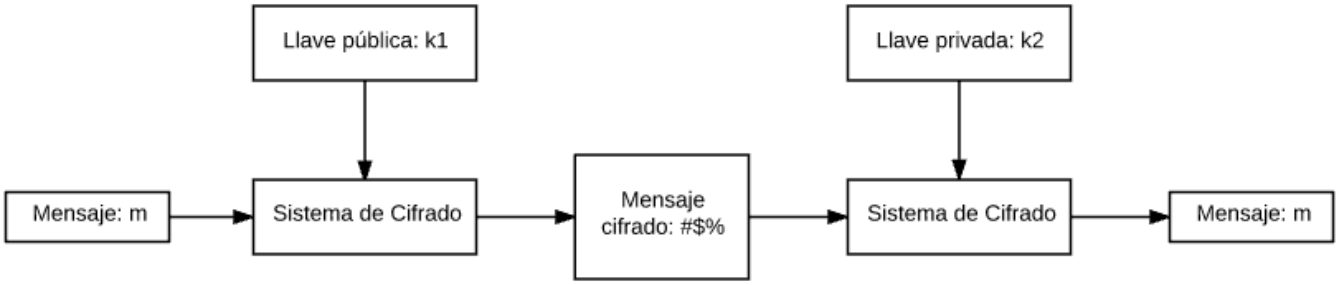
> “El mayor inconveniente de la criptografía simétrica es que esta clave, al ser compartida, ha de ser comunicada de forma segura entre las dos partes de la comunicación (por teléfono, correo certificado, etc.), previamente a ésta. Si este secreto fuese enviado por un canal inseguro, como por ejemplo Internet, la seguridad del sistema sería bastante pobre, dado que cualquiera podría interceptarla y comprometer todo el sistema. También hay que tener en cuenta la frecuencia con la que esta clave debe ser renovada para evitar que sea desvelada”. (Mamani, s.f.)

2.1.3 Cifrado Asimétrico

En los años setenta el matemático Whitfield Diffie y el ingeniero Martin E. Hellman se unieron para desarrollar un nuevo método de distribución de claves criptográficas llamado protocolo Diffie-Hellman, el cual sentó las bases del método asimétrico y son considerados los padres del cifrado moderno y ganaron el premio Turing[3] en el año 2015 por su aporte a la criptografía.

El cifrado asimétrico se diferencia del simétrico, en lugar de usar una llave utiliza dos, una pública y una privada, por lo que no es necesario compartir la llave privada para trasmitir el mensaje; solucionando la desventaja que tiene el método simétrico.

Imagen 2.1.3 Cifrado Asimétrico

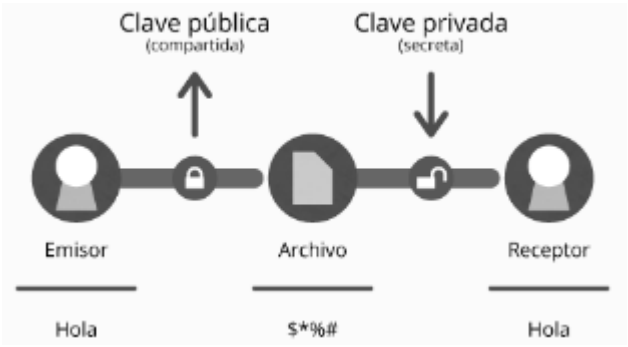


Tomado de (Fuensanta, pág. 12)

[3] http://news.stanford.edu/2016/03/01/turing-hellman-diffie-030116/

La principal ventaja de este tipo de criptosistemas es que la clave secreta ya no tiene que transmitirse entre los interlocutores y tampoco es necesario tener claves diferentes para cada pareja de interlocutores. Es suficiente con que cada usuario tenga su clave doble con componente pública y privada. (Mamani, ¶ 16)

Imagen 2.1.4 Cifrado Asimétrico



Tomado de (Gutiérrez, Tipos de criptografía: simétrica, asimétrica e hibrida, 2013)

Este sistema a diferencia del anterior utiliza dos claves o llaves, una que puede ser transmitida libremente y una secreta que solo el receptor debe conocer; así cuando una persona quiere compartir algo cifrado con otra, usara la clave pública que el receptor le dio para cifrar la información, esta solo podrá ser descifrada con la clave secreta que solo el destinatario conoce.

Sin embargo, tienen el inconveniente de ser más lentos a la hora del proceso de cifrado, “Estos algoritmos tienen la desventaja de que no son tan eficientes a nivel de velocidad como pueden ser los basados en criptografía simétrica” (Mamani, s.f., pág. 19).

2.1.4 Función Hash

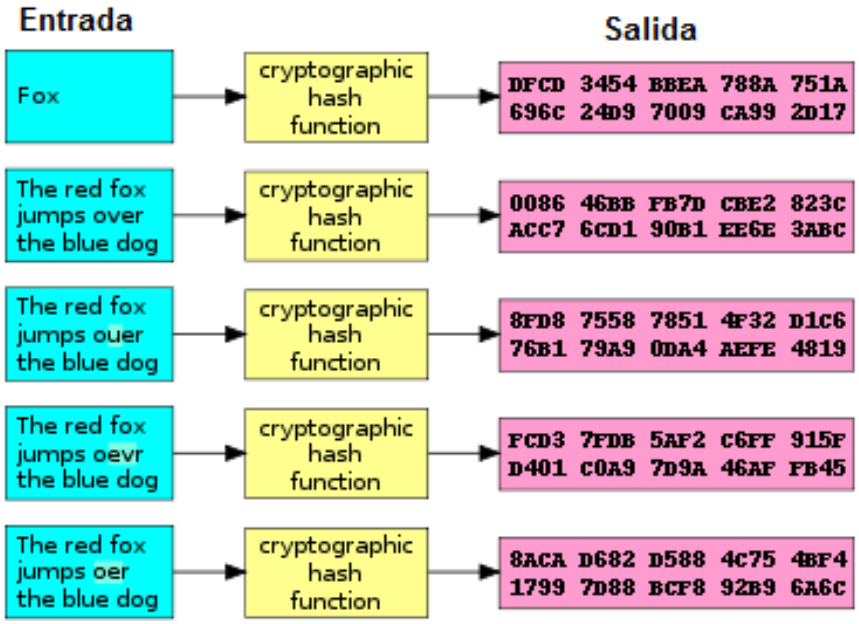
Las funciones hash son:

…algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los

datos de la entrada crea una cadena que *solo* puede volverse a crear con esos mismos datos) (Gutiérrez, GENBETA:DEV, 2013, pág. 1).

Por lo tanto, una función hash es un algoritmo que a partir de una entrada me genera una combinación alfanumérica única, que solo se podrá repetir si se le envía la misma entrada.

Imagen 2.1.5 Función Hash



Tomado de (Gutiérrez, GENBETA:DEV, 2013, pág. 1)

Como se observa en la imagen anterior, la entrada *Fox* genera una salida alfanumérica que oculta el verdadero significado de la entrada, a diferencia del cifrado, una función hash no tiene proceso de descifrar “Estas funciones no tienen el mismo propósito que la criptografía simétrica y asimétrica, tiene varios cometidos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.” (Gutiérrez, GENBETA:DEV, 2013, pág. 1).

Un ejemplo de su uso es cuando se debe guardar una contraseña, asegurando al usuario que no queda un registro legible de la misma o que los

administradores de la BD (base de datos) tienen manera de saber cuál es “Este sistema de criptografía usa algoritmos que aseguran que con la respuesta (o **hash**) nunca se podrá saber cuáles han sido los datos insertados, lo que indica que es una **función unidireccional**” (Gutiérrez, GENBETA:DEV, 2013, pág. 1), esto se logra ya que lo guardado en la BD es el hash generado a partir de la clave, así cuando el usuario vuelve a ingresar la contraseña el sistema la pasa por el hash y el resultado es lo que se compara con el dato guardado, no la contraseña del usuario en sí.

2.1.5 Llaves o claves de acceso

Como se denota anteriormente una parte muy importante de los sistemas criptográficos o de cifrado es el tamaño de la llave utilizada para ocultar la información.

> Para que el sistema sea seguro, es importante que esta clave sea mayor de 40 bits. Este sistema de cifrado tiene la ventaja de que es altamente eficiente, dado que los algoritmos utilizados son muy rápidos al poder implementarse tanto en hardware como en software de una forma fácil (Mamani, s.f.).

Esto quiere decir que mientras mayor sea la clave en bits[4] mayor será la seguridad del cifrado.

> Mientras más larga sea la llave, más segura será. La relación con los algoritmos simétricos no es directa. En este caso, una llave de 1024 bits de RSA es equivalente en seguridad a una de 75 bits de un algoritmo simétrico. (Microsoft)

Según lo mencionado, los sistemas de cifrado simétricos poseen algoritmos criptográficos más eficientes por lo que el tamaño de la llave no debe ser tan largo como en el caso de los sistemas asimétricos, sin embargo, estos sistemas son

[4] Unidad de medición para almacenamiento digital.

más confiables cuando se comparte la llave con varias personas, por lo que se deben usar llaves de mayor tamaño para mantener un nivel de seguridad óptimo.

Es importante mencionar que existen formas de cifrado asimétrico con llaves de menor tamaño, manteniendo un nivel de seguridad igual al de los métodos tradicionales, una de ellas es la criptografía de curva elíptica o ECDSA (*Elliptic Curve Digital Signature Algorithm*). “La criptografía de curva elíptica puede ser más rápida y usar claves más cortas que los métodos antiguos como RSA al tiempo que proporcionan un nivel de seguridad superior” (Preukschat, 2014). Al usar llaves más cortas mejora el tiempo de cifrado y descifrado de los datos.

> El algoritmo ECDSA crea claves de 256 bits de longitud codificados con el sistema de numeración posicional Base58 de Bitcoin que da claves de 44 dígitos sin incluir el número de versión o dígitos de control. Una clave con RSA necesitaría de 350 dígitos. (Preukschat, 2014)

Gracias a su fórmula matemática de creación de llaves, una llave de 256 bits creada mediante ECDSA equivale a una de 2048 bits utilizando un algoritmo RSA con el mismo nivel de seguridad.

También, existen otras formas de cifrado como las firmas digitales, las cuales se definen como:

> Una firma digital es un documento que permite garantizar la integridad de un documento y se puede relacionar de manera única al firmante con su firma, ya que realiza ésta con la llave privada y únicamente el firmante posee esa llave, esto se traduce en que se verifica la autenticidad del firmante. (Paredes, 2006, pág. 13)

Estas combinan el método simétrico y asimétrico obteniendo las ventajas de ambas técnicas, “combinando rapidez del cifrado simétrico con la facilidad de la administración de llaves del cifrado asimétrico”. (Paredes, 2006, pág. 13)

Tal y como puede observarse existen muchas formas de criptografía, todas tienen sus ventajas y desventajas, siempre se deberá tomar en cuenta el algoritmo matemático por utilizar y el tamaño en bits de la llave, mientras más grande sea la misma, más improbable será que un atacante pueda descifrarla.

2.2. La Seguridad de la Información en la Era Moderna

2.2.1. Normas y Estándares

Según la Organización de Estándares Internacionales o ISO por sus siglas en inglés, la información se define como:

> …se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO 27000, 2016, pág. 2).

De acuerdo con lo anterior, se puede definir información como todos aquellos datos guardados y organizados que posea una entidad que tengan valor para la misma, sin importar su origen o forma de transmisión, por lo que dicha organización debería de procurar un adecuado control y protección de los mismos.

> Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización (ISO 27000, pág. 2).

Ya que el correcto manejo, control y aseguramiento de la información ha cobrado relevancia en las organizaciones, se ha visto la necesidad de crear

estándares y normas, guías generales que ayuden a cualquier entidad sin importar su tamaño o negocio para establecer el correcto proceso para este fin.

Existen muchos tipos de estándares para la protección de los datos, dependiendo del tipo de información que estos posean, como los mencionados a continuación:

- PCI DSS[5] (Payment Card Industry Data Security Standard): Estándar de seguridad de datos para la industria de tarjeta de pago.
- HIPAA[6] (Health Insurance Portability and Accountability Act): Estándar de se seguridad para los datos médicos y de salud.
- FERPA[7] (Family Educational Rights and Privacy Act): Estándar estadounidense de seguridad de bases de datos de educación.

Como se puede observar, existen diferentes tipos de estándares, en Costa Rica las normas ISO y Cobit son dos de las más usadas por las organizaciones.

> ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (ISO 27000, pág. 2).

Según la cita anterior la norma ISO 27000 es un conjunto de estándares o guías pensados para la correcta administración de la seguridad de la información. Como otras normas ISO, la serie 27000 consta de un conjunto de estándares numerados, “Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.” (ISO 27000, pág. 3)

[5] https://es.pcisecuritystandards.org/minisite/en/
[6] https://www.hhs.gov/hipaa/
[7] https://ed.gov/policy/gen/guid/fpco/ferpa/index.html

Seguidamente, se detallan los ISO más importantes para los efectos de esta investigación.

La serie **ISO 27001**: “Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información” (ISO 27000, pág. 3), por lo tanto, esta norma es la base para la certificación de un correcto **SGSI** (Sistema de Gestión de la Seguridad de la Información).

La serie **ISO 27002:** “Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.” (ISO 27000, pág. 4) En ella se detallan los instrumentos que pueden ser utilizados para la adecuada administración y medición de los procesos de seguridad de la información. “Está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013” (ISO 27002). Entre sus 14 dominios se encuentra el numero 8 Gestión de Activos el cual tiene como objetivo “que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos” (ISO 27002).

Este dominio define como ejemplos de activos los siguientes:

> Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
>
> Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc. (ISO 27002)

Gracias a esta clasificación, se pueden identificar los activos que deban ser protegidos o que deban tener un trato especial, para ello está el objetivo de control 8.3 Manejo de los soportes de almacenamiento el cual detalla:

> Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.
>
> Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Cifre todos los datos sensibles o valiosos antes de ser transportados (ISO 27002).

Como se menciona en las anteriores citas las buenas prácticas para el manejo de la información clasificada instan a proteger la misma, mediante métodos de cifrado, para ellos ISO 27002 también posee un dominio referente al tema, el número 10. Cifrado “El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad” (ISO 27002). En este sentido, se considera que proteger la información mediante la criptografía es una técnica segura y confiable, este dominio posee el objetivo de control 10.1 Controles criptográficos donde se especifica:

> Las organizaciones deberían utilizarán controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización. (ISO 27002)

En este control se recomienda el uso de herramientas criptográficas para el resguardo de los datos que se consideren importantes para la organización y para lograr lo anterior se proponen los controles 10.1.1 Política de uso de los controles criptográficos y 10.1.2 Gestión de claves.

Políticas de uso de los controles criptográficos: “Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.” (ISO 27002) Deben existir reglamentos que controlen el acceso y el uso de las herramientas criptográficas para una adecuada administración de las mismas.

Gestión de claves: “Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.” (ISO 27002) Las claves de acceso a los sistemas de cifrado deberían ser restringidas y cambiadas periódicamente, “el uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado”. (ISO 27002) Sumado a lo anterior se deben revisar los algoritmos utilizados para cifrar los datos para verificar que cumplan con las medidas de seguridad más actuales posibles.

Se entiende que la información se ha convertido en uno de los activos más importantes de las organizaciones, que han buscado clasificarla y así poder identificar cuáles datos son de mayor relevancia y de mayor valor, mismos que deben ser resguardados, para ello nació la seguridad de la información. “La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización” (ISO 27000, 2016, pág. 3)

De acuerdo con ISO, la confidencialidad, integridad y disponibilidad, son los pilares fundamentales que deben asegurarse para brindar un adecuado proceso de seguridad de la información.

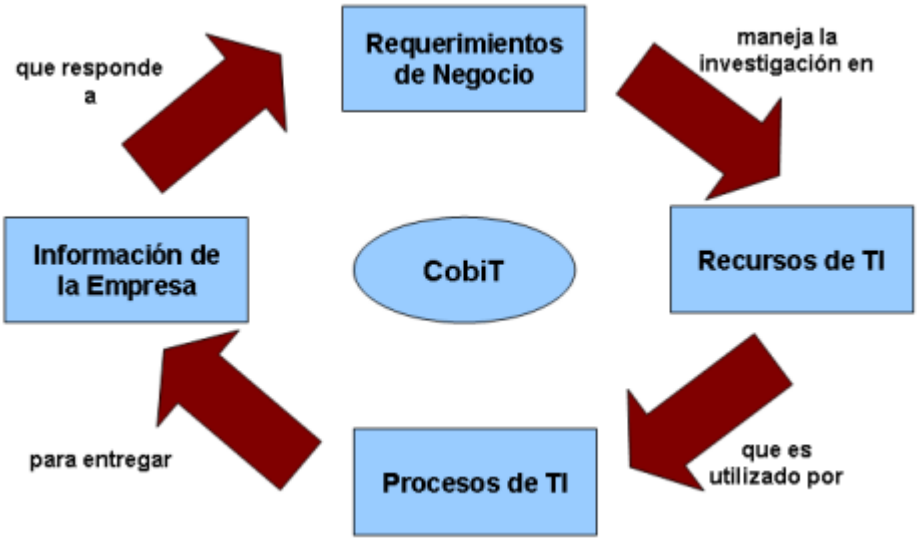
Existen diferentes organizaciones internacionales que han creado estándares, cuyo objetivo es orientar con guías metodológicas a quienes lo

requieran, otro ejemplo es el caso de Cobit, el cual es un marco de trabajo que tiene como misión:

> Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento. (IT Governance Institute, 2007, pág. 13)

Dicho de otra forma, es un estándar que permite administrar los procesos de las áreas como tecnologías de información (TI), de una manera actualizada y acorde con los parámetros internacionales. Una buena razón para su implementación es “el gobierno y los marcos de trabajo de control están siendo parte de las mejores prácticas de la administración de TI y sirven como facilitadores para establecer el gobierno de TI y cumplir con el constante incremento de requerimientos regulatorios” (IT Governance Institute, 2007, pág. 13). Como se expresa en la cita anterior el uso de este marco de trabajo tiene muchas ventajas, incluyendo buenas prácticas a la hora de administrar las áreas de TI y entrar en cumplimiento con entes reguladores como la Contraloría General de la Republica.

Imagen 2.2.1 Principios básicos de COBIT



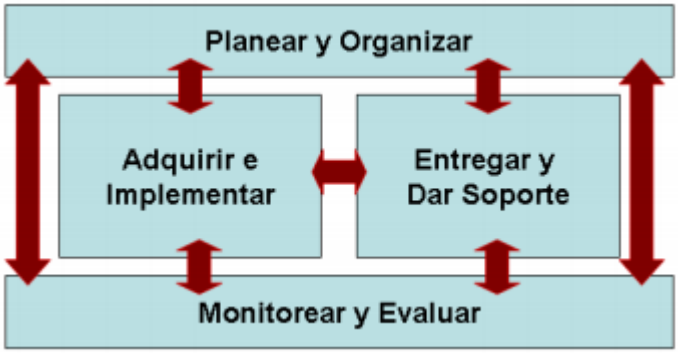
Tomado de (IT Governance Institute, 2007, pág. 14)

Como se observa en la imagen anterior, se puede hacer una idea del funcionamiento de Cobit el cual, identificando las necesidades del negocio, administra los recursos de TI utilizados en sus procesos, para aportar información o valor a la empresa. Cobit establece cuatro dominios principales donde agrupa todas las demás actividades, son los siguientes:

- **Planear y Organizar (PO):** Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI):** Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS):** Recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y Evaluar (ME):** Monitorear todos los procesos para asegurar que se sigue la dirección provista. (IT Governance Institute, 2007, pág. 16)

Cada uno de estos macro procesos se interrelaciona con los demás, ya que sus entradas y salidas son insumos para otros procesos, como se puede observar en la siguiente imagen.

Imagen 2.2.2 Dominios Interrelacionados de Cobit



Tomado de (IT Governance Institute, 2007, pág. 16)

El dominio específico que detalla la seguridad se encuentra en Entregar y dar Soporte (DS), el cual “cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos” (IT Governance Institute, 2007, pág. 17). Como se describe, el DS es el dominio encargado de brindar la plataforma requerida para soportar los servicios de la organización, así como encargarse de su mantenimiento, continuidad y seguridad.

Este dominio se divide en 13 procesos, entre ellos se encuentra el **DS5 Garantizar la Seguridad de los Sistemas**, se supeditan once objetivos de control para tratar con este tema, busca “Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.” (IT Governance Institute, 2007, pág. 117). También aporta métodos de medición como: “el número de incidentes que dañan la reputación con el público, el número de sistemas donde no se cumplen los requerimientos de seguridad, el número de violaciones en la segregación de tareas” (IT Governance Institute, 2007, pág. 117).

Dentro de estos 11 objetivos de control se encuentra el **DS5.8 Administración de Llaves Criptográficas,** el cual se encarga de “determinar que las políticas y procedimientos para organizar la generación, cambio, revocación,

destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas" (IT Governance Institute, 2007, pág. 118). En otras palabras, el DS5.8 indica la necesidad de tener instructivos claros en cuanto al manejo de las claves y métodos de cifrado, para garantizar la seguridad de los datos protegidos por ellos.

Todos estos dominios tienen modelos de madurez que indican el nivel actual de la empresa en dominar el proceso deseado, para el DS5 son los siguientes:

- **0 No existente:** es cuando "la organización no reconoce la necesidad de la seguridad para TI" (IT Governance Institute, 2007, pág. 120) en este caso no hay nada normado en cuanto a seguridad de tecnologías de información.
- **1 Inicial:** es cuando "La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI" (IT Governance Institute, 2007, pág. 120) la empresa reconoce que hay una necesidad de proteger la información, sin embargo no hay un proceso definido del cómo hacerlo.
- **2 Repetible pero Intuitivo:** cuando "Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI." (IT Governance Institute, 2007, pág. 120) se define un proceso y se asignan responsabilidades sobre la seguridad de TI.
- **4 Administrado y Medible:** cuando "Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente, se lleva a cabo un análisis de impacto y de riesgos de seguridad." (IT Governance Institute, 2007, pág. 120) ya existe un claro proceso definido, con políticas y normativa aplicada, además de una mejora continua.
- **5 Optimizado:** cuando "La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los

> objetivos de seguridad del negocio en la corporación.” (IT Governance Institute, 2007, pág. 120) la gerencia general está totalmente comprometida con la seguridad de TI, los usuarios en general están comprometidos, entienden y definen los requerimientos de seguridad.

De acuerdo a autor(es), en Costa Rica como en otros países, las organizaciones que deseen basar sus procesos en Cobit o ISO deben tener los planes de acción y las herramientas adecuadas para cumplir con estos pilares.

2.2.2. Seguridad de la información

Con la creciente actividad delictiva en el sector informático, la seguridad de tecnologías de información forma parte de este gran proceso. Como consecuencia de este aumento, en la delincuencia cibernética, cabe mencionar que las empresas deben prepararse para enfrentar estas amenazas como lo expresa la siguiente cita:

> Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos… (ISO 27000, 2016, pág. 7)

En Costa Rica, las organizaciones se preparan para enfrentar estas amenazas y optan por departamentos y sistemas de seguridad y protección de datos, un ejemplo: “en Costa Rica el Instituto Costarricense de Electricidad tiene un centro de respuesta para la protección de la infraestructura del ICE y de sus clientes…” (Rojas P. , 2014, pág. 2) Las instituciones públicas y privadas deben prepararse y tomar las medidas necesarias para evitar el robo de su información, el gobierno de Costa Rica también ha empezado una reforma en su legislación para incluir estas formas de delito, según se detalla a continuación:

> Las leyes de delitos informáticos deberían ser revisadas permanentemente, hay un problema en cuanto a que, de acuerdo a la tradición costarricense, la tipificación del delito informático va a estar siempre con un retraso enorme frente a la realidad de lo que es ese delito informático (Rojas P. , 2014, pág. 8).

Gracias a este tipo de estándares, las instituciones pueden tener un marco de referencia para el logro de la incorporación del proceso de Seguridad de la Información a sus formas de trabajo; además, preparar su infraestructura y optar por los diferentes métodos para proteger su información, cumpliendo así con las normas de sus entes reguladores (en caso de que se requiera) o simplemente proteger sus valiosos datos de personas ajenas que traten de obtenerlos.

2.3. Una infraestructura tecnológica segura

Cuando se menciona la infraestructura tecnológica se hace referencia a todo producto de hardware[8] o software[9] que se especialice en llevar a cabo las labores habituales de una empresa, en otras palabras, a la infraestructura tecnológica se le representa como, "… los distintos elementos de hardware y software empleados para optimizar la productividad y el funcionamiento de una empresa o entidad y que les facilita la gestión interna, así como mejorar la seguridad de la información." (SIOSA, 2016, pág. 1)

En la actualidad, los bienes en las organizaciones relacionados con el área de tecnologías de información son cada vez más valorados por las compañías, ya que inciden en el rendimiento y efectividad de las labores diarias que ejerce cada uno de los funcionarios; además, se transforma en una garantía para la empresa, asegurando un adecuado funcionamiento de los procesos internos, no obstante, muchas organizaciones a nivel global no se percatan de la importancia de mantener una infraestructura segura.

[8] Se refiere a las partes físicas de un equipo informático.
[9] Se refiere a los componentes lógicos de un equipo informático.

Es por esta razón que el ambiente actual en muchas organizaciones o empresas en materia de infraestructura informática, es el resultado de la acumulación de acciones no racionales o sin destreza para sobrellevar el asunto de la seguridad en la infraestructura a mediano plazo, lo que provoca que muchas empresas no aporten los recursos necesarios para llevar a cabo las labores en la compañía, esto sin duda trae consigo consecuencias en la organización y posiblemente varias de estas infraestructuras acontezcan un riesgo real para la continuidad del negocio.

> "Es fundamental para la organización gestionar adecuadamente la infraestructura tecnológica sobre la cual se sostiene nuestra información: servidores, dispositivos de red, repositorios documentales, aplicaciones de gestión, sistemas de gestión empresarial, etc." (Instituto Nacional de Ciberseguridad de España, pág. 1)

Toda empresa que cuente con equipo tecnológico con el cual trabaja diariamente y lo utiliza para el desarrollo de su negocio, debe contar con una infraestructura tecnológica consolidada, segura y de calidad, esto garantiza seguridad en los procesos, lo que representa productividad y continuidad del negocio.

La infraestructura tecnológica se compone de diversos elementos, entre ellos se pueden mencionar:

- Sistemas operativos: se define como, "Sistema tipo software que controla la computadora y administra los servicios y sus funciones como así también la ejecución de otros programas compatibles con éste." (Alegsa, 2013, pág. 1) Se puede decir que un sistema operativo es el que controla todos los procesos informáticos que ocurren en una computadora y permite ejecutar programas tipo software.

- Software de sistemas: el software es "…todo programa o aplicación programado para realizar tareas específicas." (Alegsa, 2013) Un software es todo programa que se ejecuta en la computadora y que nos facilita la ejecución de tareas.
- Bases de datos: "Una base de datos es un "almacén" que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente." (Valdés, 2007) Las bases de datos nos permiten almacenar mucha información y ésta puede ser accedida por diferentes medios para que pueda ser utilizada por diferentes usuarios.
- Servidores de aplicaciones: "Un servidor de aplicaciones es el elemento (software) que es capaz de traducir las instrucciones y además comunicar con otros servidores (como por ejemplo los servidores de bases de datos) para extraer información de la empresa que se necesita para resolver la petición." (Asenjo, 2012) Un servidor de aplicación como anteriormente se menciona, funciona para extraer la información necesaria que el usuario solicita, esto lo realiza por medio de un componente software que traduce la petición del usuario y le devuelve el resultado esperado.
- Redes e instalaciones de comunicación (internet e intranet) : "Una red es la unión de dos o más ordenadores de manera que sean capaces de compartir recursos, ficheros, directorios, discos, impresoras..." (Bueno, 2016, pág. 2) Una red de comunicación sirve para interconectar diferentes elementos de hardware para que por medio de esta comunicación los ordenadores puedan interactuar entre sí y obtener el resultado esperado por parte de los usuarios.

El objetivo principal de contar con una infraestructura informática segura y de buena calidad, es que esta no se convierta a un mediano plazo en un impedimento para el correcto devenir de información para las actividades diarias en las organizaciones. Se debe contar con soluciones y procedimientos que

ofrezcan una colaboración segura, para enriquecer la infraestructura de las organizaciones, de manera que como principal objetivo se goce de los mecanismos necesarios para realizar las labores cotidianas, sin tener que preocuparse por la seguridad que se le brinda a los clientes o personas relacionadas a los resultados que ofrece una entidad.

Una adecuada infraestructura, asegura un correcto funcionamiento de los recursos con los que cuenta una organización e incide considerablemente en la seguridad y en el nivel de los datos que se implemente en la misma; por esta razón es importante contar con un equipo de infraestructura adecuado y gestionado, que permita su máximo aprovechamiento.

Debido a la gran cantidad de información acerca de la importancia de una infraestructura segura para todo ambiente laboral, gran parte de las empresas están cada día más conscientes de los beneficios que les proporciona contar con infraestructuras de calidad. Con el propósito de adquirir aumento en los beneficios y un mayor aprovechamiento de los recursos con los que disponen a nivel empresarial, surgen diferentes recomendaciones respecto de las características de infraestructura con las que debe contar toda organización. Las siguientes son recomendaciones descritas por Rodrigo Ferrer (Ferrer, 2014, pág. 1) donde se mencionan los lineamientos a seguir en cuanto a una adecuada infraestructura:

- *Firewall* o Tecnología de *packet filtering* (filtrado de paquetes) o Tecnologías *stateful* (comprobación de estado de conexión) o DPI (*Deep Packet Inspection* - inspección profunda de los paquetes) o Firewall de nivel de aplicación (proxy).
- IDS (sistemas de detección de intrusos) o Gestión adecuada de los reportes e informes.
- IPS (sistemas de prevención contra intrusos).
- Servidores o Sistema operativo asegurado (*Hardening*) o Fuentes de poder redundante o Sistemas de discos duros confiables (Ej. RAID).

- Antivirus y gateway antivirus o Actualizable dinámicamente o Amplia base de datos.
- Antispyware o Actualizable dinámicamente o Amplia base de datos.

Sumado a los aspectos mencionados anteriormente, existen otros objetivos que se buscan para mantener un control de la seguridad infraestructural de la compañía, entre ellos se cuenta con:

- Gestión y vigilancia de los activos: se busca el control y el mantenimiento diario y frecuente de los activos con los que cuenta la empresa, entre ellos: servidores, dispositivos de red.
- Seguridad de la información: resguardar y asegurar la información en la empresa por medio de roles a los usuarios y autorizaciones consentidas.
- Protección de los sistemas: asegurarse de contar con el recurso humano y tecnológico adecuado para cumplir a cabalidad con la tarea de mantener la información a salvo de terceras personas que no estén autorizadas sobre la misma.

Además de los objetivos mencionados anteriormente, los servidores de bases de datos son una parte muy importante para mantener la infraestructura en condiciones óptimas: “Un servidor de bases de datos se utiliza para almacenar, recuperar y administrar los datos de una base de datos.” (Turner, 2014) Es decir, permiten organizar la información en tablas relacionadas en bases de datos y tener acceso a la misma. Es necesario darle mantenimiento regular a los equipos que se utilizan como servidores de bases de datos.

2.3.1. Bases de Datos

La necesidad del almacenamiento de grandes volúmenes de datos es el motivo por el que surgen los servidores de bases de datos, entre los cuales se puede mencionar:

- MySQL Server: este consiste en una base de datos de código abierto (gratis).
- PostgreSQL server: también pertenece a las bases de datos de código abierto.
- MariaDB: es otro sistema de gestión de base de datos originario de MySQL.
- SQL Server
- Oracle

Un servidor de base de datos se encarga de realizar las actualizaciones de los datos, además, permite el acceso a la información de sus bases de datos a uno o muchos usuarios a la vez, como por ejemplo cuando los usuarios acceden una página web, un usuario puede ver la información alojada en el sitio al mismo tiempo que otros usuarios también lo hacen.

Otro punto importante por tomar en cuenta con respecto al sistema gestor de bases de datos en adelante (SGBD), es el tamaño adecuado que este debe tener. Este tamaño dependerá del uso que se le va a dar a los datos y del tamaño de la base de datos que se utiliza, entre otros aspectos que a continuación se mencionan:

- Realizar una valoración del rendimiento que posee la base de datos.
- Revisar el espacio que se posee en la base de datos.
- Asegurar que la memoria RAM sea suficiente para el servidor que se eligió.

Los SGBD albergan todo tipo de información importante y sensible en las compañías, es por esta razón que manejar una adecuada gestión de la infraestructura que se utiliza y mantener en correcto funcionamiento de las bases de datos, es idóneo para conservar un balance entre el costo y el beneficio que se obtiene.

Como se ha comentado en los capítulos anteriores, la información que se encuentra almacenada en las bases de datos de toda empresa es fundamental para la continuidad del negocio, al ser éste un activo imprescindible. Uno de los mecanismos para mantener esta información segura es el cifrado de los datos, ya que proporciona los mecanismos fundamentales y esenciales para conservarla y protegerla de muchos tipos de delitos informáticos que pueden causar daños a la misma.

2.4. Seguridad de la Información en un Entorno Universitario

Actualmente, mucha de la información de las instituciones se considera como un activo valioso, esto incluye a las universidades, ya que las mismas guardan mucha información personal tanto de alumnos como de su personal docente y administrativo. Sumado a esto se debe considerar el apoyo que brindan los sistemas de datos a los procesos críticos de las entidades, por lo que se requiere un mayor control y administración de la información, complementado con estrategias de alto nivel que lo permitan.

En numerosas universidades a nivel internacional, se puede encontrar que en su gran mayoría poseen políticas bien establecidas sobre la seguridad en la información que manejan, esto se debe a que albergan muchos datos sensibles de los usuarios. Como ejemplo de esto, la siguiente cita expone la política de seguridad que aplican en una de las universidades de Colombia:

> Con la promulgación de la presente Política de Seguridad de la Información la Universidad Distrital Francisco José de Caldas formaliza su compromiso con el proceso de gestión responsable de la información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo… (Universidad Distrital Francisco José de Caldas, pág. 1)

Los centros universitarios de distintos países implementan diversidad de políticas y procesos para la protección de sus fuentes de información, realidad de la que no escapan las instituciones universitarias de Costa Rica, “Actualmente las entidades del Estado, instituciones financieras, centros de enseñanzas, instituciones de salud y empresas privadas, entre otros, acumulan una gran cantidad de información sobre sus empleados, clientes, productos y servicios; que son fundamentales para su organización” (MINAET, 2011, pág. 9).

Como consecuencia, en Costa Rica se ha desarrollado todo un estándar para ayudar en la protección de los datos. Estos estándares surgen de parte de varias instituciones a nivel costarricense que ayudan a controlar y regir las Tecnologías de la Información y de las Comunicaciones, en adelante las TIC. Las TIC se refiere al: “conjunto de avances tecnológicos que proporciona la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, Internet, la telefonía, los “mass media”, las aplicaciones multimedia y la realidad virtual.” (Álvarez, 2008, pág. 2) Es decir, se refiere a toda la tecnología que es utilizada para realizar los procesos habituales en las instituciones.

A continuación, se realiza la descripción de algunas de las instituciones que regulan las TIC en Costa Rica:

- Instituto de Normas Técnicas de Costa Rica (INTECO). INTECO por sus siglas se define como:

El Instituto de Normas Técnicas de Costa Rica (INTECO) es una asociación privada, sin fines de lucro, con personería jurídica y patrimonio propio. Creada en 1987, en el año 1995 fue reconocida, por decreto ejecutivo, como el Ente Nacional de Normalización. (INTECO, 2015).

Esta institución se encarga de fomentar y motivar a las distintas instituciones de Costa Rica a que realicen procesos de certificación a nivel

internacional, además elabora normas para mantener un equilibrio socio-económico en el país.

"…el Instituto de Normas Técnicas de Costa Rica (INTECO) ha realizado la emisión del estándar ISO/IEC 27000, desarrollando la norma INTE-ISO/IEC 27000:2010" (MINAET, 2011, pág. 10) Esta norma se basa en los estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y contiene las mejores prácticas que se recomiendan en materia de seguridad de la información.

- Contraloría General de la República (CGR)

La Contraloría General de la República, es la institución encargada de regular y controlar el uso que se le da a los recursos públicos de los que hacen uso diferentes instituciones del estado costarricense. La CGR, también dicta normas en distintos ámbitos y sectores laborales.

Existen normas dictadas por la Contraloría General de la Republica que hacen mención del resguardo de los datos y la información de las organizaciones, por ejemplo: con la resolución "Normas Técnicas para la Gestión y Control de las Tecnologías de Información (N-2-2007-CO-DFOE)", emitida el 7 de junio del 2007 en el diario oficial La Gaceta No. 119 del 21 de junio 2007, dicha norma "…se basa en algunos elementos de los estándares COBIT y el estándar internacional ISO 27001, relacionado con la seguridad de la información" (MINAET, 2011, pág. 13) Esta norma incorpora entre sus elementos el estándar ISO 27001, dicho estándar tiene como objetivo "proporcionar una metodología universal para la implementación, administración y mantenimiento de la seguridad de la información dentro de una organización" (Lign).

Como se menciona, dicho estándar procura incorporar un esquema igual en todas las organizaciones, con el fin de que la gestión administrativa y el mantenimiento de la seguridad de la información, se maneje de la misma forma en

diferentes sectores que se dediquen a labores que involucran información importante para sus clientes.

- Ley No. 8968 Protección de la persona frente al tratamiento de sus datos personales. Esta ley tiene el siguiente objetivo:

> Garantizar a 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 (Tribunal Supremo de Elecciones, 2011, pág. 1).

En resumen, esta ley procura que se respeten los derechos y la información privada de las personas que se encuentran en bases de datos o en algún depósito manual con el que cuenten para mantener almacenada la misma.

La Ley No. 8968. Protección de la persona frente al tratamiento de sus datos personales, Capitulo III, Artículo 14, ‘Trasferencia de Datos Personales, Regla General’, expone sobre la forma en que se deben transferir los datos por parte de los encargados de las bases de datos.

> Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley (Tribunal Supremo de Elecciones, 2011, pág. 12).

Además, esta ley expone sobre la función que cumple la PRODHAB ligada a dicha ley en el capítulo IV Agencia de Protección de Datos de los Habitantes (PRODHAB), sección I Disposiciones Generales.

> Se crea adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los habitantes (Prodhab). Con personalidad jurídica instrumental, la administración de sus recursos y presupuesto, podrá suscribir contratos y convenios que requiera para el cumplimiento de sus funciones (Asamblea Legislativa de la Republica de Costa Rica, 2011).

La PRODHAB tiene la potestad de acceder a los documentos y contratos que necesite para cumplir a cabalidad con las funciones que tiene como institución.

- Agencia de Protección de Datos de los Habitantes (PRODHAB)

La PRODHAB, es una institución que se encarga de

> ...garantizar a 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. (Agencia de Protección de Datos de los Habitantes)

Se puede observar que, la PRODHAB se encarga básicamente del respecto por la información privada y valiosa de las personas, muy similar al objetivo que protege la Ley No. 8968 de Protección de los datos personales.

- Ministerio de Ciencia y Tecnología (MICIT)

El MICIT se encarga de ejecutar las políticas relacionadas con la ciencia, la tecnología y la innovación.

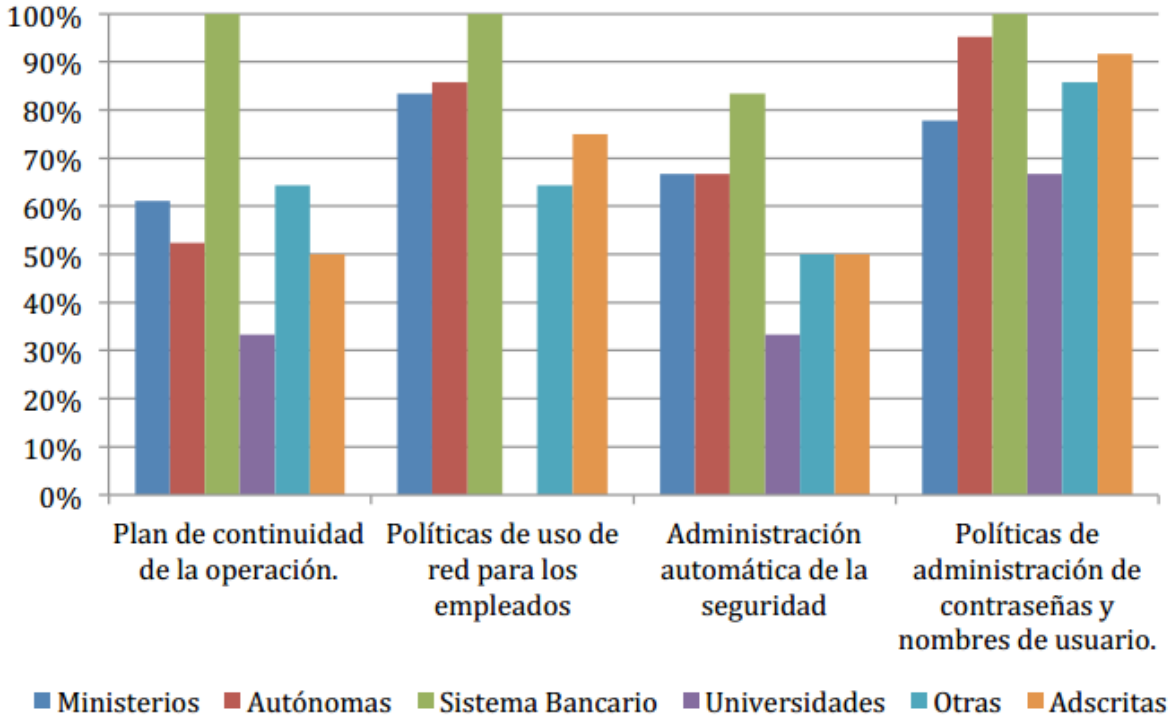
Como se ha comentado anteriormente, Costa Rica ha experimentado un gran cambio debido a la creciente era tecnológica, como consecuencia, se han definido diferentes tipos de políticas en seguridad de los datos. Entre estos

cambios, se han firmado acuerdos con otros países para contar con una mayor seguridad en cuanto al tratamiento y la gestión que se le da a la información utilizada en las instituciones del estado. A manera de complemento a estas políticas planteadas, en el marco legal en materia de seguridad de la información, se firmó un acuerdo que se describe en la siguiente noticia, “Costa Rica firma acuerdo de entendimiento sobre seguridad cibernética con Corea” (MICIT, 2015). Este acuerdo de entendimiento está conformado por:

- Centro de Atención a Incidentes de Seguridad Informática -CSIRT-CR; creado por Decreto Ejecutivo nº 37052-MICIT.
- Ley de Protección de la Persona frente al tratamiento de sus Datos Personales (Nº 8968) y su Reglamento.
- Agencia de Protección de Datos de los Habitantes (Prodhab).
- Ley N° 9048 Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos informáticos y conexos, del Título VII del Código Penal.
- La Contraloría General de la República emite en el 2007 las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información. Publicado en la Gaceta 119 del 21 de junio del 2007.

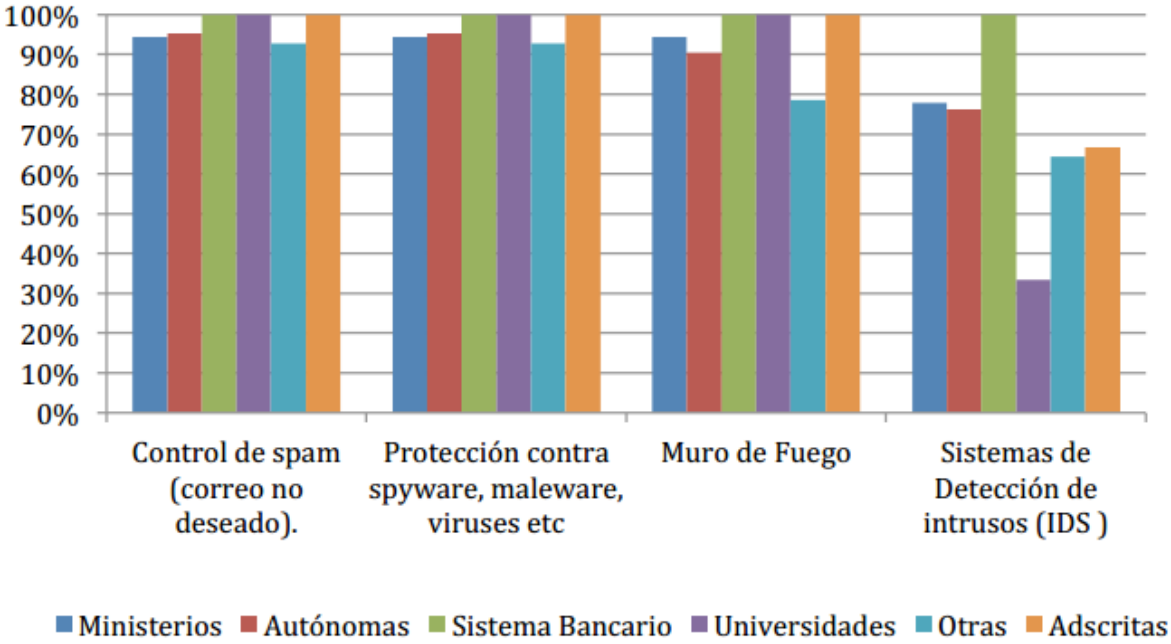
En respuesta a los ataques y las normas establecidas, las instituciones han tomado medidas de seguridad física y lógica para resguardar sus sistemas de información, como se observa en los siguientes gráficos:

Gráfico 4.1. Porcentaje de Instituciones que implementaron elementos informáticos en sus redes. (Planes y políticas)



Tomado de (MINAET, 2011, pág. 33)

Gráfico 4.2. Porcentaje de Instituciones que implementaron elementos informáticos en sus redes. (Infraestructura y programas)



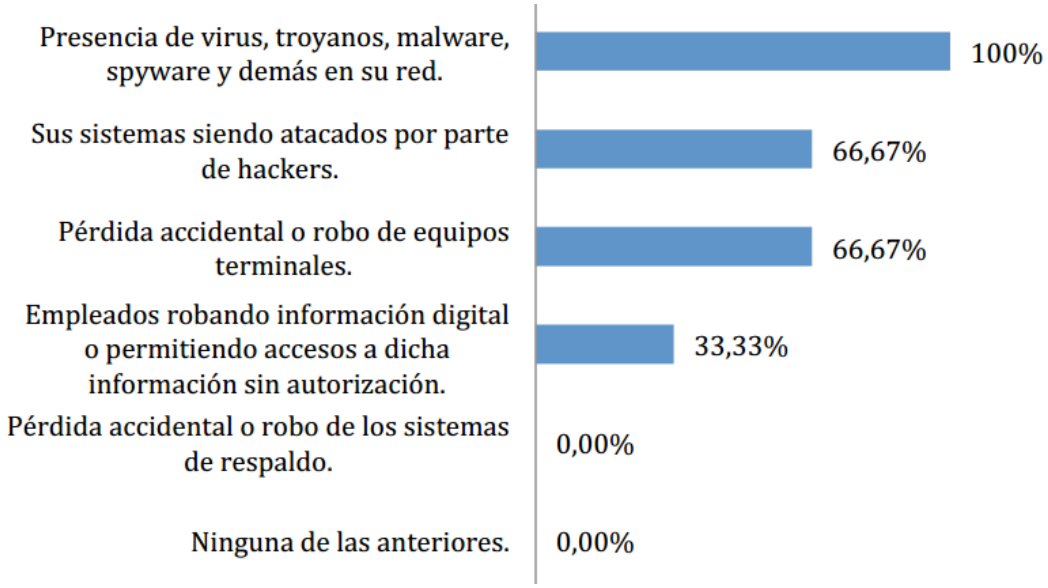
Tomado de (MINAET, 2011, pág. 34)

> “Dentro de las instituciones que presentaron mayor implementación de estas herramientas, se encuentran las correspondientes al sistema bancario y las universidades” (MINAET, 2011, pág. 34).

Esta cita concuerda con lo presentado en la información del gráfico anterior, donde las universidades y las instituciones bancarias presentaban gran porcentaje de implementación en sistemas de protección contra virus, troyanos, malware, spyware, etc.

Todo esto fundamentado en el incremento de incidentes de seguridad informática, para el presente caso se enfocará en los desplegados en las universidades, como se pueden observar a continuación:

Gráfico 4.3. Eventos informáticos registrados en las Universidades



Tomado de (MINAET, 2011, pág. 30)

En esta línea, se puede afirmar que las universidades son víctimas de ataques cada vez más especializados, por lo que es su responsabilidad es buscar las mejores prácticas en seguridad para proteger su información, contar con adecuados controles de acceso, roles y perfiles bien definidos, además sus

repositorios de información privada debidamente cifrados. Además de cumplir con las diferentes regulaciones que le competen, como se menciona en los siguientes enunciados:

- De conformidad el Transitorio I de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, N° 8968, las personas físicas o jurídicas, públicas o privadas propietarias o administradoras de bases de datos, deberán adecuar sus procedimientos y reglas de actuación, a lo establecido en la presente ley, en un plazo máximo de un año a partir de la creación de la Agencia de protección de Datos de los Habitantes, en adelante PRODHAB.
- La (PRODHAB), como ente adscrito al Ministerio de Justicia y Paz, entró en funcionamiento el 5 de marzo del 2013 con la vigencia del Reglamento a la Ley N° 8968. en virtud de que el año establecido en el Transitorio I anteriormente citado concluye en fecha 5 de marzo del año 2014, se recuerda a los responsables de bases de datos sujetas a dicha normativa, la obligatoriedad de proceder a su inscripción y elaboración de protocolos para la seguridad de esos ficheros. Requisitos indispensables para que las bases de datos puedan operar legalmente. (PRODHAB, 2014)

Se destaca la importancia que la protección de las bases de datos tiene en esta era digital, el resguardo de los repositorios de información es fundamental en la lucha contra el crimen cibernético. De acuerdo con lo normado por la PROHAB las Universidades deben adecuar su infraestructura y procesos para cumplir con estas directrices y así garantizarles a las personas que su información está debidamente protegida contra aquellos que quieran usarla con fines delictivos.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo de Investigación

En este apartado se buscará informar al lector sobre la metodología utilizada durante la creación de esta investigación, tomando en cuenta factores como: su tipo, fuentes de información y enfoque, entre otros y así dar una idea clara de su desarrollo.

El tipo de investigación por desarrollar será de carácter descriptivo, la cual es “aquella en que, como afirma Salkind (1998), “se reseñan las características o rasgos de la situación o fenómeno objeto de estudio” (p. 11)” (Torres, 2010, pág. 113).

Por lo tanto, consiste en la descripción de los datos con el fin de conocer situaciones que predominan desde la representación exacta de las actividades o procesos, ya que “una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de ese objeto” (Torres, 2010, pág. 113).

Basado en lo anterior, se buscará información sobre rasgos, cualidades, atributos, fortalezas y debilidades de los métodos de cifrado utilizados en el aseguramiento de la información en las bases de datos.

Además, esta investigación también será de tipo documental. Este tipo de investigación “consiste en un análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto al tema objeto de estudio” (Torres, 2010, pág. 111)

Por consiguiente, se examinará la información recolectada de distintas fuentes (bibliográficas, revistas, entrevistas y otras), para su posterior estudio y así realizar el análisis requerido.

Basándose en los elementos antes mencionados, se desarrolla una investigación de tipo descriptivo/documental que buscará la identificación de las mejores cualidades de los métodos de cifrado, objeto de estudio en este documento.

3.2. Tipo de Enfoque

El tipo de enfoque a desarrollar será de tipo mixto, el cual es un proceso que "… recolecta, analiza y vincula datos cuantitativos y cualitativos en un mismo estudio, en una serie de investigaciones para responder a un planteamiento del problema, o para responder a preguntas de investigación de un planteamiento del problema" (Universidad Nacional Abierta y a Distancia).

El enfoque de esta investigación será de este tipo, ya que se analizarán los distintos métodos de cifrado y a su vez se comparará la forma de cifrar la información de cada uno, el método de distribución de las llaves de cifrado y descifrado, ambos datos cualitativos y la velocidad con la que realizan el proceso, el cual es un dato cuantitativo.

Lo anterior, para establecer medidas de desempeño y probar la teoría, tomando en cuenta las buenas prácticas y lograr el establecimiento de un estándar funcional en la gestión de aseguramiento de la información.

3.3. Sujetos y Fuentes de Información

3.3.1. Sujetos de investigación

El sujeto de la investigación "Es el individuo que asume el papel de investigador, que se adentra en el conocimiento comprensión y estudio de los objetos, fenómenos y procesos de la naturaleza y de la sociedad" (Instituto de Investigaciones Ambientales).

La investigación centrará su unidad de análisis en la Dirección de Gestión de Tecnologías de la Información de la Universidad Técnica Nacional, ya que ahí se encuentra centralizada la información de los servidores de bases de datos.

Para ello, se considera que las siguientes personas podrían ser consideradas como fuentes de información:

UTN	Contacto	Rol
Dirección de Gestión de TI	Luis Diego Fernández González	Técnico
Administración de las Bases de datos	David Villalobos C	Técnico
Administración de Servidores	Sergio Quesada Espinoza	Técnico
Jefe de Gestión Estratégica	Wilmer Vindas	Técnico
Asesoría Jurídica	Jonathan Morales	Legal
Registro Universitario	Silvia Murillo Herrera	Dueño de datos
Dirección del Talento Humano	Julio González Salazar	Dueño de datos

3.3.2. Fuentes de información

“Se denominan fuentes de información a diversos tipos de documentos que contienen datos útiles para satisfacer una demanda de información o conocimiento” (Biblioteca Universidad de Alcalá).

Como fuente primaria de información se tendrá a especialistas en el país, como el PhD. Hugo Solís Sánchez quien posee un Doctorado en Computación e Informática, Máster en Física de la UCR y con vasta experiencia en investigaciones criptográficas; tiene estudios y publicaciones en internet de los principales proveedores de seguridad como Kaspersky©, McAffee© y Symantec©; en páginas especializadas de seguridad informática, como el Equipo de Respuesta ante Emergencias Informáticas (CERT). Se consultará estudios de las principales firmas de seguridad en materia de soluciones de cifrado.

3.4. Población y Tratamiento de la Información

"La población es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado" (Wigodski, 2010).

La población para esta investigación serán los colaboradores de la UTN del área de TI, ya que se entrevistará al personal encargado de la información, su tratamiento y administración.

Tratamiento de la información son "las operaciones que las personas ejecutan con la información" (Andres, 2010).

La información será tratada de forma analítica, procesando los datos recolectados para ver cuales cumplen de la mejor manera con las necesidades de la UTN a la hora de elaborar el estándar de cifrado.

3.5. Matriz Metodológica

Objetivo Especifico	**Variable**	**Definición conceptual**	**Dimensiones**	**Definición operacional**	**Definición instrumental**
Identificar los métodos de cifrado óptimos y las buenas prácticas del proceso de cifrado de datos mediante la revisión de los que se utilizan en la actualidad, para el desempeño de las bases de datos y su posterior aplicación en la Universidad.	Tipos de cifrado. Buenas prácticas en el proceso de cifrado. Desempeño de bases de datos.	Los tipos de cifrado, se refiere a las formas que se utilicen para implementar el cifrado de la información, ya sea simétrico o asimétrico. Incluyen las formas más recomendadas de implementar el cifrado para resguardar la información. Es el	Forma de uso del cifrado simétrico y del cifrado asimétrico. Utilización de las prácticas más recomendadas y utilizadas en el área de tecnologías. Hacer uso de las bases de datos, modificando su implementación sin que esto	Tiempo de duración / 1 GB./Min/Seg (cifrado y descifrado). Prácticas de cifrado y descifrado según la de base de datos y el tamaño de la misma. Bases de datos (tipos) comportamiento, utilización, desempeño, velocidad de	Entrevista a expertos. Análisis de los documentos técnicos de desempeño de los tipos de cifrado. Investigación en diferentes documentos acerca de las prácticas más utilizadas en cifrado. Entrevista al

Objetivo Especifico	Variable	Definición conceptual	Dimensiones	Definición operacional	Definición instrumental
		rendimiento que posee la base de datos a la hora de hacer transacciones.	implique una afectación en las mismas.	lectura y escritura.	personal técnico acerca de las bases de datos de la Universidad.
Determinar el método y la mejor práctica relacionada al cifrado con la información identificada, que se adapte a las necesidades de protección de datos de la Universidad.	Protección de datos. Forma de implementación en bases de datos.	Forma en que se protegen los datos considerando robustez y desempeño. Impacto en el rendimiento de la base de datos, rendimiento e implementación.	Llaves criptográficas. Tipo de base de datos con la que se vaya a trabajar para el cifrado de la información.	Llaves simétricas, asimétricas. Tamaño de la llave, bits. Algoritmos (128, 512, etc.) MySQL/MariaDB, sql-servers y postgre-sql, su capacidad de almacenamiento, rendimiento por plataforma, técnicas posibles en cada BD.	Entrevistas (expertos, personal técnico). Cuestionarios, lista de cotejo. Documentos técnicos.
Examinar las ventajas de seguridad en la información y datos de los métodos escogidos, comparando la protección actual con las mejoras que se obtendrían con este nuevo procedimiento, logrando con ello un incremento en la seguridad de los datos.	Seguridad de la información. Nivel de protección de los datos.	Se refiere al uso apropiado de las tecnologías para el cuido y resguardo de la información en las bases de datos. Es la categoría de cuido y protección que posee un dato, según los intereses de la organización.	Controles de acceso. Datos categorizados como confidenciales.	Roles, privilegios, autorizaciones, etc.) Usuarios dueños de los datos. Datos sin cifrar, datos cifrados. Utilización de los datos.	Entrevistas (expertos, personal técnico, dueños de los datos). Análisis de los documentos técnicos de desempeño de los tipos de cifrado.

Objetivo Especifico	Variable	Definición conceptual	Dimensiones	Definición operacional	Definición instrumental
Analizar las condiciones de la infraestructura universitaria, para el aseguramiento y el resguardo de información importante, mediante el aprovechamiento del estándar sugerido.	Estado de los servidores. Tipo de bases de datos. Estado de la red. Controles de acceso.	Estado en que se encuentran actualmente los equipos de la institución. Bases de datos con los que trabaja la institución. Estado en que se encuentra la red de la institución. Controles para acceder a los datos con los que cuente la UTN.	Servidores de bases de datos. Tipos de bases de datos. Estado de la red. Tipos de controles de acceso.	Capacidades técnicas del servidor de base de datos. Conocimiento de los tipos de base de datos que utilizan. Conocimiento del estado de la red. Controles de acceso a tomar en cuenta ante cualquier cambio que surja.	Entrevistas al personal técnico de la UTN. Análisis de documentos técnicos referentes al tema.
Proponer un estándar de cifrado para la Universidad Técnica Nacional, por medio de una guía técnica y metodológica que permita el cumplimento con lo establecido en la legislación vigente.	Nivel de cumplimiento. Guía técnica y metodológica.	Verificar que el estándar cumpla con lo requerido por la Ley 8968. Guía técnica y metodológica con las especificaciones necesarias para la implementación del estándar.	Protección de los datos confidenciales. Documento guía para la implementación del estándar de cifrado.	Nivel de seguridad actual sin cifrar. Nivel de seguridad cifrado. Requerimientos necesarios para poder elaborar el documento guía para el estándar de cifrado.	Entrevistas al personal técnico de la UTN y expertos en la materia. Análisis de documentos técnicos referentes al tema.

3.6. Técnicas de recolectar información

Se utilizarán las siguientes técnicas de recolección de información:

3.6.1. Internet: Se buscará información en sitios especializados en seguridad como Kaspersky©, McAffee©, Symantec©, CERT, artículos, noticias, entre otros, en formato digital, ya que la información es de más fácil acceso y está en constante actualización.

3.6.2. Análisis de documentos: Se analizarán documentos referentes al tema, como artículos, informes, tesis u otras fuentes de información impresa tales como Criptografía: historia de la escritura cifrada, Una introducción a la Criptografía Clásica, Estado de Seguridad Informática en el sector público costarricense, Advances in Cryptology-Eurocrypt 2000, esto con el fin de entender e identificar los diferentes métodos de cifrado y sus distintos usos.

3.6.3. Entrevista: se tendrá contacto con expertos en cifrado que se encuentren en el país. Se entrevistará a especialistas en el área dentro del país, como el PhD. Hugo Solís Sánchez, ya sea personalmente o por correo.

CAPÍTULO IV: ANÁLISIS SITUACIONAL

4.1. UTN, Normativa y Aspectos Legales en Materia de Protección de la Información

Como parte de las entrevistas realizadas al personal de la Universidad Técnica Nacional (UTN) en los meses de julio y agosto de 2016, se ha recolectado información sobre las directrices y leyes con las que debe cumplir la Universidad.

En materia de aspectos legales, la información relacionada con la seguridad de la información es muy básica, los encargados del Departamento de Gestión de Tecnologías de Información tienen identificadas las leyes que deben cumplir. Entre ellas la que compete es la **Ley 8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales**, actualmente se está trabajando en el desarrollo de la normativa y los procesos necesarios para seguir con lo solicitado en las leyes, como los siguientes:

- DGTI-3300010: “Control y Seguimiento de Seguridad de la Información” creado el 15 de junio de 2016.
- DGTI-DZ-07: “Comité de Seguridad de la Información” creado el 15 de junio de 2016.
- DGTI-EA-0116: “Esquema de Clasificación de la Información” creado el 15 de junio de 2016.

Ah finales del 2016, los entes reguladores no han fijado una fecha límite para cumplir con lo dictado por la ley, situación que provoca que el avance de esta nueva normativa no se desarrolle de una forma rápida. Afortunadamente, ya se estableció el área de Seguridad de la Información a cargo del área estratégica de TI, la cual todavía no tiene un encargado asignado.

4.2. UTN, Manejo de los Datos y Seguridad

Como resultado de diferentes entrevistas realizadas al personal de la Universidad Técnica Nacional en los meses de julio y agosto de 2016, se logra la

recolección de información vital y necesaria para la investigación. A continuación, se resume la información obtenida durante dicho proceso.

En Julio del 2015, la UTN hizo oficial la creación de un área de Seguridad de la Información, con el fin de velar por la seguridad de los datos de la institución.

Según el cuestionario entregado por el área de Gestión Estratégica de TI en el mes de agosto de 2016, las siguientes son funciones que se tienen identificadas que deberá desempeñar dicha área:

- Coordinar la seguridad de la información y de la infraestructura de TI, aplicando las normativas y estándares existentes, guiando a la misma en la implementación de políticas de seguridad y en la implementación de controles de seguridad y el Sistema de Gestión de Seguridad de la Información, alineando las actividades programadas en el marco de los estándares existentes y aplicables.
- Velar por el correcto mantenimiento del plan de continuidad del negocio.
- Generar políticas y controles de seguridad aplicando las normativas y estándares existentes.
- Monitorear el cumplimiento de políticas y controles de seguridad y auditar el cumplimiento de las normativas, gestionando acciones preventivas y correctivas de las no conformidades que se observen.
- Vigilar el tratamiento a los incidentes y riesgos para garantizar la continuidad del negocio, protegiendo los activos críticos.
- Definir las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como criptografía, modelos formales, análisis forense, así como en las áreas en las que la seguridad informática tiene su aplicación: redes, telecomunicaciones, sistemas operativos, aplicaciones y otros.
- Ajustar el marco de seguridad de la información a los estándares existentes (ISO 27000, COBIT, otros).

- Realizar cualquier otra actividad enmarcada dentro del manual descriptivo de puestos atinente a su cargo.

Además, la Universidad cuenta con planes de contingencia en caso de que se materialice un evento adverso que ponga en peligro la información sensible de la Universidad, contrariamente la misma no posee planes de acción para evitar este tipo de situaciones; sin embargo, consideran que el cifrado ayudaría de gran manera a mantener la confidencialidad de la información, por lo cual se está estudiando el tema.

En materia del manejo de los datos e información sensible, la Universidad Técnica Nacional ha comenzado a hacer uso de formularios donde se solicita la aprobación para el uso de su información a los estudiantes y un proceso de clasificación de información; el cual es muy importante, debido a que dará como resultado el conocimiento de las bases de datos que poseen información que debe ser protegida.

Actualmente, se tienen identificadas algunas bases de datos con este tipo de información sensible, pero no se tienen oficializados los dueños de estos datos. Una vez las bases de datos cumplan con los requisitos de la Ley No. 8968 de protección de datos personales, se inscribirán ante la PROHAB. Sobre el cifrado de datos, la Universidad no cuenta con ningún tipo de normativa o base de datos cifrada, se espera llevar el tema al comité de arquitectura universitario, el cual se creó el día 22 del mes de abril del año 2016, bajo la directriz: Comité de Arquitectura de Información, número: DGTI-DZ-08, el cual tiene entre sus responsabilidades guiar el desarrollo de sistemas de información que brinden datos confiables, íntegros y en tiempo oportuno, para un proceso efectivo de toma de decisiones. Este comité será el encargado de la toma de decisiones sobre cuál va a ser la estrategia a seguir y si se debe implementar el cifrado, esto mediante el siguiente proceso:

- Se presenta la iniciativa al comité.

- El comité revisa la misma y la valida.
- Una vez aprobada pasa a la dirección de TI para su ratificación.

La Universidad no tiene dimensionadas las implicaciones que esto traería en los momentos de recuperación de datos y tampoco tienen claro los beneficios que esto les pueda traer.

La UTN cuenta con algunas soluciones de seguridad, como son el IPS, IDS, Firewall de red y el antivirus, ninguno de estos aplicativos tiene la función de protección de datos o no esta activada. También, se indica que en estos momentos la UTN no tiene claro cuáles son sus necesidades actuales en protección de información; no obstante, con la creación del área de seguridad se espera empezar a trabajar en este tema.

4.3. UTN, Infraestructura y Servidores

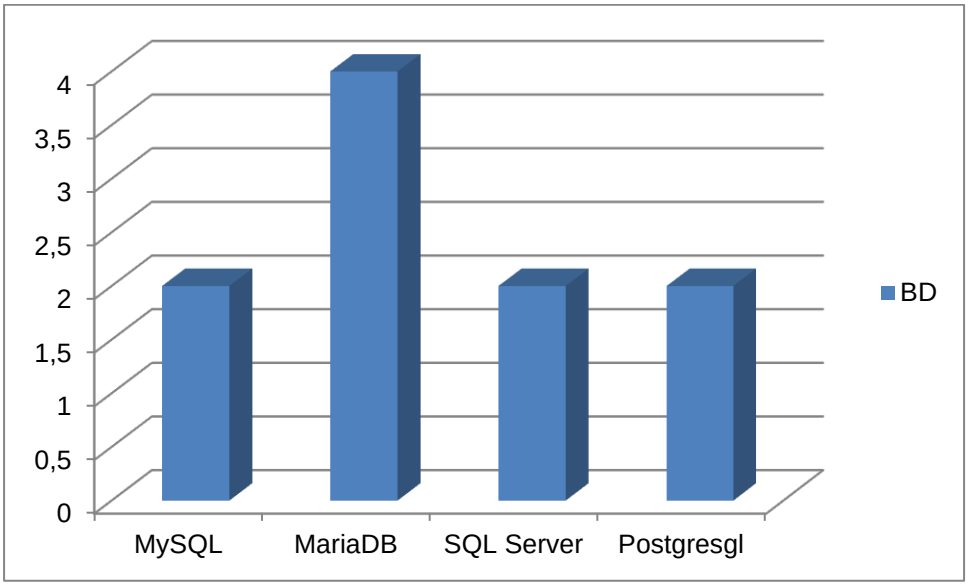
Como resultado de las entrevistas que se realizaron al personal de infraestructura de la UTN en el mes de julio de 2016, se identificó que la Universidad Técnica Nacional actualmente consta de un centro de datos local con una infraestructura para los servidores de bases de datos tipo clúster[10] con cuatro servidores físicos marca Dell PowerEdge M620 con 192GB de memoria RAM y procesadores Xeon E5-2620 de 1.9 Ghz, 320 GB de HDD (Disco Duro) en RAID1[11], tarjetas de red de 1 Gb de conexión por cable de cobre y están en alta disponibilidad. Estos servidores funcionan bajo el sistema operativo Ubuntu Server y Windows Server 2012, son exclusivos para las bases de datos, mismas que están instaladas en un ambiente virtual sobre la plataforma *VMWARE*. En este ambiente están configurados nueve servidores virtuales de bases de datos que en total tienen cuatro tipos diferentes de SGBD:

[10] Es un conjunto de ordenadores unidos entre sí, donde se busca balanceo de carga, alto rendimiento, alta disponibilidad y escalabilidad.
[11] Consiste en una arquitectura donde se guarda una copia exacta de la información en otro disco.

- Postgresql
  - 9.0.4 (Windows)
  - 9.3.10 (Linux)
- MariaDB
  - 10.1.14 (Linux)
- MySQL
- SQL Server 2016

La UTN ya tiene identificadas las bases de datos con información sensible y han seleccionado diez BD candidatas a ser cifradas, estas BD se encuentran almacenadas en una SAN[12] que posee la Universidad.

Grafico 5.1. Cantidad de DB por SGBD candidatas al cifrado



Como se muestra en el gráfico anterior las diez BD están distribuidas en varios SGBD. Por consiguiente, hay que tomar en cuenta que la Universidad se encuentra

[12] Red dedicada al almacenamiento de información, que está conectada a la red principal de la organización.

en un proceso de migración de estos sistemas, por lo que se espera que para el año 2017 todas las bases de datos queden unificadas bajo el SGBD de MariaDB, con excepción de las BD que sean Postgresql, ya que estas pertenecen a una aplicación de terceros, una vez migradas se manejarán en servidores *Standalone*[13]. La BD más grande pesa alrededor de los 30GB y el promedio de las otras es de 1GB, siendo respaldadas con la periodicidad de una vez al día.

4.4. Sobre los Métodos de Cifrado y Buenas Prácticas Relacionadas

La información contenida en las bases de datos es probablemente, uno de los activos más preciados de las empresas, razón por la cual es muy importante protegerlos adecuadamente contra intrusos o personas que deseen tener acceso a ellos sin permiso o con fines ilegales. El cifrado se ha vuelto una de las opciones por excelencia para este fin, dependiendo del tipo de base de datos que se posea, las aplicaciones que accedan a ella, el tipo de conexión que se utilice o la información almacenada, es el método de cifrado que se debe realizar.

Según expertos como el señor Hugo Solís Sánchez, para una base de datos que normalmente recibe consultas o instrucciones de aplicaciones internas o en la misma red, se debe usar un cifrado simétrico, ya que gracias a la forma en que oculta los datos es menor el costo (tiempo de procesamiento) al momento de cifrar o descifrar la información, en transacciones o consultas externas a la red o internet, se debe usar cifrado de tipo asimétrico, ya que posee un nivel de seguridad más robusto. En el caso de las bases de datos que posean consultas tanto del exterior como interior de la red, se debe implementar un cifrado híbrido combinando simétrico y asimétrico dependiendo de dónde proceda la consulta.

[13] Es un servidor que no se encuentra registrado dentro del dominio de la red.

Como se mencionó en el apartado anterior, la Universidad Técnica Nacional posee distintos SGBD, los cuales se esperan unificar bajo el motor de MariaDB 10.1.14. Mediante la investigación que se realizó se descubrió que esta base de datos acepta llaves criptográficas de 128, 192 y 256 bits. Además, se investigó acerca de que la UTN tiene actualmente toda la información en datos planos (sin cifrar); con dicha información y según las recomendaciones del experto en cifrado, la mejor práctica en este caso es usar llaves de 192 bits, ya que 128 bits ha quedado vulnerable, 256 bits es un estándar militar que requiere de un alto costo de procesamiento y tiempo, en comparación del necesario para las llaves de 192 bits, con un algoritmo de cifrado AES, ya sea AES_CBC o AES_CTR ambos aceptados por MariaDB.

Antes de realizar un proceso tan delicado como cifrar por primera vez una base de datos, los expertos y las buenas prácticas mencionan una serie de consideraciones por tomar en cuenta, en caso de cualquier percance que pueda suceder, seguidamente se citan las más importantes:

- Hacer un respaldo completo de toda la información de la base de datos que sea lo más actual posible.
- Tener una UPS o un sistema eléctrico de emergencia que actúe en caso de un fallo de fluido eléctrico.
- Asegurarse que el sistema de refrigeración de los servidores funcione correctamente.
- Tener los servidores exclusivamente trabajando en el proceso, ya que demanda una alta carga de procesamiento y de escritura sobre los HDD.

Esto a raíz de que un proceso de cifrado de datos en gran volumen, como el que se produce al cifrar una BD por primera vez, genera gran cantidad de trabajo para los procesadores y los HDD, que a su vez demandan una gran cantidad de energía y esto produce que se recalienten, por lo que si no se tienen sistemas de enfriamiento adecuados y métodos de respaldo de energía, un corte eléctrico o el

daño de un procesador o HDD sin haber terminado el proceso, puede corromper todos los datos dejando la BD ilegible, siendo necesario restaurarla por completo para iniciar con el proceso de cifrado.

Debido a que este es un proceso tan delicado, se debe hacer de una manera gradual, cifrando una por una todas las tablas o campos de la BD que tienen información que la Universidad considera necesaria su protección. Esperando que el proceso termine antes de pasar al siguiente, esto para garantizar un correcto cifrado de la información, minimizando el riesgo de corromper un gran volumen de datos.

Es importante tomar en cuenta que se deben crear nuevos protocolos de seguridad a la hora de trabajar con la base de datos, con el objetivo de saber qué hacer en caso de que un atacante logre vulnerar el cifrado de las bases de datos para realizar cambios sobre los mismos, entre otras situaciones que se pudieran presentar. Se debe contar con un procedimiento de documentación eficiente de todos los cambios que se realicen, a la estructura de la BD o a los datos que estén adentro, ya que, si ocurriera algún error o se corrompe el cifrado a la hora de modificar el dato, el mismo se vuelve no consultable. Los respaldos también deben cambiar, estos ahora deberán ser completos y no solo de los cambios realizados, porque cualquier error puede dejar los datos ilegibles, de igual importancia es el manejo que se le dará al respaldo físico de la llave maestra en caso de olvido de la misma por parte del administrador de BD, esta deberá ser almacenada en un lugar seguro y bajo los controles necesarios que defina la universidad.

4.5. Sobre los Métodos y Buenas Prácticas Relacionadas a los Procesos de la UTN

Como en toda entidad pública, la UTN tiene muchos procesos y normativa oficial, por lo que el método de cifrado a proponer y las buenas prácticas relacionadas a este, deberán adaptarse a esos instructivos y cumplir a cabalidad con lo que piden, ya que los mismos deberán alinearse al plan estratégico de la

Universidad, específicamente al de la Dirección de Gestión de Tecnologías de Información (DGTI).

Toda iniciativa que se desee implementar en la Universidad en relación con los sistemas de información, debe pasar por la aprobación del **Comité de Arquitectura de Información** (CAI), el cual tiene como miembros al:

- Director de DGTI.
- Jefatura de Gestión Técnica.
- Jefatura de Gestión Estratégica.
- Administrador de Base de Datos (DBA).
- Responsable de Seguridad de la Información.
- Representante de Desarrollo.
- Representante de Infraestructura y Telecomunicaciones.
- Responsable de Aprovisionamiento de TI.

Este comité tiene entre sus responsabilidades más importantes las mencionadas a continuación:

- Asegurar la alineación de la Arquitectura de la Información con las necesidades y objetivos de negocio, representados por el plan estratégico organizacional.
- Brindar una mejora gradual a nivel de madurez de la Arquitectura de la Información dentro de la organización.
- Aprobar o rechazar las solicitudes de cambio a la Arquitectura de la Información de la UTN.
- Promover el uso o adopción de buenas prácticas que permitan mejorar la calidad de los procesos de DGTI.

A continuación, listan las funciones más importantes de este ente en relación con lo que se está proponiendo:

- Analizar cualquier cambio de iniciativa o implementación tecnológica.
- Evaluar o aprobar cambios sobre la normativa de Arquitectura de Información.
- Examinar estrategias de migración y contingencias de los componentes tecnológicos que afecten la Arquitectura de Información.
- Advertir posibles riesgos asociados en las iniciativas de TI que son presentadas al comité.
- Considerar el impacto de cambios competitivos y nuevas regulaciones sobre la infraestructura tecnológica.

Se considera que el CAI es el ente más importante en cuanto a la aprobación de propuestas con temas sobre la arquitectura de la información, por lo tanto, nuestra guía deberá cumplir con las regulaciones de este Comité.

Otro aspecto importante por tomar en consideración, es que la DGTI cuenta con un plan táctico y estratégico alineado con los objetivos de la Institución, llamado Plan Táctico de Tecnologías de Información y Comunicación –PTAC- 2016-2018, dicho documento se ha creado para planificar las iniciativas que la DGTI prevé utilizar para alcanzar los objetivos plasmados en el Plan Estratégico de Tecnologías de Información y Comunicación (PETIC), ya que estos son imprescindibles para dar respuesta a las necesidades de la Institución.

El PTAC reconoce los siguientes factores críticos para el logro de los objetivos de TI:

- Recurso Humano.
- Control de Calidad.
- Control de la Seguridad.
- Control del Riesgo.
- Presupuesto.

El siguiente cuadro presenta la integración de los Objetivos Estratégicos de la Universidad, los Objetivos de la DGTI y cómo se relacionan con los proyectos aprobados de TI.

No	Objetivos Estratégicos Institucionales	Objetivos de TI	Proyectos de TI
1	Implementar estrategias dirigidas a la generación de recursos para el desarrollo equilibrado y sostenido de la universidad, sus sedes y centros.	Desarrollar proyectos TIC enfocados en el mejoramiento y desarrollo de los procesos estratégicos institucionales.	UTN-GPTI-2015-02 (Gestión Talento Humano)
2	Fortalecer la capacidad de autogobierno, la seguridad financiera y la independencia de gestión, para consolidar el ejercicio pleno de la autonomía universitaria.		UTN-GPTI-201504 (Sistema de Control Interno-SEVRI&PM)
3	Promover la cooperación con otras universidades del mundo y del país para fortalecer la gestión académica y el desarrollo institucional.		
4	Incorporar a la Universidad al Sistema de Coordinación de la Educación Superior Universitaria Estatal y al Consejo Nacional de Rectores.		UTN-GPTI-2016-01 (Mejoras Avatar 2016)
5	Mejorar los procesos de planificación, gestión administrativa y académica y el uso eficiente de los recursos, en función del desarrollo estratégico de la Universidad.	Gestionar en forma continua y eficiente el marco de gestión de riesgos de TI de la Universidad.	UTN-GPTI-2015-01 (Implementación Normas Técnicas de CGR)

No	Objetivos Estratégicos Institucionales	Objetivos de TI	Proyectos de TI
		Cumplir con leyes, reglamentos, normas y otros, sobre el uso y adquisición de tecnologías informáticas y de telecomunicaciones.	

Basada en el cuadro presentado anteriormente, la implementación de la propuesta puede ayudar en el cumplimiento de los objetivos de TI que responden al objetivo institucional número 5. Al cifrar la información en las bases de datos, no solo se estaría disminuyendo en gran medida los riesgos relacionados con seguridad de la información, sino que también ayuda en el cumplimiento de leyes como la Ley 8968.

Por lo tanto, la guía por proponer se ajustará a los requerimientos pedidos por el CAI al mismo tiempo que se alinea con los objetivos estratégicos de la Universidad y de la DGTI.

4.6. Sobre las Ventajas de los Métodos Escogidos

Según la información que fue transmitida por el experto en cifrado de bases de datos y a la del personal de la Universidad, se listan a continuación las ventajas de los métodos escogidos con respecto a la situación actual de la UTN que no posee este tipo de seguridad:

- Con la infraestructura que posee actualmente la UTN se considera viable realizar el proceso de cifrado de sus repositorios de información.
- No se tiene que invertir en mejoras de hardware, ya que los equipos de la Universidad tienen la capacidad necesaria para implementar el cifrado propuesto.
- Solo cuando se cifre en su totalidad una BD, provocaría una carga significativa sobre los servidores.
- No habrá mayor afectación en el uso diario, en cuanto a consultas o comandos sobre las tablas.
- Cuando se consulta una tabla o campo en específico, solo se descifra dicho campo y no la totalidad de la BD, haciendo el proceso más ágil.
- Al implementar un cifrado simétrico, se reducen los costos en cuanto a tiempo, por lo que las consultas serán más rápidas en comparación con el uso de otro tipo de cifrado.
- El proceso será sobre los campos de la propia base de datos, por lo tanto, no habrá afectación sobre las aplicaciones que consultan la misma, ya que para estas aplicaciones la información siempre llegará descifrada.
- Los datos estarán protegidos, en caso de algún incidente relacionado con la seguridad de los mismos.
- No aumenta la complejidad técnica a la hora de hacer respaldos.
- Los respaldos serán cifrados, lo que aumenta la seguridad de ellos.
- Se pueden combinar dos algoritmos distintos dentro del cifrado para tener más seguridad en caso de que se diera algún intento de robo de información, en esta situación se podría utilizar un algoritmo de tipo estándar para los datos menos sensibles y otro de tipo experimental para los datos más importantes.
- Ayuda con el cumplimiento de lo establecido en la sección 3 artículo 10 de la Ley 8968.

Como se puede observar las ventajas son muchas, en comparación con la situación actual de la UTN, entre ellas sobre sale que no se debe realizar una inversión del presupuesto para su implementación y que aumentará el nivel de seguridad de los datos de la Universidad considerablemente.

4.7. Estándar Documental Usado por la UTN

Siguiendo el formato oficial usado en los documentos formales y guías metodológicas en la dirección de TI de la Universidad Técnica Nacional, se procederá a explicar la forma en la que será estructurado el documento de la guía técnica de cifrado. Esto para seguir el estándar usado por la Universidad y darle carácter oficial a la propuesta.

Todo documento emitido por la dirección de TI debe contener entre sus elementos: un encabezado, el cual está compuesto por un cuadro que debe contener el escudo de la Universidad, el nombre de la misma, el nombre del área o dirección a la que pertenece, el número de documento, el número de versión y el número de página, además del título del documento, seguido debe colocarse el propósito y alcance del mismo, posteriormente el área emisora y definiciones (si aplican), por último el detalle o cuerpo del documento y el historial de cambios que se le ha realizado.

Ejemplo:

Universidad Técnica Nacional	**Universidad Técnica Nacional** Dirección de Gestión de Tecnologías de Información	Número: Versión: Páginas:	**XXXX-XX-XX** **X.X** **X de X**
Título del documento			

1. **Propósito.**

2. **Alcance.**

3. **Detalle.**

4. **Historial de Cambios.**

.

Versión	Fecha	Cambio Realizado	Responsable del cambio

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. UTN, Normativa y Aspectos Legales en Materia de Protección de la Información

Seguidamente se expondrán las principales conclusiones obtenidas a lo largo de la investigación; junto a estas se plantearán las recomendaciones consideradas en cada caso.

5.1.1. Conclusiones:

Faltante de asignación de personal a los nuevos procesos en materia de seguridad en la UTN.

- La Universidad se encuentra actualmente en etapa de análisis, creación y definición de una normativa en materia de protección de la información.
- La UTN tiene definidas algunas de las funciones para avanzar en este proceso y las acciones que se deben considerar para llevar a cabo el mismo.
- Hace falta una clara división de responsables y dueños de los nuevos procesos.

5.1.2. Recomendaciones:

Asignación de responsables en el proceso de la normativa y aspectos de legalidad en la protección de la información.

- Se recomienda que la Universidad continúe con la creación y modificación de la normativa que posee actualmente. Lo anterior permitiría que el proceso de cifrado se integre de manera correcta y en el tiempo adecuado.
- Definir e identificar a las personas responsables del proceso de cifrado, con el fin de cumplir con la normativa y así evitar posibles sanciones en el futuro.
- Fortalecer el área recién creada de Seguridad de la Información, ya que esta será fundamental en todo este proceso y cumplimiento de las normas de los entes reguladores, además de velar por el cifrado de información confidencial.

5.2. UTN, Manejo de los Datos y Seguridad

5.2.1. Conclusiones:

Carencia de procesos sobre protección de datos en la base de datos de la UTN.

- La UTN todavía no posee herramientas especializadas o procesos claros sobre el tema de la protección de la información.
- Ya se ha oficializado un área de Seguridad de la Información, la cual responde a la necesidad de mejorar en estos temas, aunque la misma no tiene todavía personal a cargo.
- Se ha iniciado con el proceso de clasificación de la información, este todavía está en etapas tempranas de desarrollo y falta identificar muchas necesidades y carencias que actualmente posee la institución.

5.2.2. Recomendaciones:

Clasificación de la información con el fin de identificar las bases de datos que pueden ser cifradas.

- Continuar con el trabajo de clasificación de la información, el cual es uno de los principales insumos para los procesos de seguridad de la información, mismo que ayudará a identificar cuáles son los datos sensibles de la Universidad y en cuales BD están almacenados, estas serán las BD candidatas al cifrado.
- Aplicar el cifrado de información como capa de protección para estos datos.
- Identificar las necesidades restantes que posee la UTN a nivel de seguridad de la información con el fin de prevenir problemas futuros que el cifrado no pueda proteger.

5.3. UTN, Infraestructura y Servidores

5.3.1. Conclusiones:

Estado de la infraestructura de la Universidad que deberá soportar el proceso de cifrado y SGBD relacionadas.

- La infraestructura es suficientemente robusta para soportar un proceso de cifrado de BD.
- No se necesita incurrir en la compra de equipos de hardware o software, extras para realizar este proceso.
- La UTN no cuenta con un manual sobre buenas prácticas para realizar el cifrado de las bases de datos en caso de que se decida cifrar la información.

5.3.2. Recomendaciones:

Hacer uso de las recomendaciones y buenas prácticas expuestas en la Guía Técnica de Cifrado para Bases de Datos.

- En caso de que la UTN decida realizar el cifrado de su información, realice el mismo siguiendo las consideraciones y buenas prácticas previas al mismo, que se mencionan en el capítulo anterior, esto para evitar pérdida de información en caso de algún error.
- Realizar el proceso de cifrado de las bases de datos siguiendo la guía técnica de cifrado que se menciona en el capítulo anterior, esto para evitar problemas durante el proceso.

5.4. Sobre los Métodos de Cifrado y Buenas Prácticas Relacionadas

5.4.1. Conclusiones:

Seguimiento de las recomendaciones que se encuentran en la Guía Técnica de Cifrado para Bases de Datos.

- Según la información recaba de las diferentes fuentes, se concluye que para el tipo de SGBD con la infraestructura con la que cuenta la UTN, el cifrado simétrico, con llaves de 192 bits, utilizando un algoritmo AES es la forma más apropiada de proteger las BD de la Universidad.
-

5.4.2. Recomendaciones

Aplicar las directrices con respecto a cifrado de datos y buenas prácticas relacionadas.

- Implementar el cifrado de datos siguiendo las directrices mencionadas en el capítulo anterior, siguiendo todas las recomendaciones a la hora de la implementación, esto para realizar el mismo siguiendo las buenas prácticas identificadas para este proceso.

5.5. Sobre los Métodos y Buenas Prácticas Relacionadas a los Procesos de la UTN

5.5.1. Conclusiones:

Presentar la propuesta de cifrado ante el CAI de la UTN.

- El proceso propuesto por implementar está alineado con los objetivos de la Universidad, cumple con las normas y procesos del DGTI.

5.5.2. Recomendaciones:

- Se recomienda que en caso de que se decida llevar a cabo el proceso de cifrado, se presente la propuesta ante el CAI para su valoración y se sigan todas las recomendaciones hechas en este documento, esto con el fin de utilizar las mejores prácticas relacionadas y seguir el proceso normado por la Universidad.

5.6. Sobre las Ventajas de los Métodos Escogidos

5.6.1. Conclusiones:

Aplicar cifrado en los SGBD que posean información sensible.

- Después de examinar los métodos y buenas prácticas escogidas en la etapa de investigación, se concluye que aplicar un mecanismo de cifrado sobre los datos de la UTN, marcará una diferencia sustancial en materia de seguridad de los datos comparando el estado actual de la misma.

5.6.2. Recomendaciones:

- Se recomienda aplicar cifrado en los SGBD que la Universidad haya identificado que posean información sensible o que necesitan protección, esto no solo aumentará sustancialmente el nivel de seguridad de los repositorios de datos, sino que además ayudará con el cumplimiento de regulaciones como la Ley 8968, esto con el fin de ver las ventajas que traerá el cifrado a la Universidad.

CAPITULO VI: PROPUESTA

A continuación, se presenta la propuesta para la implementación de la guía técnica, la cual se espera que sea de provecho para la implementación del cifrado en las BD de la Universidad.

6.1. Guía Técnica de Cifrado para las Bases de Datos de la UTN

Universidad Técnica Nacional	**Universidad Técnica Nacional** Dirección de Gestión de Tecnologías de Información	Número: Versión: Páginas:	**0** **1.0** **1 de 7**
Guía Técnica de Cifrado para Bases de Datos			

1. Propósito

El objetivo de esta guía es ayudar al personal encargado de la administración de las bases de datos de la UTN a implementar correctamente el cifrado de datos sobre sus SGBD MariaDB.

2. Alcance

Esta guía paso a paso proporciona las instrucciones necesarias para usar el cifrado de bases de datos con un SGBD MariaDB 10.1.14. Se recomienda realizar primero los pasos indicados en la presente guía en un entorno de laboratorio de pruebas. La guía paso a paso está diseñada para implementar el cifrado en las bases de datos de la Universidad Técnica Nacional y está basada en la documentación oficial de MariaDB[14] y la información recopilada en las entrevistas.

[14] https://mariadb.com/kb/en/mariadb/data-at-rest-encryption/

3. Guía

3.1. Motores de bases de datos que soportan el cifrado en MariaDB.

Tiene soporte completo para cifrado los motores de almacenaje XtraDB e InnoDB, adicionalmente Aria pero solo para tablas creadas con la instrucción: *ROW_FORMAT=PAGE* (Por defecto).

MariaDB ofrece las opciones de cifrar:

- Todo.
- Tablas individuales.
- Todo, con excepción de algunas tablas individuales.
- También se puede escoger la opción de cifrar los archivos de registro.

3.2. Limitaciones

- Solo los datos almacenados son cifrados, los metadatos[15] (por ejemplo, archivos frm) y los datos que son enviados al cliente no están protegidos (para proteger estos datos se recomienda cifrar el canal).
- Solo el servidor de MariaDB sabe descifrar los datos:
  - *Mysqlbinlog* no puede leer los registros en binario cifrados.
  - *Percona XtraBackup* no puede respaldar las instancias de los archivos de registro que estén cifrados en InnoDB.

[15] Son referencias o índices de otros datos.

- No se cifra el cache de disco.
- El complemento de auditoria no puede crear una salida cifrada. En caso de querer protegerlo se debe enviar los datos al *syslog* y configurarlos ahí.
- El registro general de consultas (*general query log*) basado en archivos y el registro de consultas lentas (*slow query log*) no se pueden cifrar.
- El registro de Aria no está cifrado. Sin embargo, esto afecta sólo las tablas Aria no temporales.
- El registro de errores MariaDB no está cifrado.

3.3. Consideraciones previas al cifrado

El siguiente apartado trata sobre los pasos por tomar en cuenta antes de realizar el cifrado de las bases de datos.

- Realizar un respaldo completo de toda la información que contenga la base de datos a cifrar, antes de empezar el proceso.
- Contar con un sistema eléctrico de emergencia que actué en caso de un fallo de fluido eléctrico y pueda mantener el proceso en marcha.
- Asegurarse que el sistema de refrigeración de los servidores funcione correctamente.
- Dedicar los servidores exclusivamente a trabajar en el proceso de cifrado, ya que demanda una alta carga de procesamiento y de escritura sobre los HDD.

3.4. Creación del archivo de manejo de las claves de Cifrado

La gestión de claves en MariaDB es proporcionado por un complemento de cifrado, el cual es: *file_key_management*. El mismo se debe configurar de la siguiente manera:

- *file_key_management_filename*: dirección del archivo. Esta opción es necesaria, el complemento no funcionará sin él, ejemplo:
    - *file_key_management_filename* = /home/mdb/keys.enc

  Este archivo tiene la opción de ser cifrado, usando la siguiente instrucción en la línea de comandos de OpenSSL:
    - openssl enc -aes-192-cbc -md sha1 -k clave -in keys.txt -out keys.enc
- *file_key_management_filekey:* es el parámetro utilizado para descifrar el archivo de claves. Hay dos formas para descifrar el mismo, se puede utilizar una clave o utilizar un archivo que contenga la clave.
    - Ejemplo utilizando solo la clave: *file_key_management_filekey* = clave.
    - Ejemplo utilizando un archivo: se debe iniciar con la palabra FILE, el resto del valor se interpreta como una ruta de acceso al archivo que contiene la clave, ejemplo: *file_key_management_filekey* = FILE:/ruta/archivoClave.
- *file_key_management_encryption_algorithm*: es el algoritmo de cifrado a utilizar, el cual se recomienda que sea AES.
    - *file_key_management_encryption_algorithm* = aes_cbc.

3.5. Configuración del cifrado de datos

Una vez creado el *file_key_management* se debe configurar los motores de almacenado, ya sean XtraDB o InnoDB, las siguientes instrucciones se pueden aplicar para cualquiera de los dos motores, ejemplo para el caso de InnoDB:

- Establecer el parámetro *innodb-encrypt-tables* en *ON* o en *FORCE.*
- Establecer el parámetro *innodb-encrypt-log* en *ON.*

Ejemplo para el caso de XtraDB:

- Establecer el parámetro *xtradb-encrypt-tables* en *ON* o en *FORCE.*
- Establecer el parámetro *xtradb-encrypt-log* en *ON.*

Todos los comandos presentados a continuación funcionan para los dos motores, solo se debe remplazar la palabra innodb o xtradb según corresponda. Para realizar ajustes personalizados al cifrado se pueden usar los siguientes parámetros:

Parámetro	**Valor**	**Descripción**
innodb-encrypt-tables	ON, OFF, o FORCE	Activa el cifrado para las tablas
innodb-encrypt-log	Booleano	Activa el cifrado de registros
innodb-encryption-rotate-key-age	Entero positivo	Vuelve a cifrar en segundo plano todas las páginas que fueron cifradas con una clave de una versión antigua
innodb-encryption-rotation-iops	Entero positivo	Utilizar las operaciones de entrada/salida, para la rotación de claves en segundo plano
innodb-encryption-threads	Entero positivo	Numero de subprocesos que realizan la rotación de claves en segundo plano

Para activar el cifrado de tablas y logs se deben usar las siguientes instrucciones:

- *innodb-encrypt-tables = ON.*
    - En caso de poner el parámetro en *FORCE*, obligara a que todas las tablas nuevas que sean creadas, estén cifradas.
- *innodb-encrypt-log = ON.*

Una vez activados estos parámetros, se debe activar el cifrado en las tablas que deseamos proteger, para esto se debe asegurar que la propiedad *innodb_file_per_table* se encuentre en *ON*, seguidamente para cifrar las tablas, se usa la instrucción *ALTER TABLE* para las tablas creadas y *CREATE TABLE* para las tablas nuevas, combinado con las siguientes variables:

Variable	**Valor**	**Descripción**
ENCRYPTED	YES/NO	Activa o desactiva el cifrado en la tabla
ENCRYPTION_KEY_ID	Entero positivo	Se debe colocar el identificador de la clave que se encuentra en el archivo *file_key_management*

Ejemplo, si se quiere proteger la tabla llamada **usuario** que ya fue creada con anterioridad, se usa la siguiente instrucción:

- *ALTER TABLE* **usuario** *ENCRYPTED=YES ENCRYPTION_KEY_ID*=1.

En caso de querer proteger una tabla nueva como por ejemplo **cuenta**, se debe realizar de la siguiente manera:

- *CREATE TABLE* **cuenta** *(id int, value varchar(255)) ENCRYPTED=YES ENCRYPTION_KEY_ID*=1.

Finalmente, en caso de que se quiera remover el cifrado de una tabla como por ejemplo **teléfono**, se usa el siguiente comando:

- *ALTER TABLE* **telefono** *ENCRYPTED =NO*.

4. Historial de Cambios

Versión	Fecha	Cambio Realizado	Responsable del cambio
1.0	02/01/2017	Creación del documento	Keylin Calvo Alfaro Rubén Sánchez Matamoros

Bibliografía

IT Governance Institute. (2007). *Cobit 4.1.* Ilinois: IT Governance Institute.

Agencia de Protección de Datos de los Habitantes. (n.d.). *Agencia de Protección de Datos de los Habitantes*. Retrieved Julio 04, 2016, from http://www.prodhab.go.cr//conozcanos/?resenna

Alegsa, L. (2013, Julio 16). *DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA*. Retrieved Julio 03, 2016, from http://www.alegsa.com.ar/Dic/sistema%20operativo.php

Álvarez, E. J. (2008, Agosto). *http://latn.org.ar/.* Retrieved Julio 04, 2016, from http://latn.org.ar/wp-content/uploads/2015/01/wp-98.pdf

Andres, L. (2010, Junio 15). *Elblogdemercado's Blog*. Retrieved Febrero 13, 2016, from https://elblogdemercado.wordpress.com/category/identificacion-de-la-informatica-con-la-actualidad/la-informatica-y-el-tratamiento-de-la-informacion/

Asamblea Legislativa de la Republica de Costa Rica. (2011). *PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES.* San José. Retrieved Julio 05, 2016

Asenjo, J. S. (2012). *Jorguesanchez.* Retrieved Julio 03, 2016, from http://www.jorgesanchez.net/web/iaw/iaw1.pdf

Biblioteca Universidad de Alcalá. (n.d.). Retrieved from http://www3.uah.es/bibliotecaformacion/BPOL/FUENTESDEINFORMACION/

BitCompany. (2015, Julio 30). *BITCOMPANY*. Retrieved Enero 14, 2016, from http://www.bitcompany.biz/cobit-5-gestion-de-seguridad/#.VrJE0rIrK01

Bueno, A. (2016, Julio 03). *Portaleso.* Retrieved from http://www.portaleso.com/portaleso/trabajos/tecnologia/comunicacion/ud_4_redes_v1_c.pdf

Carbajal, I. (2011, Abril 01). *Full Blog.* Retrieved 04 11, 2016, from http://israelcarbajal.fullblog.com.ar/tag/cifrado/

Díaz, J. C. (1995). *Criptografía: historia de la escritura cifrada.* Madrid: Editorial Complutense.

El Economista. (2014, Noviembre 10). Retrieved Septiembre 18, 2015, from http://eleconomista.com.mx/tecnociencia/2014/11/10/empresas-padecen-mas-robo-informacion-correo-electronico

Ferrer, R. (2014, Octubre 16). *SISTESEG.* Retrieved from http://www.sisteseg.com/files/Microsoft_Word_-_RECOMENDACIONES_PARA_SOFTWARE_E_INFRAESTRUCTURA_SEGURA.pdf

Fuensanta, J. R. (n.d.). *Una introducción a la Criptografía Clásica.* Retrieved Noviembre 06, 2015, from http://www.criptohistoria.es/files/CIFRAS.pdf

Gómez, H. (2016, Enero 21). Muchas compañías no cifran los datos privados de sus empleados. *CSO España*. Retrieved Abril 14, 2016, from http://cso.computerworld.es/proteccion-de-datos/muchas-companias-no-cifran-los-datos-privados-de-sus-empleados

Gutiérrez, P. (2013, Enero 15). *GENBETA:DEV*. Retrieved Junio 28, 2016, from http://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Gutiérrez, P. (2013, Enero 3). *Tipos de criptografía: simétrica, asimétrica e hibrida*. Retrieved Abril 12, 2016, from http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Ignacio, M. G. (2013). *Delitos Informáticos en Latinoamérica.* Retrieved Abril 14, 2016, from Conaiisi: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

Infobae. (2014, Diciembre 18). Retrieved Septiembre 02, 2015, from http://www.infobae.com/2014/12/18/1616035-tarjetas-credito-apple-y-robo-informacion-corporativa-los-preferidos-el-ciberdelito-2015

Instituto de Investigaciones Ambientales. (n.d.). Retrieved from http://www.virtual.unal.edu.co/cursos/IDEA/2007219/lecciones/cap_4/sub5.html

Instituto Nacional de Ciberseguridad de España. (n.d.). *Incibe*. Retrieved Junio 30, 2016, from

https://www.incibe.es/empresas/que_te_interesa/Buenas_practicas_en_informatica

INTECO. (2015). *Instituto de Normas Técnicas de Costa Rica*. Retrieved Julio 04, 2016, from http://inteco.or.cr/esp/

INTECO. (n.d.). La criptografía desde la antigua Grecia hasta la máquina Enigma. In *La criptografía desde la antigua Grecia hasta la máquina Enigma* (p. 12). Retrieved Abril 11, 2016, from http://www.egov.ufsc.br/portal/sites/default/files/la_criptografia_desde_la_antigua_grecia_hasta_la_maquina_enigma1.pdf

ISO 27000. (2016, Marzo 07). *ISO 27000*. Retrieved from http://www.iso27000.es/sgsi.html

ISO 27000. (n.d.). *ISO27000.* Retrieved Junio 23, 2016, from http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27002. (n.d.). Retrieved Junio 23, 2016, from ISO 27000: http://www.iso27000.es/iso27002.html

Lages, S. G. (1994). *Historia de la Escritura, de la Grafología y su evolución.* Madrid: Lulu.com.

Lign, A. (n.d.). *Servicios de Auditoria ISO 27001*. Retrieved Julio 04, 2016, from http://www.a-lign.com/iso27001-espanol/?gclid=CP-Dg4PR2s0CFRFZhgod5zwFPQ

Mamani, U. L. (s.f.). *Uni Net*. Retrieved 11 05, 2015, from http://www.uninet.edu/6fevu/text/criptografia.htm

MICIT. (2015, Noviembre 08). Retrieved Enero 26, 2016, from MICIT: https://www.micit.go.cr/index.php?option=com_content&view=article&id=8135:costa-rica-firma-acuerdo-de-entendimiento-sobre-seguridad-cibernetica-con-corea&catid=40&Itemid=630

Microsoft. (2016, Enero 20). *Microsoft Developer Network*. Retrieved Junio 28, 2016, from https://msdn.microsoft.com/es-es/library/ms345262.aspx

Microsoft. (n.d.). *Microsoft*. Retrieved 11 06, 2015, from https://msdn.microsoft.com/es-es/library/bb972217.aspx

MINAET. (2011). *Estado de Seguridad Informática en el sector público costarricense.* San Jose: Ministerio de Ambiente, Energía y Telecomunicaciones.

Paredes, G. G. (2006, Julio 10). *Revista Digital Universitaria*. Retrieved Septiembre 28, 2015, from http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf

Porolli, M. (2013, Julio 30). ¿Por qué debería cifrar mis datos? *ESET*. Retrieved Abril 14, 2016, from http://www.welivesecurity.com/la-es/2013/07/30/por-que-deberia-cifrar-mis-datos/

Preukschat, A. (2014, Enero 15). *Oro y Finanzas.* Retrieved Marzo 04, 2017, from https://www.oroyfinanzas.com/2014/01/criptografia-curva-eliptica-bitcoin-por-que-utiliza-ecdsa/

PRODHAB. (2014, Mayo 23). Retrieved Marzo 16, 2016, from http://www.prodhab.go.cr/Informacion/?AVISO-IMPORTANTE-A-TODAS-LAS-INSTITUCIONES-PUBLICAS-Y-EMPRESAS-PRIVADAS

Rojas, L. (2015, Agosto 31). *crhoy.com*. Retrieved Septiembre 02, 2015, from http://www.crhoy.com/hackean-500-mil-registros-del-sistema-de-la-caja/

Rojas, P. (2013, Julio 28). *CRHoy*. Retrieved Octubre 06, 2015, from http://www.crhoy.com/encriptacion-la-mejor-manera-de-proteger-datos-ante-ataques-informaticos/

Rojas, P. (2014, Abril 21). *CR Hoy*. Retrieved Marzo 07, 2016, from http://www.crhoy.com/los-delitos-informaticos-son-mas-comunes-en-costa-rica-de-lo-que-se-cree-segun-experto/

SIOSA. (2016, Abril 28). *SIOSA*. Retrieved Julio 01, 2016, from https://siosamantenimiento.wordpress.com/2016/04/28/infraestructura-tecnologica/

Torres, C. A. (2010). *Metodología de la Investigación.* Bogota: PEARSON.

Tribunal Supremo de Elecciones. (2011, Setiembre 05). *Tribunal Supremo de Elecciones.* Retrieved Julio 04, 2016, from http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf

Turner, S. (2014, Abril 14). *Comunidades de iWeb*. Retrieved Julio 2, 2016, from http://blog.iweb.com/es/2014/04/servidores-de-bases-de-datos/2487.html

Universidad Distrital Francisco José de Caldas. (n.d.). *Universidad Distrital Francisco José de Caldas.* Retrieved Marzo 15, 2016, from https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

Universidad Nacional Abierta y a Distancia. (n.d.). *Universidad Nacional Abierta y a Distancia*. Retrieved Febrero 13, 2016, from http://datateca.unad.edu.co/contenidos/208041/Modulo_EXE/leccin_13_enfoque_mixto_de_la_investigacin.html#_ftn1

Valdés, D. P. (2007, Octubre 26). *Maestros del Web*. Retrieved Julio 03, 2016, from http://www.maestrosdelweb.com/que-son-las-bases-de-datos/

Valenzuela, I. (n.d.). *Qué es la Criptología*. Retrieved Abril 12, 2016, from Batanga: http://www.batanga.com/curiosidades/4642/que-es-la-criptologia

Vasquez, S. B. (2011, Enero 24). *Tecnología e informática*. Retrieved Julio 03, 2016, from https://solvasquez.wordpress.com/2011/01/24/definicion-de-sistema-operativo/

Vega, C. R. (2014, Junio 12). *La Nacion.* Retrieved Enero 15, 2016, from http://www.nacion.com/tecnologia/informatica/empresas-sufrieron-incidente-inseguridad-informatica_0_1420258093.html

Velasco, J. J. (2014, Mayo 20). Breve historia de la criptografía. *Diario Turing*. Retrieved Abril 12, 2016

Wigodski, J. (2010, Julio 14). *Metodología de la Investigación*. Retrieved Febrero 13, 2016, from http://metodologiaeninvestigacion.blogspot.com/2010/07/poblacion-y-muestra.html

ANEXOS

1. Cronograma de trabajo

Cronograma de trabajo														
Actividad/Semana	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Revisión del proyecto con la UTN														
Desarrollo del marco teórico														
Recolección de datos (investigación y entrevistas) sobre los métodos de cifrado en bases de datos														
Resumir y comparar los datos recolectados														
Análisis de resultados														
Presentación del estándar e informe final														

2. Estado del arte

AÑO	LUGAR	AUTOR	CONCEPTO CLAVE
1995	Madrid	Juan Carlos Galende Díaz	Los inicios y evolución del cifrado.
2013	Madrid	Susana Gómez Lages	Los inicios de los primeros métodos de escritura y su evolución hacia un sistema de caracteres.
2015	San Jose	Lady Rojas Alvarado	Situación actual de la sociedad costarricense donde se muestra que el robo de información es un problema actual y en aumento.
2006	México D.F	Gibrán Granados Paredes	Entender qué es la criptografía, cómo está clasificada, entender el funcionamiento básico de algunos sistemas de cifrado y conocer cómo se forman los documentos digitales como firmas y sobres digitales.
2011	San Jose	Ministerio de Ambiente, Energía y Telecomunicaciones	Brindar un diagnóstico del estado actual de las instituciones públicas de Costa Rica, en materia de seguridad, herramientas que poseen y políticas establecidas.
2013	San Jose	Pablo Rojas	Ventajas del cifrado a la hora de proteger la información de ataques informáticos.
2014	México D.F	El Economista	Situación actual en Latinoamérica, enfocado al robo de información, delitos informáticos y el aumento del crimen cibernético.

3. Fichas Bibliográficas

3.1. La seguridad de la información en la era moderna

Descriptor:	
Nombre del autor:	Pablo Rojas
Año:	2014
Título de la obra:	Delitos informáticos más comunes en Costa Rica
Edición:	
Lugar:	San Jose
Editorial:	CR Hoy
No. Pág. (Para citas literales):	2
Ubicación del texto:	Amenazas de seguridad de la información en Costa Rica
Comentario-cita literal-síntesis	Las instituciones públicas y privadas deben prepararse y tomar las medidas necesarias para evitar el robo de su información.

3.2. Una infraestructura segura

Descriptor:	
Nombre del autor:	Rodrigo Ferrer
Año:	2014
Título de la obra:	Recomendaciones para una Infraestructura Segura
Edición:	
Lugar:	Bogotá
Editorial:	SISTEGEG
No. Pág. (Para citas literales):	1
Ubicación del texto:	Una adecuada infraestructura
Comentario-cita literal-síntesis	Lista de dispositivos recomendados para la seguridad de la infraestructura tecnológica.

3.3. Cifrado en la protección de datos

Descriptor:	
Nombre del autor:	Susana Gómez Lages
Año:	1994
Título de la obra:	Historia de la Escritura, de la Grafología y su evolución
Edición:	
Lugar:	Madrid
Editorial:	Lulu
No. Pág. (Para citas literales):	9
Ubicación del texto:	Inicios de la escritura
Comentario-cita literal-síntesis	Los primeros signos de escritura partieron de la imitación gráfica de seres u objetos reales por medio de la pintura o los tallados.

3.4. Seguridad de la información en un entorno universitario

Descriptor:	
Nombre del autor:	MINAET
Año:	1994
Título de la obra:	Estado de Seguridad Informática en el sector público costarricense
Edición:	
Lugar:	San Jose
Editorial:	Ministerio de Ambiente, Energía y Telecomunicaciones
No. Pág. (Para citas literales):	9
Ubicación del texto:	Implementación de políticas y procesos para la protección de fuentes de información
Comentario-cita literal-síntesis	Actualmente las entidades del Estado, instituciones financieras, centros de enseñanzas, instituciones de salud y empresas privadas, entre otros, acumulan una gran cantidad de información sobre sus empleados, clientes, productos y servicios; que son fundamentales para su organización.