UNIVERSIDAD APEC

TRABAJO DE GRADO

Para optar por el título de Ingeniero de Software

e Ingeniero de Sistemas de Computación.

TEMA:

Evaluación de la implementación de un marco de gestión de la seguridad de la información apoyado en ISO 27000: 2013 en el departamento de TI y Seguridad de la Información del Banco Hacienda.

NOMBRES Y MATRÍCULAS DE LOS SUSTENTANTES:

Shade Yasmelys Estrella	20161333
Rosa Amelia Fernandez	20121177
Ángel Vladimir Soto Vargas	20160416

ASESOR:

Félix J. Rodríguez Paulino

Santo Domingo DN, marzo 2020.

ÍNDICE DE CONTENIDOS

AGRADECIMIENTOS

AGRADECIMIENTOS

Quiero agradecer Dios, por permitirme conseguir los fondos para costear mi carrera, por darme fuerzas para seguir adelante a pesar de los obstáculos. También le agradezco a Dios por darme paciencia y una visión clara de mis objetivos.

A Ángel Soto y Rosa Fernandez, por haber estado conmigo desde el inicio de la carrera, por haber confiado en mí, por su paciencia, dedicación y los buenos consejos. Siendo ellos mucho más que compañeros, siendo verdaderos amigos.

A mis padres Gerardo Mena y Katherine Estrella, les agradezco por haberme dado los consejos que me impulsaron a seguir adelante, sin ellos todo esto no hubiese sido posible. Les agradezco infinitamente ayudarme superar las barreras económicas para sustentar esta carrera y así poder conseguir mi sueño.

Gracias a nuestro asesor por brindarnos su muy apreciada ayuda.

Shade Yasmelys Estrella

AGRADECIMIENTOS

El libro Eclesiastés dice que hay tiempo para todo debajo sol y este es tiempo de agradecer a Dios por haberme puesto en una familia maravillosa.

Por haber puesto en mi camino a aquellos profesores que intentaron sacarme de mi caparazón, aun cuando me resistía.

Por haber puesto en mi camino a Ángel Soto y Shade Estrella, dos personas con la que nadie pensó que tendría química y henos aquí, amigos inseparables.

Gracias a Rosemary Ramírez, mi mama, y Martha Pérez, mi abuela, por haberme apoyado durante esta aventura que fue la universidad. Por haber estado ahí para mi cuando quería rendirme, por los consejos, por ser quienes son.

Gracias a Félix Rodríguez por ayudarnos a hacer todo esto posible.

Rosa Amelia Fernandez Ramírez

AGRADECIMIENTOS

Primero agradecer a Dios por darme la sabiduría y la valentía de culminar esta carrera universitaria también a mis padres Ángel Soto y Águeda Vargas, por el apoyo brindado, por los consejos, la paciencia y el compromiso de motivarme a seguir adelante.

A mis queridas compañeras Shade Estrella y Rosa Fernández por ser excelentes colaboradoras en este Trabajo de Grado. Gracias por estar ahí para mí, desde el principio de nuestra carrera, brindando su apoyo, siendo compañeros inseparables.

Gracias nuestro asesor por guiarnos en este arduo camino.

Ángel Vladimir Soto Vargas

DEDICATORIA

DEDICATORIA

Este trabajo de grado es el resultado de grandes sacrificios, superación, sabiduría, esfuerzo y mucha dedicación, este se lo dedico en primer lugar a Dios, por sus bendiciones y por brindarme la fortaleza para seguir hacia delante.

En segundo lugar, se lo dedico a mis padres Geraldo Mena y Katherine Estrella por su apoyo incondicional y por su esfuerzo y sacrificio. Las palabras no son suficientes para expresar todo el agradecimiento que siento hacia todas las personas que han sido mi soporte en todo este camino.

.

Shade Yasmelys Estrella

DEDICATORIA

Este trabajo de grado se lo dedico a mi madre, Rosemary Ramírez y a mi abuela, Martha Pérez por ser siempre mi apoyo cuando he estado por desistir. Gracias por su esfuerzo, sacrificio, motivación y su confianza en mí.

Rosa Amelia Fernandez Ramírez

DEDICATORIA

A mis queridos padres por apoyarme desde el principio, por los buenos consejos, por levantarme el ánimo y motivarme a seguir adelante a pesar de las adversidades. A mis familiares y a mis amigos por siempre creer en mí, por los buenos consejos y por ayudarme cuando más lo necesite.

Ángel Vladimir Soto Vargas

RESUMEN EJECUTIVO

El presente trabajo de grado consta de 4 capítulos y busca evaluar la implementación de un marco de gestión de la seguridad de la información apoyado en ISO 27000 en el departamento de TI y Seguridad de la Información del Banco Hacienda.

En el primer capítulo, le invitamos a conocer la historia de la seguridad de la información y la ciberseguridad, al igual que la banca mundial y local. El segundo capítulo describe la metodología utilizada en el trabajo mientras que el tercer capítulo recopila información sobre el Banco Hacienda, tales como su historia, organigrama institucional, marco de Gobierno y nivel de madurez de la institución.

En el cuarto capítulo se describen las buenas prácticas, políticas, controles y actividades plasmadas en la norma ISO 27001 versión 2013 para asegurar la seguridad de la organización. De igual forma son detallados los objetivos a conseguir con cada una de las políticas y controles.

Al dar lectura a este proyecto, comprenderán la importancia y beneficios de adoptar un Sistema de Gestión de Seguridad y establecer un Gobierno de TI en el sector bancario, debido a la naturaleza de los datos que manejan.

Los beneficios observables de la investigación incluyen el establecer un nivel de madurez en desarrollo del Banco Hacienda con respecto a la Norma ISO 27001, la disminución de riesgos de capital humano y recursos de tecnología de la información mantenimiento su integridad, disponibilidad y confidencialidad.

INTRODUCCIÓN

La información es uno de los activos más importante para los distintos tipos de Instituciones o Empresas, lo cual nos obliga a buscar alternativas cada vez más confiables para proteger la información de los posibles riesgos a los que se encuentra expuesta.

Un Sistema de Gestión de Seguridad de la Información (SGSI), busca poder gestionar los riesgos tecnológicos que pueden presentarse en las Instituciones o Empresas. Los SGSI permiten gestionar la seguridad de la información de una forma eficaz, permitiendo tomar medidas que mitiguen la probabilidad de que una amenaza se materialice, a través de políticas y controles, dando esto como resultado un menor costo para las Instituciones o Empresas.

Debido a que cada día surgen nuevas amenazas es casi imposible decir, un sistema es seguro en su totalidad, sin embargo, gracias a las diferentes leyes, normas, estándares y medidas es posible gestionar los daños por parte de intrusos.

A fin de cubrir este tema, se ha desarrollado este Trabajo de Grado de 4 capítulos:

Capítulo 1: son expuestos los fundamentos teóricos que sirven de apoyo para este Trabajo de Grado. Estos incluyen desde la historia de los bancos a nivel mundial, su desarrollo

local, aclaraciones sobre la seguridad de la información y las normas que servirán de apoyo a lo largo del desarrollo de este Trabajo de Grado.

Capítulo 2: es presentada la metodología utilizada para este Trabajo de Grado. Son detallados los instrumentos utilizados como encuestas y consulta de expertos en el área de seguridad de la información, de igual forma el objetivo perseguido y los resultados obtenidos.

Capítulo 3: se muestra a detalle la situación actual en el Banco Hacienda. Siendo su seguridad fundamentada en un REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN suministrado por la Superintendencia de Bancos SIB que expone los requerimientos de una forma muy subjetiva y que da cabida a la aplicación de la norma ISO 27001 cumpliendo con las regulaciones dispuestas por la SIB.

Capítulo 4: es explicada la propuesta de mejora a través de la aplicación de la norma ISO 27001. De igual forma se detallan los pasos a seguir para su correcta implementación, los involucrados y responsables de aprobar cada una de sus etapas. También resaltan los medios utilizados como políticas, procedimientos, controles y capacitaciones para lograr una exitosa aplicación de la norma en el Banco Hacienda.

CAPÍTULO 1: MARCO TEÓRICO REFERENCIAL

1.1. Seguridad de la información.

1.1.1. Historia.

“En la antigüedad el hombre se enfrentaba a diversos peligros que ponían en riesgo su supervivencia, de tal forma que centró sus esfuerzos en poner todos los medios necesarios para salvaguardar la. Debido a ello generó herramientas de protección ante los peligros que le acechaban, principalmente peligros naturales, como fuego, inundaciones, ataques de animales, etc. Dando lugar a las primeras armas para protegerse, creadas con elementos naturales como piedras, madera, etc., de forma natural estaba desarrollando la primera seguridad: Hoy en día el objetivo de la seguridad ha evolucionado, dejando atrás el único objetivo de preservar la especie humana y diversificándose, buscando otros orientados a la seguridad jurídica, económica, laboral, social, etc.

De la misma forma que los objetivos de la seguridad han ido evolucionando, la evolución de la seguridad en las empresas no ha quedado atrás y ha experimentado un cambio sustancial desde sus inicios, principalmente motivado por los avances tecnológicos a los que se ha visto expuesta.

En la década de los 70, la seguridad en las empresas estaba centrada en garantizar el buen uso de la información por parte de los empleados confiando en el sentido común para garantizar la seguridad de la organización. Sin embargo y debido a la inclusión y evolución de la tecnología, aparecieron nuevos riesgos que hicieron que esta “seguridad” quedará obsoleta.

Uno de los principales motivos por los que el avance de la tecnología propulsó un cambio en la tendencia de seguridad de las empresas vino motivado principalmente por los virus que se convirtieron en los principales motores de crecimiento para la Seguridad de la Información a nivel mundial debido a la globalidad de sus objetivos.” (INCIBE, 2015)

Algunos descubrimientos arqueológicos denotan con evidencias la importancia de la seguridad para las antiguas generaciones, entre estos tenemos las pirámides egipcias, el palacio de Sargón, el Dios egipcio Anubis, los Sumarios, el Código de Hammurabi, entre otros.

Hasta se dice que Julio César utilizaba esquemas de seguridad en época de guerra y en el gobierno.

La seguridad moderna se originó con la revolución industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero de la administración Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice: "salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y traiciones por parte del personal, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio."

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese los equipos, ni siquiera el empleado. Con la aparición de las computadoras, esta mentalidad se mantuvo, porque ¿Quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera.

Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio, desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en

este nuevo milenio.” (Pacheco, 2015)

1.1.2. Concepto.

La Seguridad de la Información hace alusión a las normas, estándares, políticas, procedimientos, técnicas y actividades enfocadas en proteger la información, para mantener la Confidencialidad, Integridad y Disponibilidad de esta.

La seguridad de la información es el conjunto de medidas preventivas y reactivas, de las organizaciones y de los sistemas tecnológicos, que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos. (Reis, 2018)

1.1.3. Ventajas.

- Cumplimiento:

  Cumplimiento de los aspectos relacionados con la información, como es la protección o seguridad de los datos, la privacidad o el control de la tecnología de la información (TI). (ISOTools, 2019)

- Descenso de los gastos por incidentes de seguridad:

  En el caso de la seguridad de la información, los beneficios no se aprecian en forma de ganancia económica evidente, sino que se observa que los gastos disminuyen en cuanto desciende el número de incidentes relacionados con seguridad. (ISOTools, 2019)

- Organización:

  Favorece el establecimiento y la asignación de roles, responsabilidades y obligaciones, ya que obliga a definirlos para su funcionamiento y buen desempeño. (ISOTools, 2019)

1.1.4. Desventajas.

- Costos de la implementación:

  El costo asociado a la implementación de un sistema de gestión, como es la norma ISO 27001, va a ir en función del tamaño, madurez y necesidades que tenga la empresa. No obstante, calcular los costos exactos antes de realizar una evaluación previa en cuanto a la protección necesaria y los riesgos a los que está expuesto, no sirve de nada. (ISOTools, 2019)

- Costes de la formación:

  Evidentemente, implementar la norma ISO 27001 supone ciertos cambios en la empresa, los cuales llevan asociados una serie de necesidades formativas. (ISOTools, 2019)

- Asesoría externa:

  En el caso de no disponer de personal formado y capacitado para ello, será preciso de asistencia externa, para procurar una asesoría experta. (ISOTools, 2019)

- Inversión en tecnología:

  Requieren de la optimización de la tecnología que ya tienen, aprendiendo a manejarla en función de los nuevos requerimientos de seguridad de la información. (ISOTools, 2019)

- Costos de certificación:

  Para obtenerla, se debe solicitar al organismo correspondiente la auditoría de certificación, cuyo costo irá en función del tiempo que empleen los auditores en realizarla. (ISOTools, 2019)

1.2. Norma matriz ISO 27000.

1.2.1. Origen.

"La norma ISO/IEC 27000 está conformada por varios libros que abarcan detalladamente la gestión de seguridad de la información. En la tabla a continuación podemos conocer todos los componentes de la familia ISO 27000.

- 27000: Vocabulario y definiciones
- 27001: Especificación de la estructura metodológica (basada en el BS7799-2:2002)– Norma Certificable
- 27002: Código de prácticas (basada en ISO17799:2005).
- 27003: Guía de implementación.
- 27004: Métricas y medidas.
- 27005: La Administración del Riesgo (basado BS 7799-3)" (Aguirre, 2017)

1.2.2. Versiones.

- 27000-norma madre de la seguridad. (ISO, 2018).

  Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044 con 27799 finalizando la serie formalmente en estos momentos.

  - ISO/IEC 27000:2016
  - ISO/IEC 27000:2018

- 27001-gestión de la seguridad de la información (ISO, 2013)
  - ISO/IEC 27001:2005
  - ISO/IEC 27001:2013
    - ISO/IEC 27001:2013/Cor 1:2014
    - ISO/IEC 27001:2013/Cor 2:2015
  - Publicada el 15 de octubre de 2005,
  - revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SCSI de las organizaciones.
  - En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015) y en diciembre de 2015 una segunda modificación (ISO/IEC 27001:2013/Cor.2:2015) esta última matizando especificaciones en la declaración de aplicabilidad.

- 27002-buenas prácticas (ISO, 2013)
    - ISO/IEC 27002:2005
    - ISO/IEC 27002:2013
        - ISO/IEC 27002:2013/Cor 1:2014
        - ISO/IEC 27002:2013/Cor 2:2015
    - Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.
    - Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013.

- 27003-guía para la implementación (ISO, 2017)
    - ISO/IEC 27003:2010
    - ISO/IEC 27003:2017
    - Publicada el 01 de febrero de 2010 y actualizada el 12 de abril de 2017. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001.

- Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI.” (ISO27000, s.f.)

- 27004-evaluación de la Seguridad (ISO, 2016)
  - ISO/IEC 27004:2009
  - ISO/IEC 27004:2016

- 27005-recomendaciones y directrices generales para la gestión de riesgo (ISO, 2018)
  - ISO/IEC 27005:2011
  - ISO/IEC 27005:2018
  - ISO/IEC WD 27005

1.2.3. Concepto.

Es un conjunto de estándares desarrollados en fase de desarrollo por ISO (International Organization for Standardization) 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. (ISO27000, s.f.)

1.2.4. Normas asociadas.

- COBIT

  "Es un modelo para auditar la gestión y el control de los sistemas de información y tecnología, orientado a todos los sectores de una organización." (Julio Ernesto Mora Aristega, s.f.)

- ITIL V3

  ITIL (Information Technology Infrastructure Library - Biblioteca de Infraestructura de Tecnologías de Información), es un marco de trabajo para las mejores prácticas con el fin de facilitar la entrega de servicios de Tecnologías de la Información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. (Wilson Javier Aguasaco Flórez, 2016)

- NIST 800-34

  “Es una guía para la implementación de planes de contingencia para TI, identifica principios fundamentales de planificación basándose en el ámbito del gobierno de TI.” (Moreno, s.f.)

- Metodología Margerit V3

  Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los Sistemas de Información; fue creada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000. (Molina-Miranda, 2017)

1.3. Gestión de la Seguridad de la información.

1.3.1. Historia.

La Seguridad de la Información no es, necesariamente, una práctica nacida con la era de la Información. Desde los tiempos antes de Cristo ha existido la necesidad de proteger la información y tener alguna manera de detectar si dicha correspondencia ha sido alterada mientras estaba siendo transportada.

Ejemplos tempranos de esta necesidad son las historias de Heródoto, los mensajeros y el cifrado de César o desplazamiento de César.

En sus cuentos antes de la guerra persa, Heródoto cuenta como los dueños de esclavos les rapaban la cabeza a sus esclavos para tatuarles mensajes en esta. Luego de que les creciera el pelo, los esclavos eran enviados a los recipientes del mensaje. (Dubois, 2003)

Tanto en la historia como en la mitología vemos que existían los mensajeros; personas preseleccionadas, entrenadas y de confianza que transportaban comunicaciones con informaciones críticas.

Por otro lado, el cifrado César, usualmente atribuido al emperador Romano Julio César, quien aproximadamente en el año 50 a.C. ideó este mecanismo de codificación para evitar que sus mensajes fueron leídos por enemigos. Este cifrado codifica los mensajes al mover el orden predeterminado del alfabeto un número dado de veces. Para decodificar el mensaje completo solo se necesitaba conocer cuántas letras se movió el alfabeto, así que, incluso si se desconoce la clave, podía determinarse rápidamente mediante pruebas de ensayo y error. Por lo que se empezó a utilizar múltiples cifrados de sustitución en el mismo mensaje y se incrementó la cantidad de claves requeridas para decodificarlos. Esto les agrego un nuevo nivel de dificultad puesto que se requería mucho más tiempo para llegar al mensaje. A estos mecanismos se les fueron sumando herramientas tales como la caja fuerte, organizaciones gubernamentales y máquinas de rotores. (Arizzi, s.f.)

Uno de estos artilugios es la afamada máquina Enigma, utilizada por los alemanes durante la Segunda Guerra Mundial. Con ella se podía preestablecer una llave y ella se encargaba de encriptar un mensaje dado combinando múltiples cifrados de sustitución en secuencia. Sus mensajes fueron desencriptados con la máquina de Turing, antepasado de la computadora y la computación moderna. (Arizzi, s.f.)

Con la amplia aceptación de la Computadora y las tecnologías de la información, surgieron algunos inconvenientes no considerados. Uno de los primeros problemas que debió ser resuelto en la década de los 1960s era el acceso no autorizado a los ordenadores de la organización, y por proxy, a la información. De aquí nacieron las primeras contraseñas y los controles de acceso. Otra medida popularizada en esta década fue la protección contra fuego y desastres naturales. Después de todo, plataformas basadas en la nube tales como iCloud o Google Drive aún no existían.

En la década de los 70s, surge un nuevo aspecto de la Seguridad de la Información, la ciberseguridad. Bob Thomas, un investigador estadounidense, creó un programa sencillo y no malicioso que solo imprimía un mensaje diciendo ‘Soy el Creeper, encuéntrame si pueden’ mientras se desplazaba por los nodos de la entonces ARPANET. Otro investigador conocido como Ray Tomlinson, tomó el Creeper y lo modifico para que fuera auto replicante; más adelante, diseñó otro programa llamado Reaper que seguía el rastro dejado por Creeper y lo eliminaba. Estos son los primeros ejemplos de un virus de computadora y un antivirus. (Chen, 2005)

A finales de los 70 y durante los 80s, comienza a hacerse aparente otro problema que aún nos afecta y que tendría un boom en las décadas siguientes: los hackers de computadora y los cibercrímenes. A medida que más y más computadoras se conectaban vía cable de teléfono a la ARPANET, individuos como Markus Hess se infiltraron en la red a larga distancia con la finalidad de obtener información militar que luego sería vendida al mejor postor, aprovechándose de vulnerabilidades en los sistemas de antaño. (Rosteck, s.f.)

Otra demostración de lo dañino que pueden ser los ciberataques es el virus Morris de 1988. Su desarrollador, Robert Morris, lo creo con la intención de que fuera indetectable, pero hubo un fallo en sus cálculos. El virus era auto replicante, el problema es que hacía demasiadas copias de sí mismo, lo que ralentizaba enormemente las máquinas y las redes infectadas, en algunas instancias dejándolas inoperables. Esta fue la razón por la cual fue detectado y se pudo reparar las vulnerabilidades que explotaba.

Gracias a este evento, Robert Morris se convirtió en la primera persona en ser llevada a juicio y ser sentenciado por un delito tecnológico. El virus Morris hizo ver que tener una contraseña o mecanismos de seguridad en un equipo dado no era suficiente. Se necesitaba un grupo de expertos dedicados a prevenir incidentes de seguridad informática. A raíz de este hecho, se funda el Equipo Informático de Respuesta a Emergencias estadounidense, CERT por sus siglas en inglés. También se hizo aparente la necesidad de organizaciones dedicadas al desarrollo de acciones preventivas y reactivas estandarizadas ante eventualidades de seguridad en ordenadores y otros equipos informáticos. (Kelty, 2011)

Es en este periodo de tiempo que se empieza a aceptar que la Seguridad de la Información debe ser gestionada activamente a través de políticas sistemáticas, de extensa documentación y estas deben ser conocidas por toda la organización. Es con esta realización que empezamos a ver los primeros estándares internacionales de Seguridad y los primeros SGSI o Sistema de Gestión de la Seguridad de la información. (Murphey, s.f.)

Un Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos alineados con los objetivos de negocio de la institución, con el objetivo de mantener un nivel de exposición menor al nivel de riesgo que la organización ha decidido tomar.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante procesos previamente definidos, documentados y dados a conocer a todo aquel que vaya a trabajar con la información; estos procesos o políticas son revisados y mejorados constantemente. (Murphey, s.f.)

1.3.2. Conceptos.

"Información cualquier comunicación o representación de conocimiento como hechos, datos u opiniones en cualquier medio o forma, incluidos textos, numérico, gráfico, cartográfico, narrativo o audiovisual.

Seguridad de la Información: "son las medidas y procesos utilizados para salvaguardar la información de las organizaciones, independientemente de la forma en que esta se encuentre desde documentos escritos, comunicados verbales y la propiedad digital e intelectual de una organización. Este término suele utilizarse como sinónimo de la ciberseguridad, sin embargo, esto es un error." (NIST, 2019)

Ciberseguridad: "es una rama multidisciplinaria que se encarga de preservar la confidencialidad, integridad y disponibilidad de cualquier activo digital, incluyendo, pero no limitándose a:

- Redes,
- Hardware,
- Información digital

Confidencialidad: “es la protección de la información contra el acceso no autorizado o la divulgación de esta. Tiene diferentes grados, ya que información personal o financiera requiere un mayor grado de confidencialidad que, por ejemplo, un memorándum de una reunión. “(NIST, 2019)

Integridad: “se define como la protección de la información contra modificaciones no aprobadas. La integridad de un activo digital puede ser controlada a través de registros de acceso, criptografía, firmas digitales, cifrado y controles de acceso. “(NIST, 2019)

Disponibilidad: “esta garantiza el acceso oportuno a la información o los sistemas que la contengan. Incluye salvaguardar los datos para que no sean eliminados accidental o malintencionadamente. Es de alta importancia debido a que puede afectar la capacidad para tomar decisiones. Puede ser protegida haciendo uso de redundancia, copias de seguridad y controles de acceso.

Evento o eventualidad: “es cualquier cambio, error o interrupción dentro de una infraestructura de TI, tales como un fallo del sistema, un error de disco o que un usuario olvide su clave de acceso.

Incidente: violación o amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas de seguridad estándar." (NIST, 2019)

Riesgo: "nivel de impacto en las operaciones de la organización (incluida la misión, funciones, imagen o reputación), activos organizacionales o individuos resultante de la operación de un sistema de información dado el impacto potencial de una amenaza y la probabilidad de que ocurra esa amenaza. "(NIST, 2019)

Amenaza: "cualquier eventualidad con el potencial de impactar negativamente las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos de la organización, individuos, otras organizaciones o la nación a través de un sistema de información haciendo uso de acceso no autorizado, destrucción, divulgación, modificación de información y / o negación de servicios. "(NIST, 2019)

Gobierno de TI: "se define como los procesos que aseguran el uso efectivo y eficiente de TI para permitir que una organización alcance sus objetivos. Está a cargo de la gerencia de una organización y entre otras cosas, proporciona orientación estratégica, determina si los riesgos están siendo gestionados correctamente y verifica que los recursos de la organización son usados concienzudamente. "(NIST, 2019)

Gestión del Riesgo: "es el proceso por el cual una organización trata de mantener sus riesgos en niveles tolerables. Requiere el desarrollo e implementación de controles

internos para gestionar y mitigar los riesgos de la organización en conjunto, incluyendo, pero no limitándose a: riesgos financieros, físicos y cibernéticos.

Respuesta a incidentes - es un programa formal que prepara una entidad para responder ante un incidente dado.” (NIST, 2019)

Firewall: “una puerta de enlace que limita el acceso entre redes de acuerdo con la política de seguridad de la organización.” (NIST, 2019)

1.3.3. Ventajas.

Las ventajas de la Gestión de la Seguridad de la Información se hacen obvias a medida que se investiga el tema. Entre las principales ventajas encontramos:

- Asegura la información en cualquier estado en que esta se encuentre, ya sea papel, propiedad intelectual, datos en dispositivos como USB, discos duros y hasta la nube.
- Aumenta la tolerancia y resistencia contra ataques cibernéticos.
- Ofrece protección para toda la organización al considerar tanto riesgos tecnológicos como procesos ineficientes o personal con poco o ningún conocimiento en materia de seguridad.
- Reduce gastos y costos gracias a la gestión y análisis de riesgos, los cuales pueden evitar utilizar más medidas defensivas de las necesarias y viceversa.
- Hace énfasis en salvaguardar los Datos bajo los pilares de la seguridad (integridad, confidencialidad y disponibilidad).

- Mejora la cultura del negocio al educar a los empleados sobre los riesgos y controles de seguridad que deben seguirse en las actividades de la entidad.
- Gestionar la seguridad de nuestra organización también puede ser utilizada como una ventaja competitiva.
- Se reducen riesgos relacionados con la pérdida de información.

1.3.4 Metodología de gestión.

La implementación de una gestión eficaz de la Seguridad de la Información (incluida la gestión y mitigación de riesgos) requiere una estrategia de gestión continua que siga el ciclo de Deming (PHCA o Planificación, Hacer, Checar y Actuar):

- **Planificación (P)**: Identificar problemas y riesgos, recopilar información útil para evaluar los riesgos de seguridad. Definir políticas y procesos de seguridad que se puedan utilizar para abordar las problemáticas que puedan presentarse. Identificar y clasificar los recursos a nuestra disposición.
- **Hacer (H)**: Implementar las políticas y procedimientos definidos previamente según los recursos disponibles. Entrenar a los recursos.
- **Checar (C)**: Es de suma importancia monitorear la efectividad de las políticas, procesos y controles establecidos por el SGSI y así evaluar los resultados tangibles.

- **Actuar (A)**: Se debe documentar los resultados obtenidos previamente y utilizar un ciclo de retroalimentación para futuras iteraciones de las políticas y controles del SGSI en el siguiente ciclo para mejora continua.

Para lograr todo esto nos valemos de Marcos de referencias (framework) internacionales para la seguridad de la información, los cuales nos brindan una guía para lograr nuestros objetivos de seguridad.

Uno de los más populares es la ISO 27001. Aparte de este, contamos con ITIL, un Marcos de referencias bastante extendido para la Gestión de los Servicios, que cuenta con un componente dedicado exclusivamente a la Gestión de la Seguridad, cuyo propósito es alinear la gestión del servicio tecnológico con la seguridad del negocio, garantizando así que la seguridad de la información abarque todas las actividades de la organización.

Según ITIL, los objetivos de la Gestión de la seguridad de la información son garantizar que:

- La información está disponible y se puede usar cuando se requiere, y los sistemas que la proporcionan pueden resistir adecuadamente los ataques y recuperarse o prevenir fallas (disponibilidad).
- La información es observada o divulgada solo a quienes tienen derecho a conocerla (confidencialidad).

- La información es completa, precisa y está protegida contra modificaciones no autorizadas (integridad).
- Se puede confiar en las transacciones comerciales, así como los intercambios de información entre empresas o socios (autenticidad y no repudio).

Otro Marcos de referencias muy conocido para la gestión de la seguridad es COBIT, actualmente en su versión 2019, que se enfoca en el apoyo a las instituciones en el fortalecimiento del gobierno y la gestión de TI. Además, provee un modelo de Gobierno que busca mejorar el control sobre las tecnologías de la información y la comprensión y gestión de los riesgos asociados a estas. Los dominios de COBIT 2019 son: Dominio Planificación y Organizar (PO), Dominio Adquirir e Implementar (AI), Dominio Entregar y Soporte (DS) y Dominio Monitorear y Evaluar (ME).

Aprovechamos este inciso para hablar del NIST y su framework de ciberseguridad. El Instituto Nacional de Estándares y Tecnología fue fundado en 1901 como un laboratorio de ciencias, buscando mejorar la competitividad industrial de los Estados Unidos.

Una infinidad de instrumentos tales como los relojes atómicos, nanomateriales, chips de computadoras, entre otros dependen enteramente de la tecnología, medidas y estándares que esta organización ha desarrollado.

En los últimos años, han desarrollado un Marcos de referencias para el manejo de la infraestructura crítica de las organizaciones, proporcionando una reseña de las mejores prácticas en el mercado para soportar la toma de decisiones. Es conocido como NIST Cybersecurity Framework y surge ante el aumento de complejidad de las amenazas cibernéticas, que han comenzado a poner en riesgo no solo a las empresas, sino también la seguridad Nacional, la económica y hasta la salud de los ciudadanos.

1.4. Entidad de intermediación financiera (EIF).

1.4.1. Historia mundial.

"En Roma también tenían personas que manejaban las finanzas por especialidades: Los nummularis encargados de actividades cambistas y el argentarius encargados de actividades banqueras. Estos grupos decidieron aplicarse y distinguirse en las actividades bancarias, dejando como antecedente la Función Bancaria Pública.

Todo lo antes mencionado, fue el principio del desarrollo en actividades financieras y comerciales en Roma, entre ellas; cambios de monedas, transporte del dinero, recibían depósitos regulares e irregulares, había servicio de caja, intervenían en la compra y venta de muebles e inmuebles y en subastas públicas,

pero su principal actividad era el préstamo como inversión de capital propio y ajeno.

La contabilidad romana era controlada por una especie de Codex o libro de cuentas corrientes que era firmado por el deudor y dos testigos, libro que hiciera obligatorio el emperador Justiniano, así como el libro de caja, que registraba entradas y salidas de dinero.

Edad Media

Génova fue una ciudad muy activa en cuestiones bancarias, en el siglo XII ya se conocía a los banchieri (banquero, especialista en el manejo del dinero.) para designar a los cambistas que operaban sentados en sus bancos en Plazas Públicas, como los Trapezitas de la época antigua. Durante esta época, el comercio del dinero, aunque en forma rudimentaria, estaba confiado a los cambistas locales para que reconocieran las monedas acuñadas de diversas ciudades e identificaran a las que fueran falsas, también establecen con precisión el contenido y peso correcto de metal precioso.

Es el año 1400, en Génova, cuando la palabra banco comienza a diferenciarse para designar a esas entidades, lo anterior fue a partir del Banco de San Jorge de Génova que fuera creado en un sentido moderno en el año 1407 ya que anteriormente era conocido como Casa de San Jorge. Dicho banco se dividía en

dos secciones: la primera, recibía depósitos y efectuaba giroconti; la segunda, surgió como una administración autónoma de la deuda pública de Génova, acordaba préstamos a los encargados de los impuestos y de la República excepto a los particulares.

En cuanto al origen de la palabra banco, se sabe que es el derivado del nombre del mueble que utilizaban los cambistas italianos al igual que lo usaron los trapezita en la antigüedad.

En el siglo XII surgen los bancos privados, es así como se funda el Banco de San Giorgio en Génova, recibía depósitos sin interés y realizaba cambios de moneda, también se establece el Banco Vital o Fondo Común de Venecia, recibía monedas y lingotes que se registraban tomando como base de medida unitaria el peso del metal, en vez de unidades monetarias, por lo que los asientos en los libros se hacían en presencia de los interesados. Para finales de la Edad Media surgen los bancos de Estocolmo y Ámsterdam, en ellos ya no era necesaria la presencia de los interesados para operar, por lo que para algunas personas este hecho representa el antecedente de billete de banco.

Fueron los siglos del XII al XIV cuando se crearon una gran variedad de operaciones: depósitos a interés, préstamos, anticipos, giros, inversiones, así como, el perfeccionamiento de la contabilidad y el sistema de partida doble.

Época Moderna

Los grandes descubrimientos; las grandes guerras y movimientos populares; la moneda de oro que fuera el medio de cambio los últimos siglos de la edad Media y sustituida por monedas de plata, y la existencia de las rapiñas, provocaron que cambiará el rumbo del desarrollo económico, los tráficos marítimos cambiaron del Mediterráneo al Atlántico, debilitándose por causa de las guerras, el cambio de moneda provocó alteraciones por el valor del título y peso de las mismas, finalmente los saqueos y robos agravaron la ya difícil economía de los Estados Europeos.

La necesidad económica surgió en forma inmediata, los príncipes demandaban grandes cantidades de dinero para abastecer a sus soldados con nuevas armas para defenderse en las guerras, mejor conocidas como las cruzadas. La población en general demandaba dinero, se llegó al momento en que se carecía de dinero y aparecieron los sustitutos de este: letras de cambio, pagarés y otros documentos, es decir, la moneda bancaria.

La mayoría de los bancos en sus inicios habían sido Montes de Piedad, que luego de algún tiempo, o bien, luego de problemas en los mismos, se fueron fusionando con otros Montes para dar paso a instituciones bancarias

Fue Inglaterra, el país que mayor experiencia adquirió en funciones bancarias, gracias a la habilidad de la Reina Isabel (1533-1603), que promovió a la industria y el comercio, bajo los consejos de Sir Thomas Gresham (1519-1579) que fuera el primer banquero economista inglés.

Para el año 1844, se establece la primera centralización bancaria, quedando prohibido el establecimiento de nuevos bancos emisores, siendo el Banco de Inglaterra el más importante de los bancos, dejando de ser banca privada para convertirse en el primer Banco Central y de Emisión. Una de las aportaciones más importantes fue la creación de billetes de banco como sustituto del dinero metálico. Al Banco de Inglaterra se deben grandes aportaciones históricas como: el cheque, las notas de caja, las letras de cambio, los pagarés y las obligaciones.

En 1920, Estados Unidos de América fue el país que desplazó a Inglaterra en cuestiones bancarias, ya que el dominio del dólar sobre la libra esterlina fue determinante.” (Guerra Martinez, 2002)

1.4.2. Evolución local.

"La Supervisión Bancaria, en la República Dominicana, se remonta al año 1869 cuando se creó el Banco Nacional de Santo Domingo como primera entidad de esta naturaleza que aparece posterior a la independencia de la República.

En 1909 Se promulga la primera legislación bancaria la cual estaba bajo la responsabilidad de la Secretaría de Hacienda y Comercio (Finanzas) y cuya finalidad era el control de las operaciones bancarias y autorización de sucursales por parte del Estado Dominicano a través de interventores (o inspectores).

La creación del Banco Central, el signo monetario nacional y a su vez se promulga la Ley No. 1530 el 9 de octubre de 1947, la cual creó la Superintendencia de Bancos." (Superintendencia de Bancos, s.f.)

"El Advenimiento de cambios en la economía dominicana, acompañado de la presencia de nuevas entidades financieras (Banco Popular, Asociaciones de Ahorros y Préstamos) auspiciaron cambios profundos en la supervisión bancaria a través de la nueva Ley No. 708 o Ley General de Bancos del 14 de abril del 1965.

La Ley General de Bancos, No. 708, a partir de entonces se convirtió en el soporte legal del crecimiento y expansión del sistema financiero dominicano.

Hubo debilidad del Sistema Financiero Dominicano y necesidad de modificar la Ley General de Bancos, acompañada de una independencia de la Superintendencia de Bancos ya que esta estaba subordinada a la Secretaría de Estado de Finanzas, situación que cada vez más promovía la debilidad de la Supervisión Bancaria." (Superintendencia de Bancos, s.f.)

"Se promulga una nueva ley denominada Ley Monetaria y Financiera o Ley 183-02, de noviembre del 2002, la cual derogó la Ley No. 708. Esta procuraba:

- Mayores controles de las entidades financieras.
- Mayor fortaleza en su capital y reservas.
- Mejora en la Cartera de Préstamos.
- Desarticular las malas prácticas Bancarias
- Establecer una mejor Política de Supervisión Bancaria.
- Adecuación a los 25 principios de Basilea I.
- Que las entidades Bancarias respondan al índice de solvencia de 10%.
- Reducir el riesgo crediticio.
- Establecer los reglamentos y normativas que logren la aplicación de la Ley, etc." (Superintendencia de Bancos, s.f.)

1.5. Superintendencia de Bancos.

1.5.1. Origen.

"El año 1947 marcó la transformación del Sistema Financiero Dominicano se crea la Unidad Monetaria Dominicana, el Banco Central y la Superintendencia de Bancos, esta última bajo la Ley No. 1530 del 9 de octubre del 1947, fue la que creó los cimientos para la supervisión y regulación del Sistema Financiero Dominicano.

El economista Virgilio Álvarez Sánchez, fue el primero en ocupar el cargo de Superintendente de Bancos, posición que ocupó durante dos años."
(Superintendencia de Bancos, s.f.)

"En principio, la tarea de supervisión que desempeñaba esta entidad era bien simple considerando lo limitado de las operaciones comerciales de esa época y su función principal consistía en la autorización de nuevas oficinas. La Ley No. 1530 que dio origen a la Superintendencia de Bancos fue modificada y sustituida por la Ley No. 708, Ley General de Bancos, del 14 de abril del 1965, donde se pone a cargo de esta entidad la aplicación y administración del régimen legal de los bancos, bajo la dependencia de la Secretaría de Estado de Finanzas, hoy Ministerio de Hacienda.

El 3 de febrero del 1967, mediante decreto del poder ejecutivo se dictó el Reglamento No. 934 “Reglamento Interior de la Superintendencia de Bancos”, en cuyo contenido se establecieron las funciones del Superintendente de Bancos y la Organización General de la Superintendencia de Bancos, así como la Estructura Organizativa formal.” (Superintendencia de Bancos, s.f.)

1.5.2. Propósito.

“De acuerdo con el Artículo 19 de la Ley No. 183–02, Monetaria y Financiera del 21 de noviembre de 2002, la Superintendencia de Bancos tiene por función:

- “Realizar, con plena autonomía funcional, la supervisión de las entidades de intermediación financiera, con el objeto de verificar el cumplimiento por parte de dichas entidades de lo dispuesto en esta Ley, Reglamentos, Instructivos y Circulares; requerir la constitución de provisiones para cubrir riesgos;
- Exigir la regularización de los incumplimientos a las disposiciones legales y reglamentarias vigentes;
- Imponer las correspondientes sanciones, a excepción de las que aplique el Banco Central en virtud de la citada ley.
- Autorizaciones o revocaciones de entidades financieras que deba evaluar la Junta Monetaria.
- Sin perjuicio de su potestad de dictar Instructivos y de la iniciativa reglamentaria de la Junta Monetaria, la Superintendencia de Bancos puede

proponer a dicho Organismo los proyectos de Reglamentos en las materias propias de su ámbito de competencia.” (Superintendencia de Bancos, s.f.)

1.5.3. Evolución.

Con la creación de la Ley No. 183–02 Monetaria y Financiera, se le da a la Superintendencia de Bancos el marco jurídico de actuación que tiene en la actualidad, otorgándole la responsabilidad de supervisar, con plena autonomía, a las instituciones de intermediación financiera, con el propósito de proteger los fondos de los ahorrantes y los derechos de los usuarios de los servicios financieros. Así mismo, con la promulgación de esta ley, el Superintendente de Bancos se incorpora como miembro ex oficio de la Junta Monetaria. (Superintendencia de Bancos, s.f.)

Debido al vertiginoso crecimiento experimentado por el Sistema Financiero, tanto en el aspecto institucional como en el operativo, la Superintendencia de Bancos se ha visto en la necesidad de adecuar su estructura en múltiples ocasiones para asimilar dichos cambios, enmarcándose, en una profunda transformación de su marco regulatorio y de supervisión, pasando de un modelo de cumplimiento a un modelo de supervisión consolidado basado en riesgos. (Superintendencia de Bancos, s.f.)

Resumen Capitulo 1.

Desde principios de la historia humana, el hombre ha buscado formas de proteger primero su seguridad física, más adelante su seguridad tecnológica incluyendo la seguridad de la información. Pasando de confiar en quienes tienen acceso a la información a asegurarse de tener el control, esto provocado por la aparición de virus y ataques cibernéticos.

Por este motivo surge la seguridad de la información, que consiste en un conjunto de técnicas, normas y políticas enfocadas en mantener la confiabilidad, disponibilidad e integridad de las informaciones. Logrando disminuir los gastos debido a amenazas materializadas y mejorando la distribución de responsabilidades. Todo esto apoyado en la familia de normas ISO 27000 en especial la ISO 27001 en su versión 2013, que proporciona las bases para la implementación de un SGSI.

Al igual que las distintas Instituciones y Empresas, los bancos tiene la necesidad de resguardar la información, aunque es mucho más delicado que la mayoría. Siendo los bancos originados de métodos antiguos de negociaciones para convertirse en lo que son hoy, uno de los órganos que permiten obtener capital para lograr distintos objetivos. Estos regulados localmente por la Superintendencia de Bancos.

CAPÍTULO 2: ASPECTOS METODOLÓGICOS

2.1. Tipos de estudio.

Serán realizados estudios cualitativos y cuantitativos. En el caso cualitativo se utilizará para aquellos indicadores que requieran preguntas abiertas para medir percepción entre otros aspectos. El enfoque cuantitativo será empleado tanto para preguntas cerradas o de opción múltiple, estudios estadísticos, fuentes históricas medibles y para verificar nivel de cumplimiento de normativas.

2.1.1. Descriptivo

Este estudio persigue describir cómo se desarrolla el problema. Este tipo de estudio servirá para describir la problemática, en miras a entender mejor las vulnerabilidades.

2.1.2. Explicativo

Este estudio persigue analizar las causas que originan el problema. Esto a partir de las informaciones obtenidas en la investigación.

2.1.3. Por observación

Este estudio persigue la recolección de información mediante el análisis de los casos que se presenten a lo largo de la investigación, utilizando técnicas de observación.

2.2. Métodos de investigación

2.2.1. Método analítico

Será aplicado en esta investigación para el desglose de las causas que atentan contra la adecuada gestión de la seguridad de la información en el Banco Hacienda.

2.2.2. Método Deductivo

Se partirá del argumento proporcionado por la hipótesis descrita anteproyecto de grado, para llegar a las conclusiones de este trabajo de investigación. En primera instancia, se considerarán los principales motivos para aplicar las políticas de seguridad basadas en la norma ISO 27001:2013, así como los factores que impactan la seguridad de la información de la institución.

2.3. Técnicas de recolección de información

2.3.1. Encuestas

Se realizarán preguntas para validar los conocimientos y nivel de madurez que poseen colaboradores y clientes del banco Hacienda relacionados con la gestión de seguridad de la información.

De igual forma al personal de TI y a la parte gerencial, para saber cómo se comporta el banco ante la materialización de riesgos, haciendo hincapié en los procesos y pasos a seguir.

2.3.2. Consulta de expertos

Se consultará con un especialista certificado en ISO 27001:2013, con la finalidad de disponer del juicio de expertos acreditados en la materia para el trabajo de investigación de acuerdo con experiencias reales y conocimientos profesionales.

Resumen capítulo 2.

Han sido explicados el tipo de estudio a realizar, siendo este cualitativo y cuantitativo. Además, fueron detallados las técnicas de recolección de información a emplear, tales como entrevistas, consulta a expertos y encuestas y la forma en que esta fue llevada a cabo, detallando las técnicas empleadas en miras a obtener los datos necesarios.

CAPÍTULO 3: DIAGNÓSTICO DE LA GESTIÓN ACTUAL DE SEGURIDAD DE LA INFORMACIÓN EN EL BANCO HACIENDA.

3.1. Sobre el BANCO HACIENDA.

3.1.1. Historia.

El Banco Hacienda de la República Dominicana fue creado mediante la Ley Núm. 908, del 1 de junio de 1945, con el nombre original de Banco Hacienda e Hipotecario de la República Dominicana.

En el proceso de conformación del sistema financiero nacional, el Banco Hacienda e Hipotecario de la República Dominicana fue la segunda institución bancaria creada en el país, después del Banco de Reservas, establecido en el año 1941.

El Banco Hacienda e Hipotecario inició sus operaciones con un capital originalmente fijado en RD$2.0 millones, a partir de la inauguración de su primera oficina oficial localizada en el número 17 de la calle Colón en la ciudad capital, el 29 de agosto de 1945.

El Banco vino a llenar una sentida necesidad de la sociedad dominicana, relacionada con el financiamiento de las actividades productivas en la agricultura, la industria y los negocios en general. Para el siguiente año ya tenía instaladas sendas sucursales en las ciudades de Santiago y Barahona.

Posteriormente, ya promulgada la Ley Monetaria y creado el Banco Central, en el 1948, mediante la Ley Núm. 1779, del 18 de agosto de ese año, se cambió el nombre

de la institución por el de “Banco Hacienda e Industrial de la República Dominicana”, denominación más ajustada a las operaciones que realizaba este organismo en esa época.

El Banco se mantuvo operando en esas condiciones por un largo periodo, hasta los primeros años de la década de los 60, durante ese tiempo la institución extendió sus operaciones a todas las regiones del país y desempeñó un rol de primer orden en el financiamiento de las actividades productivas de los sectores agropecuarios e industriales, que para esa época aportaban alrededor del 50% del producto bruto interno.

Mediante la ley Núm. 3827, del 23 de febrero de 1962, se le asignó el nombre de "Banco Hacienda". (SISMAP, s.f.)

3.1.2. Misión, Visión y Valores.

Misión:

Ofrecer servicios crediticios diversificados, para mejorar la producción y productividad en la zona rural, mediante un permanente esfuerzo de capitalización y modernización con tecnología de punta, revalorizando y comercializando sus activos con un personal capacitado y motivado.

Visión

Mantener el liderazgo en el financiamiento al sector agropecuario y responder a las necesidades de los productores con autosuficiencia económica, adecuada infraestructura física, tecnología moderna, recursos humanos comprometidos y una amplia cobertura de la cartera que irradie credibilidad, seguridad y confianza.

Valores

- Servicio
- Calidad
- Eficiencia
- Confianza
- Creatividad
- Trabajo en equipo.

(Banco Hacienda, 2016)

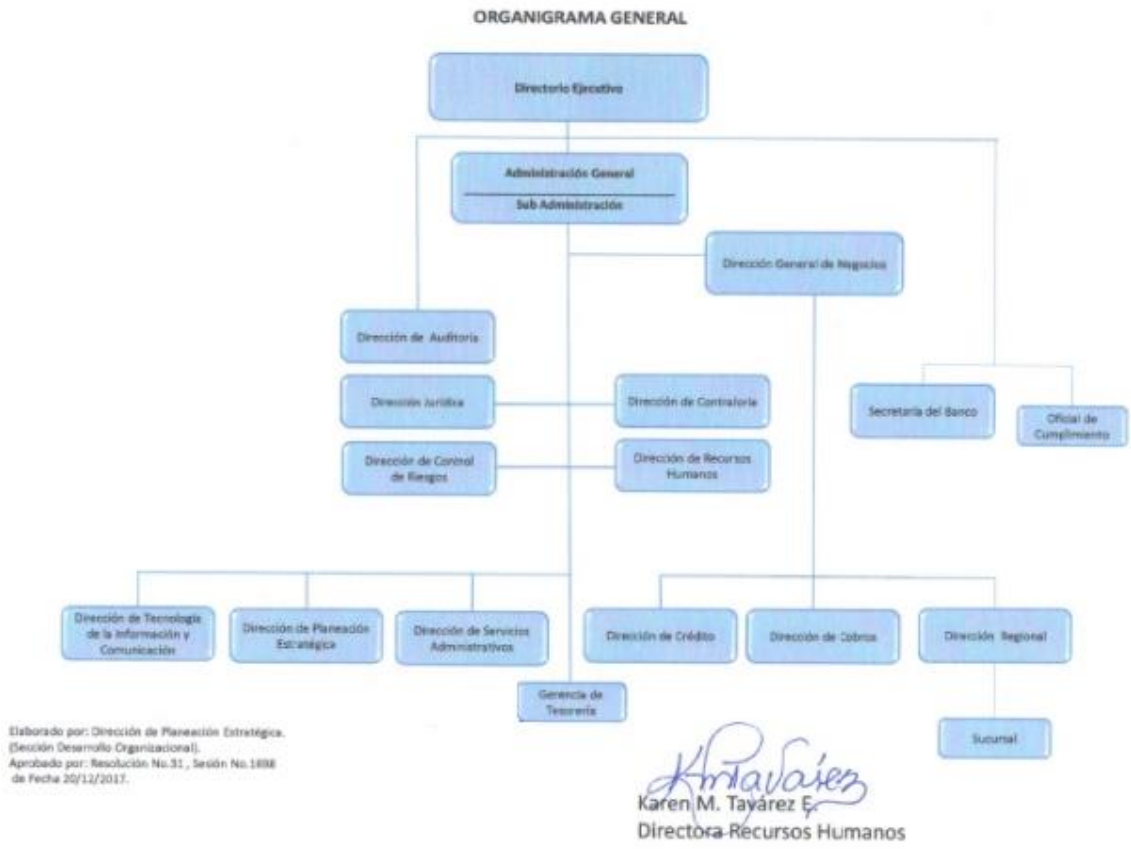
3.1.3. Objetivos Estratégicos.

- "Incrementar la rentabilidad del Banco.
- Mantener bajos niveles de morosidad.
- Contar con un fondeo de bajo costo y diversificado.
- Ser reconocido como un Banco del Sistema Financiero.
- Lograr el saneamiento de los estados financieros y hacer la publicación reglamentaria en medios de información pública.
- Utilizar eficientemente los recursos.

- Gestionar nuevas fuentes de fondeo.
- Promover el incremento de la captación de ahorros y valores del público.
- Impulsar la modificación de la Ley de Alquileres como instrumento especial de captación de recursos de bajo costo y largo plazo, esencialmente para fomento y desarrollo.
- Establecimiento de estructuras y procesos de mercado para los productos y servicios de la Institución.” (Banco Hacienda, s.f.)

3.1.4. Estructura organizacional

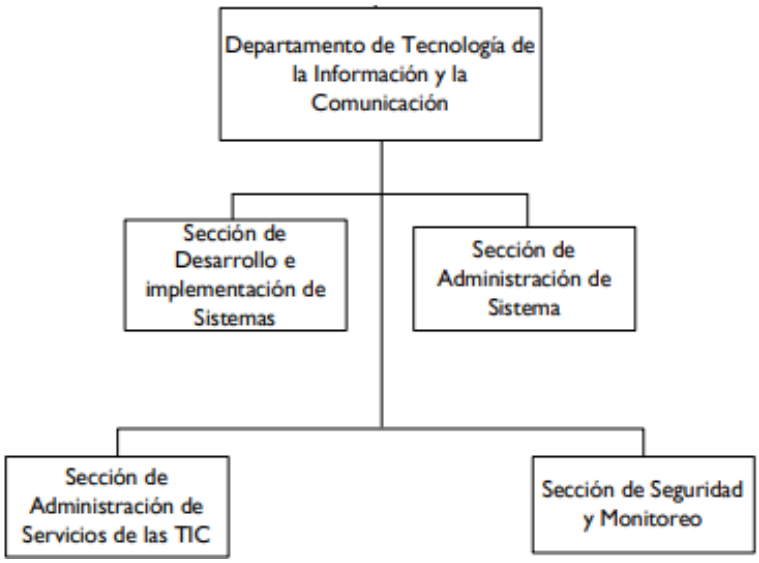
Organigrama General.



(Banco Hacienda, 2017) Ilustración del Organigrama institucional.

Estructura de tecnología.

Organigrama Dirección Tecnología de la información y comunicación.



(Banco Hacienda, s.f.) Ilustración del Organigrama departamental

Estructura de Seguridad de la Información.

El Departamento Sección de Seguridad y Monitoreo cuenta con las siguientes posiciones:

- Técnico de backup TIC.
- Técnico administrador y monitoreo de la seguridad.
- Técnico de seguridad de accesos.

(MAP, 2019)

3.1.5. Marco de Gobierno y Gestión Empresarial y de TI.

Actualmente, el Banco Hacienda no cuenta con un marco de Gobierno y Gestión Empresarial y de TI. Sin embargo, se apoyan en el REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN promulgado por la Superintendencia de Bancos de la República Dominicana (SIB). (Superintendencia de Bancos, 2018)

3.2. Estado actual del BANCO HACIENDA.

El departamento Sección de Seguridad y Monitoreo tiene las siguientes funciones:

- Administrar y coordinar diariamente el proceso de seguridad informática.
- Asegurar el buen funcionamiento del proceso de Seguridad Informática, realizando verificaciones periódicas a los diferentes niveles de seguridad de los sistemas informáticos.
- Guiar al cuerpo directivo, a la administración y a los usuarios de la organización ante posibles incidentes de seguridad mediante un Plan de Respuesta a Incidentes.
- Proponer y coordinar análisis de riesgos.
- Recomendar y presentar propuestas de políticas y procedimientos que fortalezcan la seguridad informática.

- Promover la creación y actualización de las políticas de seguridad informática.
- Elaborar planes de respuesta a incidentes de seguridad.
- Atender y responder inmediatamente las notificaciones de sospecha de un incidente o catástrofe de seguridad real.
- Llevar registro de los archivos lógicos y su contenido, así como de las claves de acceso de los sistemas informáticos.
- Supervisar la seguridad física de los archivos lógicos y procurar que tengan sus respectivos Backup (copias).
- Verificar la correcta ejecución de los procesos de respaldo (backup), así como el control del reemplazo de las cintas para su flujo.
- Funciones de help desk.
- Configuración y manejo de los firewalls de la institución, controlando así el acceso de los equipos a la red. (Banco Hacienda, s.f)

3.3. Beneficios proyectados contra el estado actual.

Los beneficios que aporta la implementación de la norma ISO 27001 se centran en los siguientes campos:

- **En el ámbito de la empresa**,
    - Beneficios proyectados: se genera un importante compromiso con la seguridad de la información. La existencia de registros y medidas de control permiten que la seguridad de la información quede garantizada en la empresa y que estos esfuerzos puedan demostrarse. (ISO 27001: ¿Qué beneficios nos aporta implantar esta norma?, 2016)
    - Estado Actual: es regida por especificaciones generales, por ejemplo

        > "Tomar medidas razonables y efectivas para procurar la protección de la información, los sistemas y la infraestructura tecnológica, frente a los ataques cibernéticos o incidentes relacionados con la seguridad de la información." (Superintendencia de Bancos, s.f.)

- **En el cumplimiento legal de las exigencias**
    - Beneficios proyectados: manifiesto de la conformidad de la organización en el cumplimiento de todos los requisitos legales que le son de aplicación para la región en la que la empresa tenga su domicilio y para la actividad que realice. (ISO 27001: ¿Qué beneficios nos aporta implantar esta norma?, 2016)
    - Estado Actual: es regido por el REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN. Este reglamento es quien dicta las directrices a seguir en ámbito de seguridad a nivel bancario que además tiene la flexibilidad de permitir la aplicación de estándares

y normas internacionales como es la ISO 27001:2013. (Superintendencia de Bancos, s.f.)

- **En el ámbito funcional**
    - Beneficios proyectados: se desarrolla una adecuada gestión de los riesgos. La organización conoce de manera exhaustiva su empresa y los sistemas de información que aplican, los problemas que se producen y los medios de protección que se aplican, para así terminar garantizando la mejora disponibilidad de los materiales y datos, además de asegurarse de su continuidad sin alteraciones perniciosas no controladas. (ISO 27001: ¿Qué beneficios nos aporta implantar esta norma?, 2016)

    - Estado Actual: las políticas y procedimientos definidos actualmente permiten tener cierto control sobre los recursos y su seguridad, sin embargo, no pueden garantizar la disponibilidad de los materiales y datos.

- **En el aspecto comercial**
    - Beneficios proyectados: se genera cierta credibilidad y confianza entre nuestros clientes. Debemos tener presente siempre que nos encontramos ante una sociedad que tiene falta de confianza de nuestros clientes que afecta a nuestras ventas de la misma forma que la calidad y la funcionalidad de nuestros productos, por lo tanto, se debe cuidar

tanto un aspecto como el otro. (ISO 27001: ¿Qué beneficios nos aporta implantar esta norma?, 2016)

- Estado Actual: en la actualidad el banco muestra muy buena reputación económica, siendo una de las primeras opciones, sin embargo, debido a su desfase tecnológico muchos procesos son manuales, provocando cierto escepticismo de su capacidad de resguardarse de ataques cibernéticos.

- **En el aspecto financiero**
  - Beneficios proyectados: las empresas consiguen reducir los costes que se encuentran vinculados a todos los incidentes y se consiguen minimizar las primas de seguros. (ISO 27001: ¿Qué beneficios nos aporta implantar esta norma?, 2016)
  - Estado Actual: los incidentes ocurridos anteriormente en el banco, aunque no han sido de gran impacto, han sido muestra de la vulnerabilidad, provocando gastos en materia de corrección de errores.

- **En el aspecto humano**
  - Beneficios proyectados: se produce una sensibilización del personal en relación con la importancia de la correcta manipulación de la información, dentro de la aplicación adecuada a las medidas de seguridad que deben adoptarse y a las responsabilidades personales y de la organización con relación a la información de la que disponen,

además de los dueños de la información. (ISO 27001: ¿Qué beneficios nos aporta implantar esta norma?, 2016)

- Estado Actual: los colaboradores resguardan la información sensible, sin embargo, los mecanismos disponibles no son los más recomendables.

3.4. Especificaciones de requerimientos.

En algún momento se debe ser comprobada su viabilidad técnica y que los procedimientos establecidos fueron seguidos de una manera correcta. La principal recomendación es proporcionada por el control en la norma ISO 27001. Se tiene que definir todos los parámetros de una manera clara y los resultados se deben cumplir. (ISO 27001 ¿Cuáles son los requisitos de seguridad?, 2017)

Requisitos de capacitación de los colaboradores:

- Definir un plan de capacitación y concientización continua para colaboradores internos y externos.
- Definir política de sanciones por incumplimiento de los lineamientos de seguridad.

Requisitos de documentación del SGSI:

ISO 27001:2013 requiere que se confeccione la siguiente documentación:

- Definir alcance y límites del SGSI.

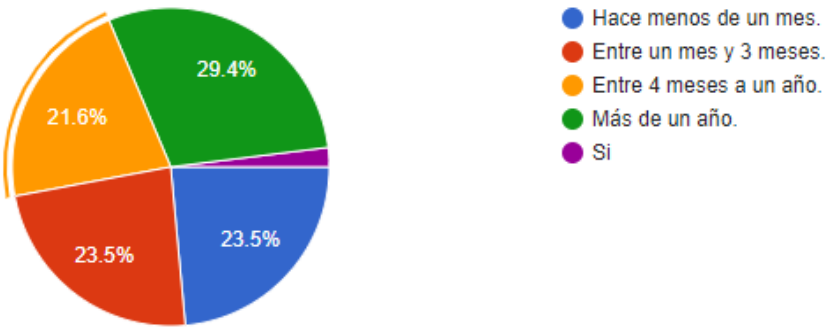
- Definir políticas y objetivos del SGSI.
- Definir validación del Riesgo.
- Identificar los Riesgos.
    - Inventario de activos
- Analizar y evaluar los Riesgos. (Espinosa, 2016)
- "Selección de objetivos de control y controles.
    - Procedimientos para continuidad del negocio
    - Monitoreo y resultados de medición
    - Programa de auditoría interna
    - Registros sobre actividades de los usuarios, excepciones y eventos de seguridad
- Determinar Riesgos residuales.
    - Resultados de medidas correctivas
- Preparar declaración de aceptabilidad.
- Preparar plan de tratamiento de Riesgos.
    - Definición de roles y responsabilidades de seguridad
    - Política de seguridad para proveedores" (¿Qué es norma ISO 27001?, s.f.)

3.5. Análisis de datos.

3.5.1. Encuestas

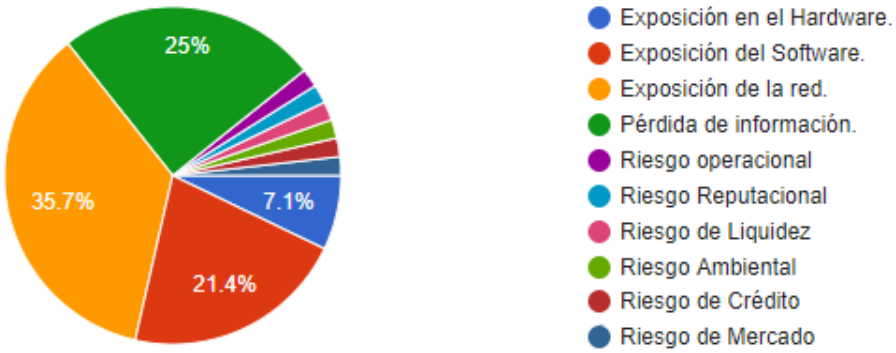
Fue evaluada una muestra de 101 usuarios pertenecientes a distintas entidades financieras como bancos, asociaciones, cooperativas y financieras.

- ¿Cuándo fue el último incidente de Seguridad de la Información ocurrido en el banco?



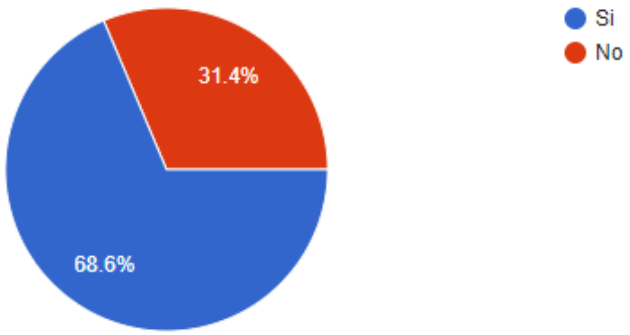
Se determinó que la gran mayoría de EIF están recibiendo ataques en un periodo menor a los 4 meses, por lo que es necesario reforzar la seguridad.

- ¿Qué tipo de evento se presentó?



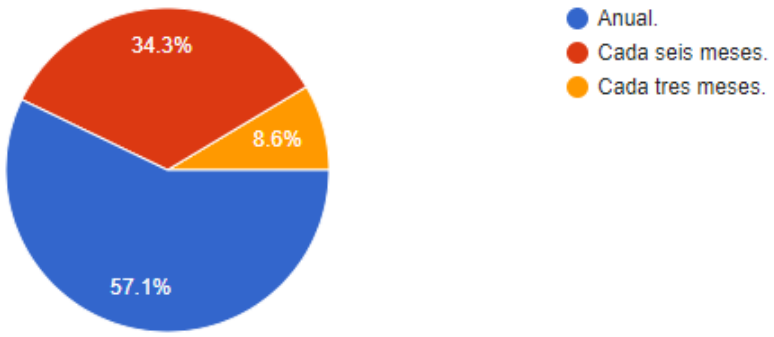
Se evidencia que la mayor vulnerabilidad de los sistemas de las EIF está relacionada a la seguridad de la red y pérdida de información.

- ¿Pudo la organización resolver la situación según el SLA (tiempo de respuesta) establecido?



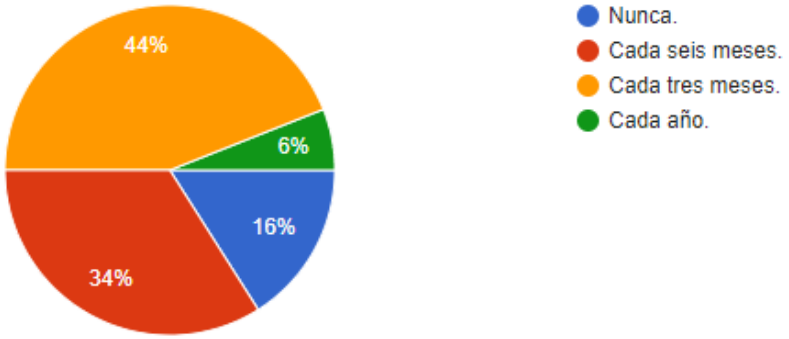
Se percibe una buena respuesta luego de ocurrido el incidente, en miras a corregir la situación. Sin embargo, esto provoca pérdidas en las EIF y un daño reputacional en caso de darse a conocer.

- ¿En caso de ser si, con qué frecuencia se realiza una auditoría de seguridad en su lugar de trabajo?



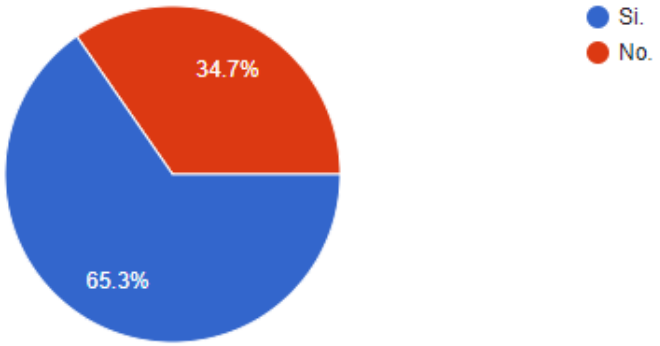
A pesar de estar la mayor parte de los incidentes en un rango de 4 meses, según los primeros resultados, la frecuencia de las auditorías no corresponde al mismo margen. Siendo una de las pautas principales cambiar la recurrencia de las auditorías a 6 meses o a un tiempo menor según lo requiera la organización, en miras a preservar la confidencialidad, integridad y disponibilidad de los recursos de las EIF.

- ¿Con qué frecuencia el personal de TI realiza actualizaciones a su ordenador de trabajo?



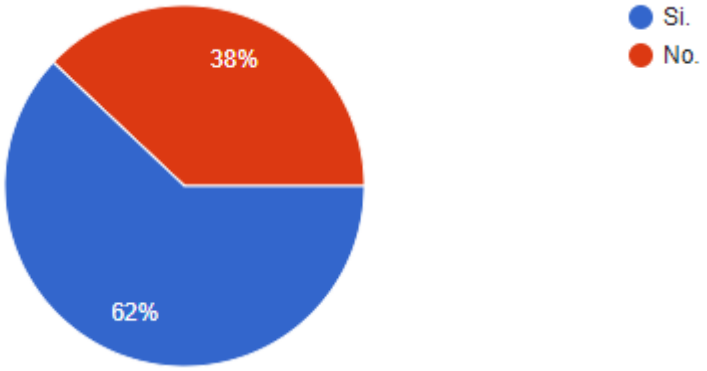
Se puede observar un 78% de las muestras tienen un mantenimiento de aplicaciones de los ordenadores igual o menor a 6 meses.

- ¿Su lugar de trabajo cuenta con un plan de contingencia en caso presentarse un ataque cibernético?

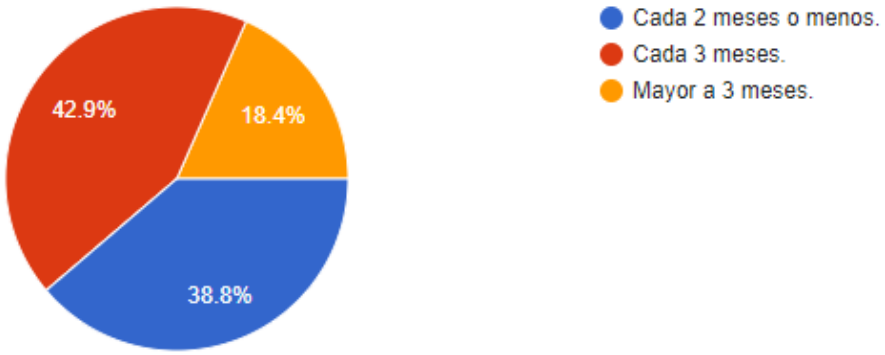


Cabe destacar que una parte de la población de respuesta “no” se debe a que desconocen la misma y a un sistema de capacitación deficiente.

- ¿La empresa cuenta con un canal para reportar brechas de seguridad?

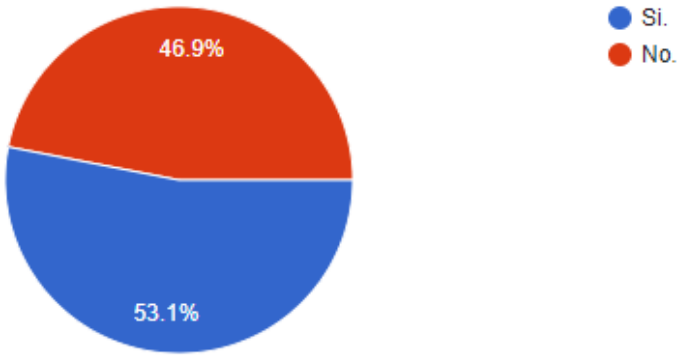


- ¿Qué frecuencia tiene el cambio de contraseña de las computadoras en su trabajo?



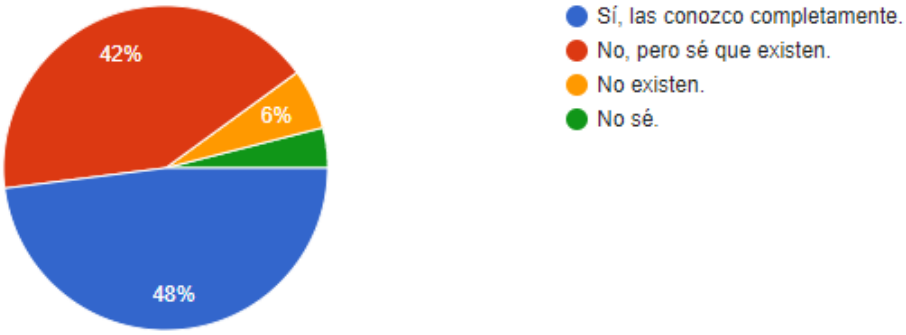
Es más que claro el nivel de resguardo de los equipos de colaboradores, siendo más del 80% de los ordenadores, actualizado con regularidad.

- ¿Ha recibido alguna capacitación sobre la gestión de seguridad de la información?



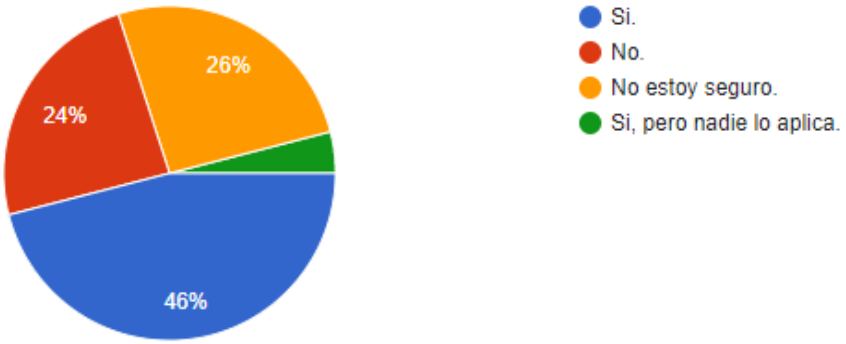
La mayoría de las instituciones cuentan algún tipo de capacitación para sus colaboradores, sin embargo, en mucho de los casos es limitado. Por otro lado, es preocupante el 46.9% que no está siendo entrenado para enfrentarse a los ciberataques.

- ¿Conoce usted sobre las políticas de seguridad informática en su trabajo?



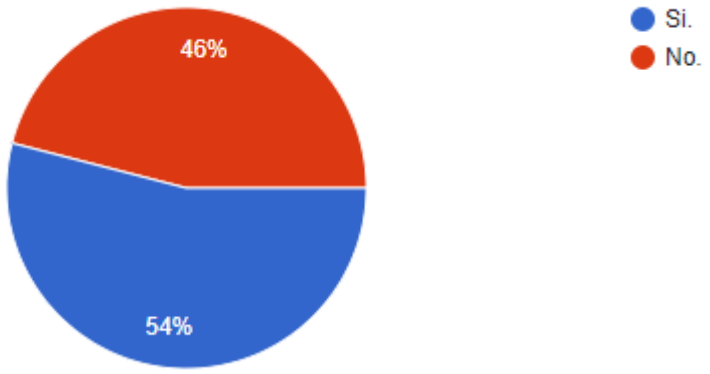
Con relación al gráfico anterior se denota que un 48% conoce las políticas de seguridad de su organización, por otro lado, es de notar que un 42% sabe que existen, pero no las conocen.

- ¿La empresa te exige encriptar la información sobre los clientes?



Se observa que más de 50% de los casos se encuentra expuesto a robo de información.

- ¿Ha presenciado usted una auditoría de seguridad en su lugar de trabajo?



3.5.2. Consulta de expertos

El experto en SGSI nos externó sus recomendaciones y puntos claves. Estas fueron algunas de las preguntas realizadas:

- ¿Qué recomendaciones nos daría para evaluar la implementación de la norma ISO 27001 en un banco?

  Bueno, a mi entender pueden orientar su esfuerzo en estos temas:

  Fortaleza en las políticas y procedimientos de seguridad y protección de la información. Sobre todo, deben tener clara la relación de un SGSI con las normas asociadas, por ejemplo, COBIT, ISO 31000 entre otras.

- ¿Qué tipo de capacitación se le debería dar al personal o debería tener antes de iniciar con el proceso?

Las capacitaciones pueden ir orientadas en:

Las mejores prácticas de seguridad. Esto para asegurarnos que no se estén tomando atajos que luego puedan poner en riesgo la triada de los datos o exponer la red.

El uso aceptable de los equipos. Más que nada es concientización de lo que debemos y que no debemos hacer con los recursos de la organización.

Es esencial que revisemos el nivel de experiencia del personal líder del área de seguridad, además de sus acreditaciones y formación en materia de seguridad.

Se debe tener muy claro que la seguridad no solo depende del equipo de TI, por lo que es necesario el adiestramiento del personal ajeno a TI o SI. Dicho de otra forma, todo el personal debería orientarse en los temas de seguridad.

Resumen capítulo 3.

El Banco Hacienda fundado el 1 de junio de 1945 con la misión de ofrecer servicios crediticios diversos en miras a mejorar la producción rural. Con una organización departamental u organigrama bastante detallado.

Aun así, con una infraestructura tecnológica respecto a la seguridad con grandes oportunidades de mejora. Dentro de ellos, la ausencia prácticamente de un Marco de Gobierno y Gestión Empresarial basado en el REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN proporcionado por la Superintendencia de Bancos SIB.

Luego de que sea implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) se proyectan beneficios como mejor imagen ante la población, disminuyendo el riesgo reputacional, mejora continua de los procesos del Banco Hacienda, se reducen los costos asociados a los incidentes y un mayor compromiso con la seguridad de la información por parte de los empleados.

CAPÍTULO 4: EVALUAR LA IMPLEMENTACIÓN DE UN MARCO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APOYADO EN ISO 27001:2013 PARA EL DEPARTAMENTO DE TI Y SEGURIDAD DE LA INFORMACIÓN DEL BANCO HACIENDA.

4.1. Evaluación de los requerimientos.

Requisitos de capacitación de los colaboradores:

- Definir un plan de capacitación y concientización continua para los colaboradores internos y externos.

Es necesario capacitaciones que abarquen todas las personas que laboren en el banco. Estas capacitaciones serán dirigidas según los perfiles que tengan asignado. A su vez los gerentes serán quienes determinen las necesidades de capacitación del personal a su cargo en relación directa con lo especificado en los perfiles del cargo y los objetivos del Banco Hacienda.

Es considerado capacitación como:

“Proceso dinámico de enseñanza-aprendizaje, planeado, intencionado y progresivo; a través del cual los empleados adquieren conocimientos y desarrollan habilidades y actitudes basados en las necesidades reales y específicas de un área o de la organización en general. La Capacitación puede darse por personal de la propia organización.”

Los medios de capacitación aceptados son:

- Charla
- Conferencia
- Seminario

- Demostración
- Video
- Separata
- Libro
- Simulacro
- Práctica
- Prueba

Estas capacitaciones deben ser agendadas en el mes de octubre para dar inicio en enero del año posterior acorde a los resultados de las evaluaciones realizadas.

Los gerentes de cada área deben presentar las constancias de participación del personal a su cargo en la oficina del presidente ejecutivo del Banco Hacienda. La fecha prevista para estas entregas es septiembre de cada año.

En caso de no ser satisfactorias las capacitaciones, la asistente de Recursos Humanos en conjunto con el Director de Control de Riesgos deben establecer las medidas de lugar.

Las capacitaciones impartidas deben sumar al menos un total de 128 horas anuales, siendo impartidas en las instalaciones del Banco Hacienda.” (Luque, 2019)

Requisitos de documentación del SGSI:

ISO 27001:2013 requiere que se confeccione la siguiente documentación:

- Analizar y evaluar los Riesgos.

  Se calcula el riesgo actual, Para determinar el riesgo se multiplican los valores asignados a la probabilidad de una amenaza por los valores asignados a la magnitud del impacto, creando una matriz que se denomina mapa de riesgo

  - Se define una escala de riesgos con los niveles Alto, Medio Alto, Medio, Medio Bajo, Bajo y las acciones que debe tomar la dirección y responsables.
  - Se marca un nivel sobre el impacto en la información (disponibilidad, confiabilidad, integridad)
  - Con estos niveles se procede a realizar el cálculo del riesgo que será la multiplicación entre la probabilidad y el impacto en la información. Se crea una tabla con escenario, probabilidad (nivel/calificación), Impacto operación (nivel/calificación), Resultado Riesgo.” (Arango, 2016)

- **Definir alcance y límites del SGSI.**

“Este Trabajo de Grado abarca las áreas más vulnerables del Banco Hacienda y TI. El alcance del proyecto abarca solo el Proceso de evaluación de la Gestión de la seguridad, para la sede principal del Banco Hacienda, por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos sólo se realizará para la sede antes mencionada.

Para el desarrollo de este Trabajo de Grado se utilizará como guía principal la norma ISO 27001 versión 2013, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

Este Trabajo de Grado consistirá solo en la evaluación y análisis del Sistema de Gestión de Seguridad de la Información para el Banco Hacienda, basado en la norma ISO 27001:2013." (Silva, 2015)

- **Definir validación del Riesgo.**

  "Los criterios de aceptación de riesgo demandados por Banco Hacienda establece que riesgos de niveles "Alto" y "Medio Alto" se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios requeridos.

  Así mismo para los niveles Medio y bajo su tratamiento depende del aporte del control para mitigar riesgos, la relación costo/beneficio y la contribución que este aporte al cumplimiento de los objetivos del negocio."

  (Arango, 2016)

- **"Identificar los Riesgos.**
  - Inventario de activos

- Activo de información

  Datos de clientes, datos de proveedores, Documentos Físicos, manuales. Inventarios de hardware, contratos con terceros, otros.

- Software y licencias

  Software SO licenciado, Software ofimático licenciado, licencias de uso de software en outsourcing, otras licencias

- Instalación red eléctrica

  Red e instalaciones eléctricas para computadores, (norma RETIE), sistema de protección de aterrizaje eléctrico (polo o malla a tierra)

- Servicios de terceros

  Conectividad a internet, mantenimiento y soporte de hardware, mantenimiento y soporte de software, soporte y actualizaciones en software en outsourcing.

- "Selección de objetivos de control y controles.
  - Procedimientos para continuidad del negocio

    La gestión de la continuidad del negocio hace parte de la gestión del riesgo operacional de la alta gerencia y se debe realizar para que la operatividad del negocio continúe de una manera razonable, con el fin

de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en las operaciones de la empresa.

No debe ser sólo medidas reactivas, sino que se requiere de un proceso de planeación exhaustivo y sistemático en el que se involucre el personal, la tecnología y por supuesta la infraestructura.

Este plan de continuidad de negocio debe contener:

- Plan de gestión de la crisis.
- Plan de comunicación.
- Plan de gestión del personal.
- Plan de recuperación de la infraestructura.
- Plan de recuperación de sistemas de información.
- Plan de mantenimiento.” (Amaya Guzman, s.f.)

- Monitoreo y resultados de medición

  Definir los lineamientos para las auditorías por parte del Departamento Sección de Seguridad y Monitoreo. (Quisoboni, 2017)

- Programa de auditoría interna

  Evaluar la auditoría, solicitar evaluación de auditores de forma periódica cada año. (Quisoboni, 2017)

- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad.

La seguridad de la información no es sólo cuestión de tener nombres de usuario y contraseñas, sino que requiere de reglamentos y diversas políticas de privacidad y protección de datos que imponen unas obligaciones para organizaciones, igualmente debe ser integral y encajar en una empresa sin problemas, además de lo mencionado: seguridad del personal, control de acceso de usuarios, debe contener: seguridad de red y aspectos regulatorios. (Martelo, 2015)

- Determinar Riesgos residuales.
    - Resultados de medidas correctivas

      Se debe determinar niveles de riesgo aceptable y riesgo residual. (Solarte, 2015)

- Preparar declaración de aceptabilidad.

  Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de estos.

  La declaración debe contener todos los objetivos de control y los controles contemplados por el Sistema de Gestión de Seguridad de la Información (SGSI), los cuales se concluyó en los resultados de los procesos de evaluación y tratamiento del riesgo. (Mora Palacios, 2017)

- Preparar plan de tratamiento de Riesgos.
    - Definición de roles y responsabilidades de seguridad

      Esto será definido por el Departamento Sección de Seguridad y Monitoreo.

- Política de seguridad para proveedores.

  Debe ser definida una política de seguridad en cuanto a los lineamientos de seguridad para la relación con los proveedores con el propósito de evitar accesos no autorizados a la información. (NIEVES, 2017)

4.2. Definir áreas, procesos y sistemas.

La norma ISO27001:2013 exige que sean identificadas las áreas, proceso y sistemas involucradas por los cambios a realizar. El Gerente del Departamento Sección de Seguridad y Monitoreo, el Director de Control de Riesgos y el equipo de implementación tendrán como responsabilidad realizar el levantamiento de las funciones de las áreas, procesos y sistemas en cuestión.

"Áreas involucradas:

- Dirección Ejecutiva.
- Dirección de Auditoría.
- Dirección de Tecnología de la Información y Comunicación.
  - Sección Desarrollo e Implementación de Sistemas.
  - Sección de Seguridad y Monitoreo.
  - Sección de Administración de Sistema.
- Dirección de Recursos Humanos.
- Dirección de Control de Riesgos." (Banco Hacienda, 2017)

4.3. Definir aprobaciones necesarias.

Es necesaria la participación y aprobación de los siguientes recursos, tanto en la elaboración del documento de aceptabilidad como la aprobación de este:

- Director Ejecutivo
- Director TIC
- Director de Control de Riesgos

4.4. Definir dominios, objetivos de control y controles de la norma ISO 27001 ha ser aplicados.

“Los objetivos de control definen meta perseguida por el control implementado.

El esquema que será utilizado es Dominio, Control, Objetivo de Control.

- Política de seguridad.
    - Política de Supervisión Bancaria
        - Definir los criterios para la toma de decisiones.
    - Política de sanciones
        - Definir las acciones a tomar en caso de faltas leves, moderadas o graves.

    - Política de seguridad para proveedores
        - Describir los requerimientos mínimos necesario para ser aceptado como proveedor y los lineamientos a seguir en todo el ciclo.
    - Política General de Seguridad de la Información
        - Definir los procedimientos y las políticas de apoyo para los distintos para evitar violaciones de seguridad.” (ISO, 2013)

- “Organización de la seguridad.
    - Separación de Roles.
        - Restringir acceso a los distintos sistemas.
    - Definición autorizaciones requeridas.
        - Comprobación de expertos antes de aplicar cambios.
- Gestión de activos.
    - Identificación de los activos de información.
        - Definir el uso correcto y ubicación de los activos del Banco Hacienda.
- Seguridad del Recurso Humano.
    - Definir responsabilidades de los colaboradores internos y externos del Banco Hacienda.
        - Asegurar que las tareas tengan un responsable.
    - Asignación de Roles.
        - Homogeneizar las funciones de los equipos.

- Seguridad Física y del entorno.
    - Control de acceso.
        - Denegar el paso a personal no autorizado.
    - Control de identificación.
        - Conceder accesos según perfil asignado.
    - Perfiles de seguridad.
        - Definir grupos por nivel de acceso.
    - Código vestimenta y utensilios.
        - Restringir el uso de vestimentas y herramientas que puedan prestarse para violar la seguridad del Banco Hacienda.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
    - Protocolos de pase a producción.
        - Homologar los sistemas.
        - Asegurar que cumplan con los requerimientos mínimos aceptables.
- Gestión de la continuidad del negocio.
    - Protocolos de operación en ubicación foránea.
        - Preservar las operaciones del Banco Hacienda en su mínima capacidad aceptable en caso de algún siniestro.
    - Definición de concurrencia de las copias de respaldo de los sistemas.
        - Preservar las informaciones de los clientes.” (Salcedo, 2014)

4.5. Definir cronograma de actividades del Proyecto planeación de la implementación.

ID	Task Mode	Task Name	Duration	Start	Finish	Cost	Resource Names	Predecessors
1		**Proyecto de implementación**	**24 days**	**Wed 3/11/20**	**Mon 4/13/20**	**$1,294,400.00**		
2		**Identificar Riesgos**	**2.5 days**	**Wed 3/11/20**	**Fri 3/13/20**	**$76,800.00**		
3		Identificar Riesgos	1 day	**Wed 3/11/20**	Wed 3/11/20	$33,600.00	Experto ISO27000,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2	
4		Evaluar los riesgos	1 day	Thu 3/12/20	Thu 3/12/20	$26,400.00	Técnico Seguridad 3,Técnico Seguridad 4,Técnico TIC 1,Experto ISO27000	3
5		Fijar responsables	0.5 days	Fri 3/13/20	Fri 3/13/20	$16,800.00	Experto ISO27000,Project CEO,Project Owner	4
6		**Idenfiticar los objetivos**	**2 days**	**Mon 3/16/20**	**Tue 3/17/20**	**$120,000.00**		**2**
7		Definir objetivos	1 day	Mon 3/16/20	Mon 3/16/20	$64,000.00	Director Auditoria,Director Ejecutivo,Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico TIC 1	
8		Definir áreas responsables	1 day	Tue 3/17/20	Tue 3/17/20	$56,000.00	Director Auditoria,Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico TIC 1	7
9		**Definir Alcance y limites del SGSI**	**2 days**	**Wed 3/18/20**	**Thu 3/19/20**	**$240,000.00**		**6**
10		Alcance	1 day	Wed 3/18/20	Wed 3/18/20	$64,000.00	Director Auditoria,Director Ejecutivo,Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico TIC 1	
11		Limitantes	1 day	Wed 3/18/20	Wed 3/18/20	$56,000.00	Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico TIC 1,Director Auditoria	
12		Definir tiempos	1 day	Wed 3/18/20	Wed 3/18/20	$56,000.00	Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico TIC 1,Director Auditoria	
13		Definir Declaración de aceptabilidad	1 day	**Thu 3/19/20**	Thu 3/19/20	$64,000.00	Director Auditoria,Director Ejecutivo,Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico TIC 1	10,11,12
14		**Definir politicas**	**6 days**	**Fri 3/20/20**	**Fri 3/27/20**	**$305,600.00**		
15		Politica general de seguridad de la información	1 day	Fri 3/20/20	Fri 3/20/20	$57,600.00	Director Auditoria,Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2	
16		Politica de uso adecuado de los recursos	1 day	Mon 3/23/20	Mon 3/23/20	$49,600.00	Director Auditoria,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 3,Técnico Seguridad 4	15

ID	Task Mode	Task Name	Duration	Start	Finish	Cost	Resource Names	Predecessors
17		Politica de Gestión de activos	1 day	Tue 3/24/20	Tue 3/24/20	$49,600.00	Director Auditoria,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 3,Técnico Seguridad 4	16
18		Politica de seguridad fisica y del entorno	1 day	Wed 3/25/20	Wed 3/25/20	$49,600.00	Director Auditoria,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 3,Técnico Seguridad 4	17
19		Politica de Adquisición, desarrollo y mantenimient	1 day	Thu 3/26/20	Thu 3/26/20	$49,600.00	Director Auditoria,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 3,Técnico Seguridad 4	18
20		Política de seguridad para proveedores	1 day	Fri 3/27/20	Fri 3/27/20	$49,600.00	Director Auditoria,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 3,Técnico Seguridad 4	19
21		**Definir Registros de usuarios**	**1 day**	**Mon 3/30/20**	**Mon 3/30/20**	**$47,200.00**		**14**
22		Definir proceder por evento	1 day	**Mon 3/30/20**	Mon 3/30/20	$47,200.00	Director Auditoria,Director TIC,Experto ISO27000,Técnico Seguridad 1,Técnico Seguridad 2,Técnico TIC 1,Técnico TIC 2,Técnico TIC 3	
23		Definir controles	3 days	Tue 3/31/20	Thu 4/2/20	$148,800.00	Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2,Técnico Seguridad 3,Técnico Seguridad 4	21
24		**Definir Objetivos de control**	**4 days**	**Mon 4/6/20**	**Thu 4/9/20**	**$220,800.00**		**23**
25		Definir Plan de Continuidad del negocio	2 days	Mon 4/6/20	Tue 4/7/20	$108,800.00	Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2,Técnico Seguridad 3,Técnico Seguridad 4,Técnico TIC 1,Técnico TIC 2	
26		Monitoreo y resultados	0.5 days	Mon 4/6/20	Mon 4/6/20	$20,800.00	Experto ISO27000,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2,Técnico Seguridad 3,Técnico Seguridad 4	
27		Identificar Riesgos residuales	0.5 days	Tue 4/7/20	Tue 4/7/20	$20,800.00	Experto ISO27000,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2,Técnico Seguridad 3,Técnico Seguridad 4	26
28		Verificar declaración de aceptabilidad	1 day	Wed 4/8/20	Thu 4/9/20	$70,400.00	Director Auditoria,Director Ejecutivo,Director TIC,Experto ISO27000,Project CEO,Project Owner,Técnico Seguridad 1,Técnico Seguridad 2,Técnico TIC 1,Técnico TIC 2	27
29		Definir proceso de auditoria	1 day	Fri 4/10/20	Fri 4/10/20	$44,000.00	Director Auditoria,Experto ISO27000,Project Owner,Técnico Seguridad 3,Técnico Seguridad 4,Técnico TIC 3	24
30		**Definir plan de capacitaciones**	**3 days**	**Thu 4/9/20**	**Mon 4/13/20**	**$91,200.00**		**24**
31		Definir tipos de capacitaciones	0.5 days	**Thu 4/9/20**	Thu 4/9/20	$24,800.00	Director Auditoria,Director TIC,Experto ISO27000,Project CEO,Project Owner	
32		Definir horarios	0.5 days	Fri 4/10/20	Fri 4/10/20	$24,800.00	Director Auditoria,Director TIC,Experto ISO27000,Project CEO,Project Owner	31

ID	Task Mode	Task Name	Duration	Start	Finish	Cost	Resource Names	Predecessors
33		Definir requisitos para proveedores e	1 day	Mon 4/13/20	Mon 4/13/20	$41,600.00	Director Ejecutivo,Experto ISO27000,Project CEO,Project Owner	32

4.6. Evaluar recursos necesarios.

Resource Name	Type	Material	Initials	Group	Max.	Std. Rate	Accrue	Base
Experto ISO27000	Work				100%	$2,000.00/hr	Prorated	Standard
Project CEO	Work		P		100%	$1,000.00/hr	Prorated	Standard
Project Owner	Work		P		100%	$1,200.00/hr	Prorated	Standard
Técnico Seguridad 1	Work		T		100%	$500.00/hr	Prorated	Standard
Técnico Seguridad 4	Work		T		100%	$500.00/hr	Prorated	Standard
Técnico Seguridad 3	Work		T		100%	$500.00/hr	Prorated	Standard
Técnico Seguridad 2	Work		T		100%	$500.00/hr	Prorated	Standard
Director Ejecutivo	Work		D		100%	$1,000.00/hr	Prorated	Standard
Director Auditoria	Work		D		100%	$1,000.00/hr	Prorated	Standard
Director TIC	Work		D		100%	$1,000.00/hr	Prorated	Standard
Técnico TIC 1	Work		T		100%	$300.00/hr	Prorated	Standard
Técnico TIC 2	Work		T		100%	$300.00/hr	Prorated	Standard
Técnico TIC 3	Work		T		100%	$300.00/hr	Prorated	Standard

Resumen capítulo 4.

Este capítulo abarca las buenas prácticas plasmadas en la norma ISO 27001 versión 2013, además de las políticas, controles y actividades para su correcta implementación. En este capítulo fueron detallados los distintos departamentos involucrados y los responsables del diseño del Plan de implementación.

De igual forma son detallados los objetivos a conseguir con cada una de las políticas y controles. Cada política le fueron asignadas sus responsables, presupuestos y los tiempos de esperados para su definición.

Como parte integral de un buen SGSI fue presentado el plan de capacitación de colaboradores internos y externos. Siendo detallados los tipos de capacitación, su frecuencia, responsables y la política para los proveedores en este caso instructores.

CONCLUSIÓN

Fueron expuestas las actividades, la documentación y las directrices de seguridad como parte fundamental del diagnóstico y planeación de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para ser aplicado en el Banco Hacienda de forma específica, aunque puede ser aplicado en múltiples Entidades de Intermediación Financiera (EIF).

Para la elaboración de esta investigación, fue de vital importancia estudiar los antecedentes del Banco Hacienda, términos y conceptos relacionados a la Banca. De igual forma detallar las metodologías empleadas en la investigación científica en miras a conseguir la muestra de la población seleccionada.

Se concluyó que parte de la documentación necesaria no estaba presente, en algunos casos ausentes las aprobaciones necesarias, en otras, no se había adoptado una estrategia de capacitación con la facultad de cubrir a todo el personal tanto interno como consultores del Banco Hacienda. Debido a esto se desarrollaron el Plan de capacitación y en la política de proveedores en la que se detalla la necesidad de instructores internos y externos.

RECOMENDACIONES

RECOMENDACIONES

Es de suma importancia la constante revisión de la política de la seguridad de la información en miras a mantener la misma actualizada y acorde a las mejoras tecnológicas con una periodicidad de 1 año y en casos particulares 6 meses.

Es necesaria la evaluación del buen funcionamiento de los controles y la revisión de las pautas especificadas a lo largo de este Trabajo de Grado, tanto en el proceso de diagnóstico, como en el proceso de diseño del SGSI, sustentado en la norma ISO 27001 versión 2013.

Dar continuidad al Plan de capacitación en materia de seguridad de la información en miras a lograr un compromiso con la seguridad del Banco Hacienda, dando lugar a una mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI).

REFERENCIAS BIBLIOGRÁFICAS

Arizzi, R. (s.f.). History of Information Security. Retrieved from https://study.com/academy/lesson/history-of-information-security.html

B. Rajesh, Y. J. (2015). A Survey Paper on Malicious Computer Worms. Brief History of Computer Worm, 161.

Chen, W. W. (2005). Statistical Methods in Computer Security. New York: Marcel Dekker.

Dubois, P. (2003). Slaves and Other Objects. University of Chicago.

Guerra Martinez, C. (2002, 03 11). Retrieved from http://www.economia.unam.mx/secss/docs/tesisfe/GuerraMC/tesis.html

INCIBE. (2015, 03 11). https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio. Retrieved from https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

ISO27000. (s.f.). Sistema de Gestión de la Seguridad de la Informacion. Retrieved from http://www.iso27000.es/download/doc_sgsi_all.pdf

ISOTools. (2019, 01 11). Retrieved from 5 beneficios de implementar un sistema de gestión de seguridad de la información: https://www.isotools.org/2019/01/11/5-beneficios-implementar-sistema-gestion-seguridad-informacion/

Karl De Leeuw, J. B. (2007). The History of Information Security: A Comprehensive Handbook. Amsterdam: ELSEVIER.

Kelty, C. (2011). The Morris Worm. Retrieved from https://escholarship.org/uc/item/8t12q5bj

Murphey, D. (n.d.). A history of information security. Retrieved from https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

NIST. (2019, 07 03). Retrieved from Glossary of Key Information: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Rosteck, T. S. (s.f.). Hackers: Rebeldes con Causa. Retrieved from https://www.internautas.org/documentos/hack_rebe.htm

Sans Penetration Testing. (2003). Retrieved from https://cyber-defense.sans.org/resources/papers/gsec/implementation-methodology-information-security-management-system-to-comply-bs-7799-requi-104600

Superintendencia de Bancos. (s.f.). Retrieved from https://www.sib.gob.do/acerca-de-la-sib

Wawak, S. (2010). THE IMPORTANCE OF INFORMATION SECURITY MANAGEMENT IN CRISIS PREVENTION IN THE COMPANY. Opava: Silesian University.

Amaya Guzman, E. H. (s.f.). Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2955/00002022.pdf?sequence=1

Arango, P. A. (2016). Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/9/pmayaaTFM0616presentaci%c3%b3n.pdf

Banco Hacienda. (2016). Retrieved from http://memorias.minpre.gob.do/api/documents/484/download

Banco Hacienda. (s.f). Retrieved from https://www.sismap.gob.do/Municipal/uploads/evidencias/6641_2_396_manual%20BCO%20AGRICOLA%20PDF.pdf

Banco Hacienda. (s.f.). Retrieved from http://extwprlegs1.fao.org/docs/pdf/dom146536.pdf

Espinosa, M. L. (2016). Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/12406/1/UPS%20-%20ST002224.pdf

ISO. (2013). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO 27001 ¿Cuáles son los requisitos de seguridad? (2017). Retrieved from https://www.pmg-ssi.com/2017/03/iso-27001-requisitos-de-seguridad/

ISO 27001: ¿Qué beneficios nos aporta implantar esta norma? (2016). Retrieved from Pmg-ssi: https://www.pmg-ssi.com/2016/07/iso-27001-beneficios-aporta-implantar-esta-norma/

Luque, J. R. (2019). Retrieved from http://repositorio.usil.edu.pe/bitstream/USIL/8999/1/2019_Kupa-Luque.pdf

MAP. (2019). Retrieved from https://www.sismap.gob.do/Central/uploads/evidencias/636903219999493816-BANCO-AGRICOLA.pdf

Martelo, R. J. (2015). Retrieved from https://scielo.conicyt.cl/scielo.php?pid=S0718-07642015000200015&script=sci_arttext&tlng=en

Mora Palacios, J. C. (2017). Retrieved from http://gis.unicafam.edu.co/index.php/gis/article/view/22/70

NIEVES, A. C. (2017). Retrieved from http://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Pacheco, G. F. (2015). Retrieved from http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tesis-Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequence=1&isAllowed=y

Quisoboni, A. V. (2017). Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2648/00004068.pdf?sequence=1

Reis, J. D. (2018, Julio). Retrieved from http://mendillo.info/seguridad/tesis/Dos%20Reis.pdf

Salcedo, R. J. (2014). Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC1214memoria.pdf

Silva, C. A. (2015). Retrieved from http://repository.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

SISMAP. (s.f.). Retrieved from https://www.sismap.gob.do/Municipal/Directorio/Dir/Details/145

Solarte, F. N. (2015). Retrieved from http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Superintendencia de Bancos. (2018, noviembre). Retrieved from https://www.sib.gob.do/sites/default/files/nuevosdocumentos/20181101_Segunda%20Resolucion_Reglamento_seguridad_cibernetica_de_la_informacion.pdf

Superintendencia de Bancos. (s.f.). Reglamento de Seguridad Cibernetica. Retrieved from https://www.sib.gob.do/sites/default/files/nuevosdocumentos/20181101_Segunda%20Resolucion_Reglamento_seguridad_cibernetica_de_la_informacion.pdf

Banco Hacienda. (2017). *Ilustración del Organigrama institucional.* Retrieved from https://www.bagricola.gob.do/transparencia/index.php/organigrama-p

Banco Hacienda. (s.f.). *Ilustración del Organigrama departamental.* Retrieved from https://www.sismap.gob.do/Central/uploads/evidencias/636586049377400087-OrgsBagricola.pdf

Julio Ernesto Mora Aristega, J. V. (s.f.). *El modelo COBIT 5 para auditoría y el control de los sistemas de información.* Retrieved from http://repositorio.pucesa.edu.ec/bitstream/123456789/2355/1/Modelo%20Cobit.pdf

Molina-Miranda, M. F. (2017). *Analisis de Riesgo de Centro de Datos basado en la herramienta pilar de Magerit.* Retrieved from http://www.revistaespirales.com/index.php/es/article/view/125/68

Moreno, H. P. (s.f.). *Continuidad del negocio.* Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2795/00001618.pdf?sequence=1

Wilson Javier Aguasaco Flórez, J. A. (2016). *Diseño de un modelo de implementación De Itil V3 (Biblioteca de infraestructura de Tecnologías de Información) para el*

mejoramiento en los procesos del departamento de Sistemas en la fundación Santa Fe de Bogotá. Retrieved from https://repositorio.itc.edu.co/handle/001/231

ANEXOS

Formulario Encuestas y entrevistas

Entrevistas sobre casos de riesgos materializados y acciones tomadas:

1. ¿Cuándo fue el último incidente de Seguridad de la Información ocurrido en el banco?
    a. Hace menos de un mes.
    b. Entre un mes y 3 meses.
    c. Entre 4 meses a un año.
    d. Más de un año.
2. ¿Qué tipo de evento se presentó?
    a. Exposición en el Hardware.
    b. Exposición del Software.
    c. Exposición de la red.
    d. Pérdida de información.
3. ¿Pudo la organización resolver la situación según el SLA (tiempo de respuesta) establecido?
    a. Si.
    b. No.
4. ¿Cuándo fue la última vez que ocurrió el evento de seguridad presentado?
    a. Hace menos de un mes.
    b. Entre un mes y 3 meses.
    c. Entre 4 meses a un año.
    d. Más de un año.

5. ¿Ha presenciado usted una auditoría de seguridad en su lugar de trabajo?
    a. Si.
    b. No.
6. ¿En caso de ser si, con qué frecuencia se realiza una auditoría de seguridad en su lugar de trabajo?
    a. Anual.
    b. Cada seis meses.
    c. Cada tres meses.
7. ¿Con qué frecuencia el personal de TI realiza actualizaciones a su ordenador de trabajo?
    a. Nunca.
    b. Cada seis meses.
    c. Cada tres meses.
    d. Cada año
8. ¿Su lugar de trabajo cuenta con un plan de contingencia en caso presentarse un ataque cibernético?
    a. Si
    b. No
9. ¿La empresa cuenta con un canal para reportar brechas de seguridad?
    a. Si
    b. No
10. ¿Qué frecuencia tiene el cambio de contraseña de las computadoras en su trabajo?
    a. Cada 2 meses o menos.
    b. Cada 3 meses.
    c. Mayor a 3 meses.

11. ¿Ha recibido alguna capacitación sobre la gestión de seguridad de la información?

    a. Si.

    b. No.

12. ¿Conoce usted sobre las políticas de seguridad informática en su trabajo?

    a. Sí, las conozco completamente.

    b. No, pero sé que existen.

    c. No existen.

    d. No sé.

13. ¿La empresa te exige encriptar la información sobre los clientes?

    a. Si.

    b. No.

    c. No estoy seguro.

    d. Si, pero nadie lo aplica.

nummularis (Ciudadano romano, especialista en el reconocimiento del valor y originalidad de las monedas que se intercambiaban.)

argentarius (Ciudadano romano, especialista en el intercambio de monedas.)

Anteproyecto de Grado

UNIVERSIDAD APEC

Decanato de Ingeniería e Informática.

Escuela de Informática.

ANTEPROYECTO DE TRABAJO DE GRADO

Para optar por el título de Ingeniero de Software

e Ingeniero de Sistemas de Computación.

TÍTULO DEL TRABAJO DE GRADO:

Evaluación de la implementación de un marco de gestión de la seguridad de la información apoyado en ISO 27000 en el departamento de TI y Seguridad de la Información del Banco Hacienda.

NOMBRES Y MATRÍCULAS DE LOS SUSTENTANTES.

Shade Estrella 20161333

Rosa Fernandez 20121177

Ángel Vladimir Soto Vargas 20160416

Santo Domingo DN.

Octubre 2019.

ÍNDICE DE CONTENIDO 1

1. TEMA

Evaluación de la implementación de un marco de gestión de la seguridad de la información apoyado en ISO 27000 en el departamento de TI y Seguridad de la Información del Banco Hacienda.

2. INTRODUCCIÓN

En la actualidad, la Gestión de la Seguridad de la Información es suma importancia, debido al gran incremento de los atacantes cibernéticos. Estos hackers buscan apropiarse de los recursos tecnológicos y/o las informaciones de las organizaciones. En muchos otros casos, los incidentes son auspiciados por el personal de la empresa, en ocasiones por negligencia humana o premeditadamente.

Los bancos almacenan una gran cantidad de información sensible tanto de sus clientes como propias de la organización, lo cual los convierte en un blanco predilecto para tomar sus recursos a través de ataques cibernéticos.

En el presente documento será expuesto el anteproyecto “Evaluación de la implementación de un marco de gestión de la seguridad de la información apoyado en ISO 27000 en el departamento de TI y Seguridad de la Información del Banco Hacienda”, compuesta por justificación, delimitación del tema y planteamiento del problema para establecer el enfoque del objeto de este anteproyecto. También se compone de los objetivos generales y específicos

de esta investigación, a su vez, un marco teórico referencial en el que se basa este documento. La propuesta incluye el diseño metodológico y las fuentes de documentación para sustentarlo.

3. JUSTIFICACIÓN

La presente documentación busca evaluar las implicaciones de implementar un marco de gestión de la seguridad de la información apoyado en la norma ISO 27001, en miras a gestionar los riesgos cibernéticos relacionados al Banco Hacienda.

La investigación nace de la necesidad creciente de salvaguardar las informaciones de los bancos y sus clientes. Esta propuesta busca para mejorar las vulnerabilidades.

La investigación persigue exponer de una forma clara y objetiva, los beneficios del Anteproyecto de Trabajo de Grado. En ese sentido, la aplicación de esta propuesta busca poder gestionar de forma eficiente los incidentes relacionados a seguridad cibernética mejorando la operatividad y confianza en el Banco Hacienda.

4. DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA.

4.1. Delimitación

4.1.1. Delimitación espacial

Esta propuesta será ofertada al Banco Hacienda ubicado en Av. George Washington 601, Santo Domingo 10103.

4.1.2. Delimitación temporal

Esta propuesta abarcaría desde octubre 2019 hasta abril 2020.

4.2. Planteamiento del problema.

El Banco Hacienda es una Entidad Financiera fundada en 1945, en un principio fue un banco de mucha aceptación, sin embargo, debido a oportunidades de mejora operativa, gestión e innovación tecnológica fue permitiendo la ocurrencia de incidentes de seguridad cibernética, ocurridos en sus sistemas.

Actualmente cuenta con una distribución de personal aceptable para administrar los sistemas y salvaguardar los recursos tecnológicos e informaciones del Banco Haciendo. Sin embargo, no tienen aplicadas normativas de seguridad cibernética propias de ISO 27001. Siendo esto

imprescindible para una mejor aceptación o popularidad entre los clientes.

5. OBJETIVOS

5.1. Objetivo General

Evaluar la implementación de un marco de gestión de la seguridad de la información apoyado en ISO 27000 en el departamento de TI y Seguridad de la Información del Banco Hacienda.

5.2. Objetivos Específicos

- Analizar las medidas de seguridad de la información actuales en el banco.
- Identificar las Entidades de Intermediación Financiera que han aplicado normas de ISO 27001.
- Identificar las normas y mejores prácticas asociadas para el fortalecimiento de los procesos de gestión de la seguridad de la información.

- Diagnosticar las brechas existentes que puedan comprometer una adecuada gestión de la seguridad de la información.
- Evaluar los requerimientos necesarios para la aplicación de normas de seguridad de la información basadas en ISO 27001.

6. MARCO TEÓRICO REFERENCIAL

6.1. Marco teórico

- “El cibercrimen es la amenaza más grande para cualquier compañía en el mundo, y uno de los problemas más grande para el hombre.” (Reporte de Cibercrimen, 2019)

- “432 casos de robo de datos bancarios a través de páginas web o correos electrónicos fraudulentos pusieron en juego más de RD$120 millones de cuentas en República Dominicana.” (Diario Libre, 2014)

- “Concéntrese en hacer la seguridad una parte integral de la cultura de su empresa durante todo el proceso de desarrollo.” (OWASP, 2017)

- “República Dominicana ha recibido en lo que va de año más de 26 millones de ataques cibernéticos.” (Listin Diario, 2017)

- “Toma 20 años construir una reputación y unos pocos minutos de ciber-incidente para arruinarla.” (Stephane Nappo, 2018)

- “Nos hemos dado cuenta de que la idea de que la seguridad comienza y termina con la compra de un firewall pre-empaquetado, es simplemente errónea.” (Art Wittmann, s.f.)

- “Si gasta más en café que en seguridad informática, serás atacado. De hecho, mereces ser hackeado.” (Richard Clarke, 2002)

- “La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización.” (Ladino et. al., 2011)

- “Para ejecutar los objetivos de ciberseguridad de la empresa, los empleados deben tener una actitud positiva, que vaya acorde con las políticas y procedimientos establecidos por los líderes de la empresa. Las empresas regularmente luchan por el cumplimiento de estas, pero no analizan internamente por qué no hay mejores enfoques para lograr la participación de los empleados. Necesitamos estar más alertas y ayudar a educar para que realmente cambiemos la cultura en ciberseguridad.” (Victor Congionti, 2019)

- “Cuando todo está conectado, todo el mundo es vulnerable. La tecnología que aceptamos de manera rutinaria en nuestras vidas puede volverse contra nosotros.” (Marc Goodman, 2015)

Visto esto, podemos deducir que la ciberseguridad no es solo un esfuerzo de un departamento, sino que necesita el respaldo de toda la organización y es imperativo seguir adecuados estándares o marcos de referencias que permitan fortalecer dicha gestión.

6.2. Marco conceptual

- **Banco:** son entidades financieras con permiso del estado para recibir depósitos y prestar dinero. Entre otros servicios, pueden encargarse de manejo de riquezas, cambio de moneda y cajas de seguridad.
- **Seguridad de la Información:** conjunto de medidas preventivas tomadas por las organizaciones para salvaguardar la información independientemente de las formas que tenga.
- **Ciberseguridad:** rama de la seguridad de la información que se encarga de la protección de activos digitales, incluyendo la infraestructura computacional como la información almacenada en los sistemas.
- **Norma:** son reglas que se establecen para regular cómo hacer un trabajo, una tarea o un proceso.
- **Ciclo Deming:** o ciclo PDCA (Plan-Do-Act-Check, por sus siglas en inglés) es una metodología de mejora continua de la

calidad que se aplica a lo largo del ciclo de vida de un servicio o producto.

- **SGSI:** o Sistema de Gestión de la Seguridad de la Información, son un conjunto de políticas que permite la administración de la información.
- **ISO 27001:** es una norma internacional que especifica los requisitos necesarios para establecer, implementar, mantener y mejorar un SGSI basado en el ciclo de Deming. Esta norma pertenece a la norma matriz ISO 27000.
- **Incidente:** son una violación o una amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.
- **Evento:** es cualquier cambio, error, o interrupción observable dentro de una infraestructura de TI, tales como un fallo del sistema, un error de disco o un usuario que olvide su contraseña.
- **Riesgo:** es la posibilidad de que una vulnerabilidad se convierta en una amenaza y ocurra un desastre. No pueden ser eliminados, pero pueden reducirse o manejarse.
- **Información Sensible:** es toda aquella información privada que pertenece a un individuo, tales como empleados, clientes o proveedores.
- **Información Valiosa:** conjunto de información que cuenta con un valor agregado, tales como propiedad intelectual, récords

financieros, récords legales, información comercial o datos operacionales.

- **Amenaza:** es toda aquella acción que se aprovecha de una vulnerabilidad para atentar contra la seguridad de un sistema de información. Pueden ser ataques (como un virus), físicas (un incendio o inundación) o negligencia (no usar cifrado).
- **Vulnerabilidad:** es una debilidad o fallo en un sistema de información que pudiera permitir a un atacante comprometer un sistema de información.
- **Cibercrimen:** es cualquier tipo de actividad criminal que involucra el uso de computadoras y la red.
- **Hacker:** es una persona que se dedica a descubrir y explotar vulnerabilidades en un sistema de información.
- **Error:** acción humana que produce un resultado no esperado o incorrecto.
- **Defecto:** es la presencia de un error en el software.
- **Fallo:** es la manifestación de un defecto.
- **Brecha:** es una violación de la seguridad de sistema de información que resulta en la liberación, destrucción, pérdida o alteración de información.
- **Firewall:** también conocido como cortafuegos, es una herramienta que impide el acceso no autorizado a una red determinada. Pueden existir varios firewalls en la misma red.
- **Modelo OSI:** es un modelo que abstrae el flujo de los datos de una red a otra red en 7 capas.

7. HIPÓTESIS

Hipótesis	Variables	Definición Conceptual	Indicadores
"La aceptación del Banco Hacienda aumenta cuando se anuncia la aplicación de normas de seguridad"	La aceptación del Banco Hacienda	Nivel de preferencia entre los clientes.	*Variaciones en la cantidad de clientes. *Resultados de encuestas. *Nivel de quejas.
	Aplicación de normas de seguridad	Cambios en las medidas de seguridad de la información apoyadas en ISO 27001	*Cantidad de normas cumplidas. *Resultados de pruebas de seguridad.

8. DISEÑO METODOLÓGICO: METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN CUALITATIVA Y/O CUALITATIVA.

8.1. Tipos de estudio.

Serán realizados estudios cualitativos y cuantitativos. En el caso cualitativo se utilizará para aquellos indicadores que requieran preguntas abiertas para medir percepción entre otros aspectos. El enfoque cuantitativo será empleado tanto para preguntas cerradas o de

opción múltiple, estudios estadísticos, fuentes históricas medibles y para verificar nivel de cumplimiento de normativas.

8.1.1. Descriptivo

Este estudio persigue describir cómo se desarrolla el problema. Este tipo de estudio servirá para describir la problemática, en miras a entender mejor las vulnerabilidades.

8.1.2. Explicativo

Este estudio persigue analizar las causas que originan el problema. Esto a partir de las informaciones obtenidas en la investigación.

8.1.3. Por observación

Este estudio persigue la recolección de información mediante el análisis de los casos que se presenten a lo largo de la investigación, utilizando técnicas de observación.

8.2. Métodos de investigación

8.2.1. Método analítico

Será aplicado en esta investigación para el desglose de las causas que atentan contra la adecuada gestión de la seguridad de la información en el Banco Hacienda.

8.2.2. Método Deductivo

Se partirá del argumento proporcionado por la hipótesis descrita en el punto 7, para llegar a las conclusiones de este trabajo de investigación. En primera instancia, se considerarán los principales motivos para aplicar las políticas de seguridad basadas en la norma ISO 27001:2013, así como los factores que impactan la seguridad de la información de la institución.

8.3. Técnicas de recolección de información.

8.3.1. Entrevistas

Se realizarán entrevistas al personal de TI, así como a la alta gerencia, para saber cómo se comporta el banco ante la materialización de riesgos, haciendo hincapié en los procesos y pasos a seguir.

8.3.2. Consulta de expertos

Se consultará con un especialista certificado en ISO 27001:2013, con la finalidad de disponer del juicio de expertos acreditados en la materia para el trabajo de investigación de acuerdo con experiencias reales y conocimientos profesionales.

8.3.3. Encuestas

Se realizarán preguntas para validar los conocimientos y nivel de madurez que poseen colaboradores y clientes del banco Hacienda relacionados con la gestión de seguridad de la información.

9. FUENTES DE DOCUMENTACIÓN (FUENTES BIBLIOGRÁFICAS PRIMORDIALES SOBRE EL TEMA).

A., L., ISABEL, M., S., V., ANDREA, P., E., L., & MARÍA, A. (2011). *FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS.* Pereira, Colombia: Universidad Tecnológica de Pereira.

Centro Nacional de Ciberseguridad. (2019, Febrero). *boletines*. Retrieved from cncs.gob.do: https://cncs.gob.do/boletines/

Congionti, V. (2019, Octubre 18). *Culture Is Where Great Cybersecurity Begins*. Retrieved from RSA Conference: https://www.rsaconference.com/industry-topics/blog/culture-is-where-great-cybersecurity-begins

Creative Commons. (2017). The Ten Most Critical Web Application Security Risks. *OWASP*, 9.

Disterer , G. (2013). ISO/IEC 27000, 27001 and 27002 for Information. *Scientific Research*, 6.

Herjavec Group. (2019). 2019 Official Annual Cybercrime Report. *Cybersecurity Ventures*, 5.

Nappo, S. (2019). *cyber startup observatory ciso week stephane nappo societe generale.* Retrieved from cyber startup observatory:

https://cyberstartupobservatory.com/cyber-startup-observatory-ciso-week-stephane-nappo-societe-generale/

NQA. (2013). *ISO 27001:2013 INFORMATION SECURITY IMPLEMENTATION GUIDE.* United States of America: NQA.

Reyes Rodríguez, P. (2017, Diciembre 7). Registran 24 millones de ataques cibernéticos en RD. *Listin Diario,* p. 1.

shrivastava, G., Kumar, P., Bala, G., & Dey, N. (2018). *Handbook of Research on Network Forensics and Analysis Techniques.* United States of America: IGI Global.

10. ESQUEMA PRELIMINAR DE CONTENIDO DEL TRABAJO DE GRADO.

1. Presentación
2. Dedicatoria
3. Agradecimientos
4. Tabla de Contenidos
5. Introducción
6. CAPÍTULO 1: ANÁLISIS DE LA GESTIÓN DE LASEGURIDAD DE LA INFORMACIÓN Y VULNERABILIDADES BANCARIAS EN LA ACTUALIDAD.
   - 6.1. Seguridad de la información.
     - 6.1.1. Historia.
     - 6.1.2. Conceptos.
     - 6.1.3. Ventajas.
     - 6.1.4. Desventajas.
   - 6.2. Norma matriz ISO 27000.
     - 6.2.1. Origen.
     - 6.2.2. Versiones.
     - 6.2.3. Conceptos.
     - 6.2.4. Normas asociadas.
   - 6.3. Gestión de la Seguridad de la información.
     - 6.3.1. Historia.
     - 6.3.2. Conceptos.
     - 6.3.3. Ventajas.
     - 6.3.4. Metodología de gestión.
   - 6.4. Entidad de intermediación Financiera.
     - 6.4.1. Historia mundial.
     - 6.4.2. Evolución local.
   - 6.5. Súper Intendencia de Bancos.
     - 6.5.1. Origen.
     - 6.5.2. Propósito.