ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016

TESIS PARA OPTAR EL GRADO ACÁDEMICO DE:

MAESTRA EN GESTION PÚBLICA

AUTOR

Br. Pérez Castillo, María Rosario

ASESOR:
Dr. Noel Alcas Zapata

SECCIÓN:
Ciencias Empresariales

LÍNEA DE INVESTIGACIÓN
Dirección

PERÚ 2018

Página del Jurado

……..……

Presidente

……

Secretario

……..

Dr. Noel Alcas Zapata

Vocal

Dedicatoria

A Dios por estar siempre a mi lado. A mis padres por ser mi modelo de vida y a mi hija Tiffany Luz que me cambio la forma de mirar el mundo. A mi esposo Henry e hijos, Azucena del Rosario y Cristopher Henry porque son mi amor. A mis hermanos, Ado, Narciso, William, Adán, Miguel, César, Mirian y Fernán que los llevo en mi corazón.

Agradecimiento

A los docentes de la Escuela de Post Grado Maestría en Gestión Pública de la Universidad César Vallejo. En especial a los Doctores Noel Alcas Zapata, Edwin Martínez López y Genebrardo Mejía Montenegro por su vocación de servicio y enseñanza.

A mi suegro, Carlos Ramírez a María Flores y mis compañeros del Banco de la Nación, porque sin la colaboración de ellos no hubiese sido posible culminar esta investigación.

Declaración Jurada

Yo, Br. Pérez Castillo, María Rosario, estudiante del Programa Académico de Maestría en Gestión Pública de la Escuela de Postgrado de la Universidad César Vallejo, identificado con DNI 27727965, con la tesis titulada "Administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016" declaro bajo juramento que:

1) La tesis es de mi autoría.
2) He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.
3) La tesis no ha sido auto plagiado; es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4) Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad investigada.

De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), auto plagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo.

Los Olivos, noviembre de 2016.

Firma:……

Br. Pérez Castillo, María Rosario

DNI: 27727965

Presentación

Señor presidente

Señores miembros del jurado

Presento la Tesis titulada: Administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016, en cumplimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo para optar el grado académico de Magister en Gestión Pública

Esperando que mis modestos aportes contribuyan con algo en la solución de la problemática de la gestión pública en especial en los aspectos relacionados con la administración de tecnologías de información, los procedimientos de seguridad informática, y particularmente en el Banco de la Nación.

La información se ha estructurado en siete capítulos teniendo en cuenta el esquema de investigación sugerido por la universidad.

En el primer capítulo se expone la introducción. En el segundo capítulo se presenta el marco metodológico. En el tercer capítulo se muestran los resultados. En el cuarto capítulo se abordado la discusión de los resultados. En el quinto se precisan las conclusiones. En el sexto capítulo se adjuntan las recomendaciones que se ha planteado, luego del análisis de los datos de las variables en estudio. Finalmente en el séptimo capítulo presentamos las referencias bibliográficas y apéndices de la presente investigación.

El autor.

Índice de contenido

Apéndice 6: Esquema del artículo científico

Lista de tablas

Página

Lista de figuras

Página

Resumen

En la investigación administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016, el objetivo general de la investigación fue determinar la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016.

El tipo de investigación es básica, el diseño de la investigación es no experimental, transversal, correlacional causal y el enfoque es cuantitativo.

La muestra estuvo conformada por 110 profesionales de seguridad informática del Banco de la Nación. La técnica que se utilizó es la encuesta y los instrumentos de recolección de datos fueron dos cuestionarios aplicados a los trabajadores del Banco de la Nación. Para la validez de los instrumentos se utilizó el juicio de expertos y para la confiabilidad de cada instrumento se utilizó el alfa de Crombach que salió muy alta en ambas variables: 0,965 para la variable administración de tecnologías de información y 0,924 para la variable procedimientos de seguridad informática.

Con referencia al objetivo general: Determinar la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016. Como se demuestra con el área representado por los datos incidencia de la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, el cual se muestra el reporte del mismo con 83.0% de área bajo la curva COR. (p – valor = 0.00 < 0.05).

Palabras Clave: Administración de tecnologías de información y procedimientos de seguridad informática.

Abstract

In the administration of information technology research in computer security procedures of Banco de la Nacion, 2016, the overall objective of the research was to determine the incidence of management of information technologies in computer security procedures of Banco de la Nacion, 2016.

The research is basic, the level of research is descriptive and the research design is not experimental, correlational and causal approach is quantitative.

The sample consisted of 110 workers of the Banco de la Nacion. The technique used is the survey and data collection instruments were two questionnaires applied to workers in the Banco de la Nacion. Expert judgment was used and the reliability of each instrument's alpha Crombach came out very high in both variables was used for the validity of the instruments: 0.965 for variable management information technologies and 0.924 for procedures variable security computing.

Referring to the general objective: To determine the incidence of management of information technologies in computer security procedures of Banco de la Nacion, 2016. As demonstrated with the area represented by the incidence data management information technology impacts security procedures of Banco de la Nacion, which the report thereof is shown with 83.0% area under the ROC curve. (P - value = 0.00 <0.05).

Keywords: Managing information technology and security procedures.

INTRODUCCIÓN

1.1 Antecedentes:

1.1.1 Antecedentes internacionales

Barrionuevo y Ortiz (2015) en su tesis de maestría titulada: Desarrollo de un modelo para logros de cumplimiento de las normativas del sector financiero público en la “Gestión de Servicios de TI”; sustentada en la Escuela Politécnica Nacional de Quito, cuyo objetivo general fue: Desarrollar un modelo para la “Gestión de Servicios de TI”, que brinde apoyo al cumplimiento, en un alto porcentaje, de las normativas del sector financiero público; y, que sea afín a estándares y mejores prácticas de la industria, el mismo que fue validado en un caso de estudio en la Corporación Financiera Nacional. En este estudio se arribó a las conclusiones relevantes: (a) Las instituciones financieras públicas tienen modelos de “Gestión de Servicios de TI” similares; y por consiguiente, es factible concebir un modelo estándar, que pueda ser aplicado en cualquiera de las entidades, el mismo que permita cumplir de una manera más eficiente las normativas establecidas por los organismos de supervisión y control, para las entidades financieras públicas, (b) Existe duplicidad en los requerimientos entre las diferentes normativas; lo cual, es ineficiente ya que implica trabajo adicional, desperdicio de recursos (humanos, financieros y técnicos), duplicidad de esfuerzos durante los procesos de auditorías; y dificultad para implementar un modelo de “Gestión de Servicios de TI” estándar para dar cumplimiento a las exigencias de dichas normativas, (c) Del análisis realizado a los estándares y mejores prácticas de la industria, se determinó que para dar cumplimiento a los requerimientos de las normativas establecidas por los organismos de supervisión y control, se puede adoptar estándares de la industria; tales como: ITIL v3 (2011);Y, COBIT5 ; por tal motivo, resulta práctico determinar un modelo genérico, basado en esos estándares, el mismo que será aplicable a todas las empresas financieras públicas, y (d) Una adecuada taxonomía para los requerimientos de las normativas, así como para los procesos de los estándares y mejores prácticas utilizados, permitirá generar un modelo más preciso y fácil de gestionar; logrando de esta manera incorporar al modelo características para mejora continua

Colorado (2012) presentó la tesis titulada: Propuesta de Optimización y Normalización del Proceso Adquisitivo de Tecnologías de la Información y Telecomunicaciones del Instituto de Seguridad Social del Estado de México y Municipios; para obtener el grado de maestro en ingeniería de calidad otorgado por la Universidad Iberoamericana de México, D.F.; la tesis tuvo como objetivo general: Evaluar el desempeño del proceso adquisitivo de tecnologías de información y comunicaciones, para que permita tomar acciones de mejora del mismo en la Unidad de Tecnologías de la Información del Instituto de Seguridad Social del Estado de México y Municipios permitiendo estabilizar el desempeño del proceso adquisitivo de tecnologías de la información; los objetivos específicos son: (a) Realizar un diagnóstico del proceso de adquisiciones de la Unidad de Tecnologías de la Información del ISSEMMyM, (b) Identificar áreas de oportunidad de mejora en el proceso de adquisiciones, y (c) Establecer una propuesta de mejora del proceso de adquisiciones.

Gallegos y Murillo (2015) en su tesis de maestría titulada: Metodología de gestión de seguridad de la información enfocado a las industrias de telecomunicaciones en el ecuador"; sustentada en la Escuela Politécnica Nacional de Quito, cuyo objetivo fue: Proponer una metodología de Gestión de Seguridad de la Información, enfocada en la Industria de las Telecomunicaciones del Ecuador, basándose en eTom v12, Cobit 5 For Security Information y la ISO 27001. La población y muestra se centró en un conjunto reducido de procesos de eTom; para el efecto, se propuso y aplicó una metodología de selección de procesos, que se basa en dos criterios; el primero, son los Procesos críticos para el negocio y el segundo son Los procesos con mayor nivel de riesgo, tras la aplicación de la metodología de selección de procesos propuesta, se reduce de 86 a 6 procesos de nivel 2 de eTom, sobre los cuales, se enfoca el desarrollo de la metodología de Gestión de Seguridad de la Información. La integración formal entre Cobit 5 For Security Information y la ISO 27002 propuesta por ISACA. En este estudio se arribó a las conclusiones relevantes: (a) El fraude en la industria de las telecomunicaciones y el estudio exploratorio de la gestión de la seguridad de la información en las empresas del Ecuador, se determina que las empresas por fraude a nivel mundial ascienden al 10% de su rentabilidad y en el Ecuador no

es la excepción, debido a que las telecomunicaciones ecuatorianas carecen de una estrategia de gestión de seguridad de la información a nivel de toda la organización y se confunde la gestión de la seguridad de la información con el concepto de seguridad informática, y (b) El resultado del proceso de selección de estándares y buenas prácticas realizado, que determinó la utilización de eTOM v12, COBIT 5 e ISO/IEC 27011 para el desarrollo de la metodología de gestión de seguridad de la información, fue exitoso, ya que existe una integración formal, específicamente entre COBIT 5 y la ISO/IEC 27002, que constituye la parte neurálgica y un sólido soporte conceptual para la metodología, de donde se desprenden las guías de implementación de procesos de la gestión de la seguridad de la información, contextualizadas a los procesos de las telecomunicaciones, para cubrir sus principales necesidades.

Corletti (2011) en su tesis doctoral titulada: Estrategia de seguridad informática por capas, aplicando el concepto de operación militar por acción retardante, sustentada en Universidad nacional de educación a distancia de Madrid, cuyo estudio es básico. Uno de los objetivos planteados fue: Emplear estrategias militares en la seguridad informática. Concluyo lo siguiente: El resultado de este análisis es "La acción retardante". Esta operación realmente se propone objetivos cuya semejanza al problema de seguridad en redes informáticas es llamativo. En virtud de esa similitud es que se comienza a investigar cómo se pueden aplicar los principios de redes de computadoras para organizar una "operación informática de acción retardante". Dando como resultado una operación informático - militar denominada "estrategia de seguridad informática por acción retardante", y que en definitiva propone cambiar la actual defensa estática por una nueva metodología de trabajo dinámica, basada en el concepto de dejar avanzar al enemigo, para poder observarlo, desgastarlo, aprender de él y erradicar el problema de raíz.

1.1.2 Antecedentes nacionales

Valenzuela (2015) en su tesis de maestría titulada: Sistema de gestión del conocimiento para la optimización de la relación entre los servicios y las inversiones del Banco de la Nación, sustentada en Universidad San Martín de Porres, cuyo estudio es básico, con estudio causal. El objetivo general fue desarrollar un modelo de gestión del conocimiento para el Banco de la Nación. La población eligió a siete (7) Expertos en gestión de conocimientos escogidos al azar entre las listas de expertos de prestigio que están disponibles para esta prueba. Concluyo lo siguiente: (a) El modelo de Gestión del Conocimiento, diseñado en primera aproximación y propuesto al BN en este estudio, tiene la validez necesaria para ser eventual componente del diseño de una nueva estrategia Competitiva del BN, en un contexto de creciente competencia motivada en parte por el rápido crecimiento y modernización del Banco de la Nación desde el año 2006, y (b)Las perspectivas objetivas que se derivarían de la eventual implementación de este modelo por el BN, para el próximo quinquenio, bajo distintos escenarios posibles del clima de negocios del país y de la banca, serán significativamente mejores para el BN.

Carbajal (2013) presentó la tesis titulada: Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano; para optar el grado de Master en dirección estratégica en tecnologías de la información otorgado por la Universidad de Piura; la tesis tuvo como objetivo: Proponer una metodología que permita guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos que se realizan en el sector público peruano. Para alcanzar dicho objetivo, se han planteado los siguientes objetivos específicos: (a) Aplicar la normativa emitida por la Contraloría General de la República en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos, (b) Aplicar la normativa emitida por otras entidades del Estado Peruano en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos

Marchand (2013) presentó la tesis titulada: Metodología de implantación del modelo balanced scorecard para la gestión estratégica de tecnologías de información y comunicaciones. Caso: universidad nacional agraria de la selva; para optar el grado de Master en dirección estratégica en tecnologías de la información otorgado por la Universidad de Piura; la tesis tuvo como objetivo: Proponer una metodología de implantación del modelo de balanced scoreCard para la gestión estratégica de tecnologías de información. Caso de estudio en la Universidad Nacional Agraria de la Selva; los objetivos específicos son: (a) Conocer los lineamientos estratégicos de acuerdo a un plan estratégico institucional, su relación con el soporte de tecnologías de información y comunicaciones y la importancia estratégica de estos servicios de soporte, (b) Conocer normas, estándares, buenas prácticas y metodologías relacionadas con la gestión estratégica de tecnologías de información y comunicaciones es una organización, (c) Conocer acerca del modelo de balanced scoreCard, procedimientos, herramientas y su utilidad para la gestión estratégica de tecnologías de información, y (d) Desarrollar las fases de una metodología de implantación del modelo de balanced scoreCard para la gestión estratégica de TI, y su validación aplicando al caso de estudio de la Universidad Nacional Agraria de la Selva.

Horna (2016) en su tesis de maestría titulada: Implementación de la ISO/IEC 12207:2008 para mejorar los procesos asociados al ciclo de vida de software en una micro empresa peruana cuyo objeto social es el desarrollo de sistemas de información, sustentada en la Pontificia Universidad Católica del Perú. El objetivo general fue Implementar un conjunto de propuestas de mejora de procesos en una micro empresa en base a las evaluaciones de los procesos priorizados que corresponden al ciclo de vida de desarrollo de software, tomando como referencia la ISO/IEC 12207:2008, los objetivos específicos fueron: (a) Realizar el diagnóstico de los procesos según el ciclo de vida de desarrollo de software, (b) Elaborar propuestas de mejora de procesos y (c) Implementar el piloto con las propuestas de mejora y realizar las evaluaciones correspondientes. Se determinaron aquellos procesos relevantes para conseguir el cumplimiento de los objetivos de negocio. Concluyo lo siguiente: (1) Elaborar propuestas de mejora

de procesos según las mejoras prácticas, (2) Implementar el piloto con las propuestas de mejora y realizar las evaluaciones correspondientes.

Bullón (2010) en su tesis de doctorado titulada: Ventaja competitiva de las capacidades operacionales y dinámicas de la tecnología de la información: caso de Lima, Perú, sustentada en la Pontificia Universidad Católica del Perú, El método de investigación fue descriptivo y explicativo; y la lógica, deductiva. El diseño de investigación fue un estudio de sección transversal enmarcado en un diseño no experimental con una fuente de datos primaria y secundaria, siendo una investigación básica con datos de los sectores industriales, financiero y de servicio de Lima, Perú. El objetivo de la investigación fue evaluar el efecto de las capacidades operacionales y dinámicas sobre la ventaja competitiva. La población se tomó como referencia el PERU Top 10000 Companies (Cavanagh, 2007) que está basado en el resultado del 2006 y a los alumnos del postgrado de la PUCP-CENTRUM, que conformaron el marco de muestreo. Estas 10,000 mejores compañías del Perú contabilizan aproximadamente el 98% de las ventas formales. El tamaño de la muestra fue de 233 casos, que es un tamaño medio de acuerdo a Kline (2005). Concluyó lo siguiente: (a) El estudio de investigación fue dirigido a evaluar empíricamente el impacto de la TI en la ventaja competitiva, y (b) El análisis por sesgo común no arrojó evidencias suficientes de que existiera un sesgo común entre estos dos tipos de variables independientes y dependientes.

1.2 Fundamentación teórica

1.2.1 Bases teóricas de la variable administración de tecnologías de información

Según la Cumbre Mundial de la Sociedad de la Información (2005) refiriéndose a la administración de tecnologías de información indicaron:

> En la última década, "sociedad de la información" es sin duda la expresión que se ha consagrado como el término hegemónico, no porque exprese necesariamente una claridad teórica, sino gracias al bautizo que recibió, en las políticas oficiales de los países más desarrollados y la coronación que significó tener una Cumbre Mundial dedicada en su honor. Los antecedentes del término, sin embargo, datan de décadas anteriores. En 1973, el sociólogo estadounidense Daniel Bell introdujo la noción de la «sociedad de información» en su libro El advenimiento de la sociedad post-industrial, donde formula que el eje principal de ésta será el conocimiento teórico y advierte que los servicios basados en el conocimiento habrían de convertirse en la estructura central de la nueva economía y de una sociedad apuntalada en la información, donde las ideologías resultarían sobrando. Esta expresión reaparece con fuerza en los años 90, en el contexto del desarrollo de Internet y de las TIC. A partir de 1995, se lo incluyó en la agenda de las reuniones del G7 (luego G8, donde se juntan los jefes de Estado o gobierno de las naciones más poderosas del planeta). Se ha abordado en foros de la Comunidad Europea y de la OCDE (los treinta países más desarrollados del mundo); también lo adoptaron el gobierno de Estados Unidos, así como varias agencias de Naciones Unidas y el Grupo Banco Mundial. Todo ello con gran eco mediático. A partir de 1998, fue escogido, primero en la Unión Internacional de Telecomunicaciones y luego en la ONU, para el nombre de la Cumbre Mundial a realizarse en 2003 y 2005. En este contexto, el concepto de "sociedad de la información", como construcción política e ideológica, se ha desarrollado de la mano de la globalización neoliberal, cuya principal meta

> ha sido acelerar la instauración de un mercado mundial abierto y "autorregulado". La Organización Mundial del Comercio (OMC), el Fondo Monetario Internacional (FMI) y el Banco Mundial, para que los países débiles abandonen las regulaciones nacionales o medidas proteccionistas que "desalentarían" la inversión; todo ello con el conocido resultado de la escandalosa profundización de las brechas entre ricos y pobres en el mundo. (p.2)

La sociedad de la información desde su concepción hasta la fecha sigue manteniendo su importancia y eso es debido a que se instituyo en los jefes de Estado o gobierno de las naciones más poderosas del planeta. Se abordado en foros de la Comunidad Europea y de los países más desarrollados del mundo, también porque lo adoptaron el grupo de los 7 o G7 que es un grupo informal de países del mundo cuyo peso político, económico y militar es temido a nivel mundial, formado por Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y Reino Unido, los países del G-7 representan más del 64% de la riqueza del mundo. Las tecnologías de la información han sido un factor importante en la aceleración de la globalización económica y también en los aspectos de sociales, las tecnologías de información se unieron a las comunicaciones, ya que sin ella la tecnología no tiene movimiento. La rápida innovación tecnológica crea un mundo más inteligente y móvil en dónde las tendencias globales es de que los consumidores cada vez quieren dispositivos y aplicaciones más poderosas, mientras que las empresas buscan una tecnología más efectiva en costos para hacer frente a los desafíos cada vez más complejos, las empresas deberán competir en los análisis de la gran cantidad de información para diferenciarse, la movilidad inteligente va a cambiar la forma en que la gente interactúa, la tecnología ya rompió las fronteras, se guarda información en la nube, lo virtual hace que veamos otra forma de mirar, ya fue el dinero físico y plástico, incrementar el ancho de banda, big data para estar preparados ante los ataques cibernéticos, tanta información que implica que se debe dedicar más tiempo para analizar la información con el objetivo que esta sea oportuna y relevante, el teletrabajo como una nueva forma de trabajar y en ambientes colaborativos y confortables.

Definiciones de la variable administración de tecnologías de información:

Según Bon et al (2008) refiriéndose a la administración de tecnologías de información indicaron:

> La administración de servicios de tecnologías de información ha pasado a ser el enfoque centrado en servicios y procesos de lo que anteriormente se llamó gestión de las tecnologías de la información. El desplazamiento de la gestión desde la infraestructura hasta los procesos ha llevado a la aparición de la gestión de servicios de tecnologías de información como una disciplina centrada en servicios y procesos. Los procesos siempre deben tener un objetivo definido. El objetivo de los procesos de gestión de servicios de tecnologías de información es contribuir a la calidad de los servicios de tecnologías de información. La gestión de la calidad y el control de procesos forman parte de la organización y sus políticas. (p. 86)

Esta variable permite que las organizaciones públicas y privadas brinden servicios de calidad razonables a los usuarios y clientes, estos a su vez están soportados por tecnologías de información que para asegurar un servicio de calidad están sustentados por procesos definiendo un dueño de proceso, responsable de evaluar los riesgos del mismo aterrizados en procedimientos de seguridad informática que describen las actividades propias de las funciones que desempaña cada área, evitando que se traslapen las funciones, esos procedimientos deben ser flexibles ya que al realizar la retroalimentación debe permitir de manera natural en la mejora continua. Tiene la característica de apalancar los objetivos definidos en el plan operativo de informática y de seguridad. Junto con la dimensión activos de servicio forman la base para crear valor en forma de bienes y servicios. En el caso de una organización pública o privada, la administración de tecnologías de información debe estar razonablemente definida en la organización, es decir quiénes van hacer los responsables y que funciones van a realizar.

Según la Norma internacional ISO/IEC 27001 (2013) refiriéndose a la administración de tecnologías de información indicó: “Debe implementarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso” (p. 19)

En la gestión de accesos e identidades de los sistemas informáticos, sistemas de información y plataformas de información se formaliza el registro y baja de los usuarios, es la norma donde la alta dirección le asigna responsabilidad a la Gerencia de Recursos Humanos que debe remitir de forma inmediata al área encargada de realizar el registro o baja las renuncias y ceses que se hayan producido en la organización con el objetivo de que el usuario no tenga acceso a los sistemas y plataformas minimizando el riesgo de fraude. Asimismo, la gerencia de recursos humanos, debe comunicar a la instancia correspondiente la relación de trabajadores que estarán de vacaciones programadas, así como la lista del personal con licencia por descanso prenatal, posnatal u otras circunstancias contempladas en la ley que ameriten su ausencia temporal, para la suspensión de los accesos a los sistemas informáticos, sistemas de información y plataformas tecnológicas hasta el retorno a sus labores

Gómez (2007) refiriéndose a la administración de tecnologías de información indicaron:

> En este aspecto, el compromiso de la alta dirección resulta de especial importancia, ya que su implicación es necesaria para que se pueda destinar los recursos suficientes para una adecuada gestión de la seguridad de la información. Por este motivo, sería conveniente elaborar informes detallados sobre los costes y las consecuencias de la falta de seguridad para la organización, para conseguir de este modo su sensibilización sobre esta delicada cuestión. No debemos olvidar un problema adicional con los directivos de la organización, ya que suelen tener acceso a información sensible y, en algunos casos sus conocimientos

> y habilidades informáticos son bastante reducidos, por lo que pueden ser víctimas fáciles de estafas y ataques basados en determinado tipo de engaños. (p. 82)

Hoy en día es de vital importancia concientizar a los directivos de la organización, ya que los conocimientos informáticos que tienen son lo básico y por lo tanto son víctimas de fraudes ya que son a través de ellos que se puede vulnerar la seguridad y como tienen accesos restringidos puede materializarse los riesgos y llegar a cometerse fraudes. Se debe concientizar de manera periódica en temas de seguridad de la información, en la gestión de accesos e identidades, clasificación de la información así de esta manera ellos tomaran conocimiento que son responsables de dar los acceso necesarios de su personal que tienen a cargo y que es su función velar por la actualización de suspender los accesos cuando los trabajadores o proveedores culminen sus funciones para darles de baja no solo físicamente si no también darle de baja en los sistemas informáticos, sistemas de información y plataformas tecnológicas.

Costas (2011) refiriéndose a la administración de tecnologías de información dijo que “Los elementos principales a proteger, en cualquier sistema informático son software, hardware y los datos. Habitualmente los datos constituyen el primer elemento a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar” (p. 26).

Los activos informáticos deben estar identificados en todos los procesos de información y esto se realiza a través de la clasificación de la información en la que se identifica los activos teniendo en cuenta los criterios de criticidad e importancia, y una vez identificados se realiza un tratamiento de la información a través del uso de sellos de agua identificándolo como confidencial, dándole la importancia en su almacenamiento, proceso y transporte. Las bases de datos de la organización deben ser protegidas, es decir encriptar la base de datos debido a que ella contiene la información sensible de los clientes, de esta manera se está asegurando que las personas que no tienen autorización a la base de datos no podrán tener acceso a las mismas.

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009) en la Circular N° G-140 sobre la administración de tecnologías de información, preciso: “La seguridad lógica debe contar con procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios” (p. 3).

En un sistema de gestión de seguridad información se establecen lineamientos de seguridad de la información para la administración de accesos a los sistemas de información, servicios informáticos y plataformas tecnológicas, utilizando un método de control de accesos basada en roles. Con la finalidad de atender de manera oportuna, eficiente y segura las solicitudes de accesos a los sistemas de información, servicios informáticos y plataformas tecnológicas de la organización. También es importante que considere los lineamientos para la creación de cuentas de usuario y contraseñas, así como las responsabilidades y uso. Las disposiciones establecidas son de aplicación a todo el personal y proveedores que utilizan los sistemas, servicios y dispositivos informáticos de la organización, titulares de la información, propietarios de la aplicación y administradores de los sistemas de información, servicios informáticos y plataformas tecnológicas de la organización.

Gómez (2013) refiriéndose a la administración de tecnologías de información indicaron:

> Los responsables de la organización deberían definir las condiciones de uso aceptable para cada uno de estos servicios del sistema informático, así como qué áreas o departamentos se van a encargar de ofrecer los distintos servicios y qué personas serán las responsables de administrar y supervisar cada uno de estos servicios. (p. 87)

Los responsables de la organización, mediante normas y directivas son los que definen las responsabilidades en el proceso de la administración de las tecnologías de información para que estas se han seguras. El propietario de la aplicación define y mantiene actualizado los perfiles de acceso de la aplicación que administra mediante los cuales autoriza el acceso a los usuarios de las diferentes áreas que lo requieran. Los jefes de las áreas son responsables de crear, mantener y asignar roles funcionales a los usuarios de su dependencia de acuerdo a las funciones que realizan en la organización, asimismo deben validar los accesos de los usuarios bajo su dependencia en el Sistema de Administración de Accesos e Identidades, a fin de asegurar que cada usuario tenga las cuentas con su rol funcional debidamente autorizado. Así como los jefes de área tienen responsabilidades, es importante que el usuario también los tenga y la responsabilidad de los usuarios es utilizar su cuenta de usuario y contraseña para acceder a los sistemas de información, servicios informáticos y plataformas tecnológicas de la organización, no compartir su cuenta de usuario y contraseña bajo responsabilidad, usar la cuenta asignada sólo para fines laborales y darle el uso adecuado a los servicios al que se tiene acceso debido q que a veces se descarga o ingresa a páginas indebidas infectando a través de su computador a toda la red de la organización elevando el riesgo a un nivel crítico.

Beynon (2014) refiriéndose a la administración de tecnologías de información indicó “Está relacionada con el mantenimiento de la infraestructura de las TI de la organización, desarrollo de nuevas aplicaciones y mantenimiento de las ya existentes. Este es el objetivo de los técnicos especialistas de la organización” (p. 451)

En organizaciones en que la única constante es el cambio, la creación, actualización o eliminación de un rol funcional puede darse por diversos motivos, entre ellos los más importantes tenemos lanzamiento de un servicio o producto con el objetivo de satisfacer las necesidades del mercado para satisfacer necesidades cada vez más personalizado. Otro es la modificación de los manuales de organización y funciones en que las organizaciones modifican sus organizaciones para fusionar áreas para hacer más ágil el proceso de atención y minimizar los tiempos de atención siempre con el objetivo de fortalecer la misión

que es de dar atención de calidad al cliente. También hay cambio debido a las recomendaciones de las auditorias, con el objetivo de mejorar el proceso de mejora continua. En la creación, actualización o eliminación de un rol funcional es importante la participación directa del propietario de la aplicación que es el responsable de definir los perfiles de acceso de sus aplicaciones, basado en roles funcionales, a través de los cuales se realiza la gestión de accesos. Asimismo, es vital que los administradores de los servicios informáticos y plataformas tecnológicas de la organización en coordinación con las áreas usuarias, son responsables de definir los perfiles de acceso correspondientes que permitan gestionar los accesos basado en roles funcionales. Todo rol funcional está conformado por un conjunto de perfiles de acceso debidamente autorizados por el propietario de la aplicación.

Macau (2004) Tecnologías de información y comunicaciones: ¿Para qué? Funciones de las tecnologías de la información y la comunicación en las organizaciones, indicó:

La utilización de tecnologías de información y comunicaciones para conseguir ventajas competitivas pone al orden del día: servicios de cajeros automáticos en línea 24 horas al día en las entidades financieras más punteras, intercambio electrónico de documentos entre los proveedores y los fabricantes más innovadores. (p. 8)

Actualmente se ha desencadenado ataques a los cajeros automáticos por parte de los ciber delincuentes como el la carga de un malware a través de un disco booteableen en el cajero automático y este habilita a un atacante realizar retiros de dinero del cajero de manera autorizada. Otra forma de modalidad de ataque es el phishing para engañar a los usuarios de una organización y a través de ellos ingresar un software malicioso en los quipos, con el objetivo de escalar privilegios en la red hasta llegar a la red de cajeros para realizar actividades maliciosas para retirar dinero. También hay una modalidad de ataque es el snifferen que son equipos que permiten escuchar todo el tráfico que sale e ingresa al cajero y si este canal no está cifrado, el atacante podría escuchar el tráfico o

alterarlo afectando la información de los clientes.

Dimensiones de la variable administración de tecnologías de información:

Dimensión gestión de servicios de tecnologías de información y procesos:

Bon *et al* (2008) refiriéndose a la gestión de servicios de tecnologías de información y procesos indicaron que:

> Un enfoque orientado a procesos permite utilizar mejores prácticas de gestión de servicios de tecnologías para describir la provisión de servicios usando la serie más eficaz y eficiente de actividades. El ciclo de vida del servicio en la versión tres de ITIL está basado en estas descripciones de procesos. La estructura y asignación de tareas y responsabilidades entre funciones y departamentos depende del tipo de organización. Estas estructuras pueden variar mucho de un departamento de tecnología de información a otro y cambian con frecuencia. Sin embargo, la descripción de la estructura de procesos ofrece un punto común de referencia que cambia con menos rapidez. (p.86)

Esta dimensión permite que las organizaciones públicas y privadas brinden servicios de calidad a los usuarios y clientes, estos están soportados por tecnologías de información que para asegurar un servicio de calidad están sustentados por procesos definiendo un dueño de proceso, responsable de evaluar los riesgos del mismo aterrizados en procedimientos que describen las actividades propias de las funciones que desempaña cada área, evitando que se traslapen las funciones, esos procedimientos deben ser flexibles ya que al realizar la retroalimentación debe permitir de manera natural la mejora continua. Tiene la característica de apalancar los objetivos definidos en el plan operativo informática. Junto con la dimensión activos de servicio forman la base para crear valor en forma de bienes y servicios. En el caso de una organización pública o privada, la gestión de servicios de tecnologías de información debe realizarse mediante un centro de llamadas registrando un ticket de atención, donde se pueda centralizar los requerimientos de los usuarios y se puedan medir mediante indicadores que indiquen la cantidad de tickets atendidos con sus respectivos informes de

resolución los cuales servirán para consolidar una base de datos de conocimientos que servirán para una próxima atención más rápida. Es razonable para esta dimensión documentar de manera obligatoria los procedimientos de los procesos críticos del negocio para cumplir con las obligaciones normativas, de control y de las de regulación tanto internas como externas.

Bauset y Rodenes (2013) refiriéndose a la gestión de servicios de tecnologías de información y procesos dijeron:

> Que los servicios de tecnologías de la información son cada vez más complejos, se incrementan sus niveles regulatorios, se producen frecuentes desviaciones en tiempo o en costes en su ciclo de vida, continuos avances tecnológicos, etc., todo lo cual hace su gestión más necesaria para que sigan siendo eficientes, pero a la vez más compleja. Si la gestión eficaz se consigue que los cambios se adapten proactivamente a la estrategia del negocio. (p. 55)

Actualmente desde el punto de vista de tecnologías de información la única constante es el cambio, esto quiere decir que las organizaciones para mantenerse en el mercado deben desarrollar estrategia para aceptar el cambio, tanto los cambios regulatorios como los de las necesidades de los clientes que cada día son más específicos y generalizados entonces los procesos son más complejos y es ahí donde las herramientas de tecnologías de información deben apoyar a la gestión de servicios para seguir siendo eficientes y satisfacer las necesidades del cliente y se debe tratar de superar las expectativas del cliente para considerarlo en la cartera de proyectos.

Según la Contraloría General (2006) en la Resolución N° 320 en que aprueban las Normas de Control Interno, refiriéndose a la gestión de servicios de tecnologías de información y procesos precisó que:

> Las Normas de Control Interno, constituyen lineamientos, criterios, métodos y disposiciones para la aplicación y regulación del control interno en las principales áreas de la actividad administrativa u operativa de las

> entidades, incluidas las relativas a la gestión financiera, logística, de personal, de obras, de sistemas de información y de valores éticos, entre otras. Con el propósito de promover una administración adecuada de los recursos públicos en las entidades del Estado. (p. 4)

En las organizaciones grandes y complejas se considera una estructura organizacional con gerencia de finanzas y contabilidad para planificar el presupuesto y a su vez contabilizar los gastos de la empresa. La gerencia de logística con el objetivo de elaborar el plan anual de adquisiciones y contrataciones y hacer seguimiento al proceso de adquisiciones y contrataciones y finalmente seguimiento del cumplimiento de los contratos para facturar en los tiempos establecidos a los proveedores que dan un servicio o bien. La gerencia de recursos humanos es aquella que poya en facilitar personal mediante el proceso de reflotación de recursos en sus diversos modalidades. Gerencia de informática tiene como misión mantener las tecnologías de información , sistemas de información y plataformas tecnológicas disponibles 24 por siete por 365 días de acuerdo a los productos y servicios que ofrezca la organización las tecnologías de información es el soporte del negocio y es transversal a todos los procesos.

Piattini y Hervada (2007) citado por Bauset y Rodenes (2013), sobre la gestión de servicios de tecnologías de información y procesos destacaron:

> Que la experiencia ha demostrado que la calidad en el nivel de servicio no es algo que se pueda obtener únicamente con fuertes inversiones en tecnología o personal altamente cualificado, sino que es el resultado de una buena gestión y planificación a nivel empresarial. Es necesario implantar un sistema de gestión de servicios de TI (SGSIT), potenciar la labor de los gestores y utilizar métricas para el seguimiento y control del progreso. (p. 55)

En cualquier rublo de negocio la gestión y planificación es vital para las empresas porque una vez planificado se puede gestionar para ejecutar los proyectos definidos. En las organizaciones grandes y complejas se debe

considerar dentro de la gerencia de informática un área que se encargue de la gestión del servicio de tecnologías de información y estos deben contar con los recursos adecuados para responder a los incidentes o requerimientos del negocio en niveles aceptables esto se puede medir a través de indicadores de un sistema de gestión de calidad con el objetivo de estar alineados a la misión del negocio y permanecer en una mejora continua.

Gómez (2013) refiriéndose a la gestión de tecnologías de información y procesos indicaron:

> Los responsables de la organización deberían definir las condiciones de uso aceptable para cada uno de estos servicios del sistema informático, así como qué áreas o departamentos se van a encargar de ofrecer los distintos servicios y qué personas serán las responsables de administrar y supervisar cada uno de estos servicios. (p. 87)

Las empresas grandes y complejas, dentro de su estructura organizacional definen una gerencia de informática a su vez esta está compuesta por áreas que van a ser responsables de administrar, monitorear y supervisar los la gestión de servicios de tecnologías de información, esta área atiende los incidentes y requerimientos de primer y segundo nivel el tercer nivel debe ser resuelto por el área de infraestructura y comunicaciones y comunicaciones o el área de desarrollo de sistemas de información y el cuarto nivel es cuando el soporte se ha escalado a los proveedores. El monitoreo lo realiza el área de operaciones y control de plataformas, el área de gestión de servicios de tecnologías de información definen los indicadores de gestión y reportan periódicamente a la gerencia de informática el resultado de los indicadores, estos a su vez se comunican a la gerencia de planeamiento y desarrollo que es la encargada del sistema de la gestión de calidad para ser incluidas en ella.

Dimensión funcionalidad y garantía:

Bon *et al* (2008) refiriéndose a la funcionalidad y garantía indicaron que:

> El valor no solo se aprecia en los resultados del negocio del cliente, sino que también depende en gran medida de la percepción del cliente. Esto es consecuencia de la diferencia entre valor económico y percepción económica. La percepción depende de la imagen, los atributos de valor y la experiencia personal del cliente. Es importante recordar que la definición y diferenciación del valor son aspectos subjetivos para el cliente. El valor económico no siempre se corresponde con las percepciones del cliente. La funcionalidad de un servicio se comunica por medio de ciertos resultados o con la eliminación de ciertos riesgos y costes. Los clientes están ansiosos por externalizar la gestión de activos que eliminan recursos financieros en sus activos básicos. También desean evitar la falta de capacidad. (p. 25)

Esta dimensión permite que las organizaciones públicas y privadas cuenten con los recursos y las capacidades para soportar la atención al cliente producto de la cartera de servicios que brindan las organizaciones, esta dimensión está soportada por personas, procesos, sistemas y tecnologías de información. Las capacidades viene hacer lo que las personas pueden hacer con los recursos destinados mediante los conocimientos adquiridos a través de la experiencia, capacitación y entrenamiento. Tiene la característica de motivar al personal para fortalecer sus funciones mediante el desarrollo de competencias. Tiene la característica de apalancar los objetivos definidos en el plan anual de capacitación. Junto con la dimensión comunicación en organizaciones de servicios de tecnologías de información forman la base para el valor de un servicio, este valor está orientado a conseguir un determinado objetivo. En el caso de una organización pública o privada, los recursos y capacidades deben estar definidas en las funciones del área de recursos humanos, en la que se tiene como una de las funciones la planificación y ejecución del plan de capacitación de

los recursos considerando a todas las áreas de la organización mediante criterio de competencias además de otras.

Gómez (2007), refiriéndose a la funcionalidad y garantía dijo que:

> La organización debería incluir en sus Políticas de Seguridad las directrices relativas al proceso de solicitud, creación, configuración, seguimiento y cancelación de cuentas de usuarios. Asimismo, se debería definir una norma homogénea de identificación de usuarios para toda la organización. En relación con estas cuentas de usuario con privilegios administrativos, se tendrá que especificar hasta qué punto y en qué determinadas condiciones este usuario o usuarios podrán hacer uso de los privilegios administrativos para acceder a carpetas o ficheros de otros usuarios, monitorizar el uso de la red y de los equipos, instalar o desinstalar aplicaciones, cambiar la configuración de los equipos, etcétera, contando para ello con la autorización de la organización. (p. 60)

Las cuentas de usuario de acceso e identidades en el proceso de solicitud, creación, configuración, seguimiento y cancelación deben estar definidas en una norma de gestión de accesos e identidades basadas en una metodología de roles estos a su vez compuesta por perfiles donde el jefe del área es responsable de dar accesos a su personal que se encuentra bajo su despacho. En lo que se refiere a las cuentas de usuario con privilegios administrativos se debe normar a través de la gestión de cuentas principales y privilegiadas en ella se define las responsabilidades, las actividades a realizar y quienes están autorizados a desarrollar estas funciones. En ambos casos de accesos de cuentas de usuarios y cuentas con privilegio, la organización tiene que planificar auditorías internas para velar por el cumplimiento de las políticas de seguridad de la información.

Gómez (2013) refiriéndose a la funcionalidad y garantía dijo que:

> Un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. Para ello, el equipo

> responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de la Alta Dirección. (p. 71)

En un nuevo servicio o producto o en una modificación que se haga a los mismos siempre deben estar presentes las áreas de planeamiento y desarrollo, riesgos e informática y el más importante el propietario. El propietario como conocedor del proceso del sistema informático con el apoyo del área de riesgos deben de evaluar los riesgos del sistema para determinar el nivel de riesgos para asegurar la funcionalidad y garantía del sistema, calificándola por niveles bajo, medio y alto y el resultado es alto se deben tomar las medidas correctivas inmediatas para mitigar el riesgo. Si es medio se deben planificar acciones a largo plazo y cuando el riesgo es bajo es decisión del propietario si se acepta o lo trata.

Beynon (2014) refiriéndose a la funcionalidad y garantía dijo:

> La funcionalidad de un sistema de información se determina normalmente examinando los requisitos de la organización con detalle. La funcionalidad de un sistema de información es lo que un sistema hace o debería ser capaz de hacer. Determinar el núcleo de la funcionalidad de un sistema de información es un aspecto crítico en el proceso de desarrollo de los sistemas. (p. 8)

La funcionalidad de un sistema de información se determina examinando los requisitos de la organización con detalle y para que esto sea posible el área de planeamiento y desarrollo especializada y conocedor de los procesos de la organización apoya en examinar que debería hacer cada área para garantizar la funcionalidad del sistema de información. Es importante la participación del propietario en todo el proceso porque él sabe quiénes van a utilizar el sistema de información en toda la empresa

Dimensión recursos y capacidades:

Bon *et al* (2008) refiriéndose a los recursos y capacidades indicaron que:

> Los recursos y las capacidades son tipos de activos que las organizaciones utilizan para crear valor en forma de bienes y servicios. Los recursos forman la entrada directa para la puesta en producción y se convierten en valor a través de la gestión, la organización, el personal y el conocimiento. Las capacidades representan la habilidad de una organización para coordinar, gestionar y aplicar recursos con el fin de producir valor. Los recursos suelen estar basados en experiencias; requieren mucho conocimiento e información y están íntimamente relacionados con las personas, sistemas, procesos y tecnologías de una organización. (p. 28)

Esta dimensión permite que las organizaciones públicas y privadas cuenten con los recursos y las capacidades para soportar la atención al cliente producto de la cartera de servicios que brindan las organizaciones, esta dimensión está soportada por personas, procesos, sistemas y tecnologías de información. Las capacidades viene hacer lo que las personas pueden hacer con los recursos destinados mediante los conocimientos adquiridos a través de la experiencia, capacitación y entrenamiento. Tiene la característica de motivar al personal para fortalecer sus funciones mediante el desarrollo de competencias. Tiene la característica de apalancar los objetivos definidos en el plan anual de capacitación. Junto con la dimensión comunicación en organizaciones de servicios de tecnologías de información forman la base para el valor de un servicio, este valor está orientado a conseguir un determinado objetivo. En el caso de una organización pública o privada, los recursos y capacidades deben estar definidas en las funciones del área de recursos humanos, en la que se tiene como una de las funciones la planificación y ejecución del plan de capacitación de los recursos considerando a todas las áreas de la organización mediante criterio de competencias además de otras.

Gómez (2007) refiriéndose a los recursos y capacidades dijo:

> La importancia del factor humano en la seguridad de la gestión de servicio de tecnologías de información es fundamental, por lo tanto, contemplar el papel de las personas y su relación con los sistemas y redes informáticas de la organización. Además, la disponibilidad en Internet de todo tipo de herramientas y programas, así como de la documentación necesaria para su instalación y configuración ha venido a complicar la situación para los responsables de informática de las organizaciones, ya que ahora la "tentación" se encuentra a un simple clic de distancia. (p. 72)

Siempre se habla que el activo más importante de una organización es el recurso humano y de igual manera el factor humano juega un rol muy importante en el sistema de gestión de seguridad de la información porque ellos son los encargados de mantener operativo los sistemas de información, darle soporte técnico y en cada producto y servicio asegurar la calidad y por último mantener la seguridad informática para que esto sea posible el recurso humano debe estar en constante capacitación por lo que se debe elaborar un plan anual de capacitaciones donde se incluyan cursos que incrementen la capacidad de los recursos y este proceso se inicia con la evaluación del recurso para ver su conocimiento actual y hasta donde queremos que tenga capacidad y con los resultados se toma una brecha de capacidades, es importante hacer esto debido a que la única constante es el cambio.

Según la Contraloría General (2006) en la Resolución N° 320 en que aprueban las Normas de Control Interno, refiriéndose a los recursos y capacidades precisó que:

> Es necesario que el titular o funcionario designado establezca políticas y procedimientos necesarios para asegurar una apropiada planificación y administración de los recursos humanos de la entidad, de manera que se

> garantice el desarrollo profesional y asegure la transparencia, eficacia y vocación de servicio a la comunidad. (p. 13)

La gerencia de recursos humanos deben contar con áreas de capacitación, asistencia social, registro de personal, selección de personal, cultura organizacional, cada una de estas áreas garantizan una adecuada administración, de los recursos humanos. El área de capacitación es el encargado de hacer el plan anual de capacitaciones y debe estar acompañado en situaciones difíciles el trabajo para que este pueda desarrollar sus funciones sin afectar su rendimiento, en el proceso de selección se reclutan los recursos humanos para cubrir las necesidades de las áreas con el perfil solicitado para que se garantice el desarrollo profesional.

Bauset y Rodenes (2013) refiriéndose a los recursos y capacidades dijeron “la Orientación futura son Indicadores relacionados con la innovación, haciendo uso de recursos humanos y tecnológicos que permitan entregar los servicios a tiempo” (p. 55).

Los recursos humanos de la mano con la tecnologías de información permite entregar servicios o productos dentro de los tiempos establecidos y para medir el cumplimiento de los mismo es importante hacerlo mediante indicadores de gestión, una vez que se cumplan los indicador después de un año se debe reformular el indicador para mejorar los servicios y productos. En paralelo se debe mejorar las capacidades de los recursos humanos e incentivar la innovación a través de premios e incentivos que gratifique al recurso humano.

Dimensión activos del servicio:

Bon *et al* (2008) refiriéndose a los activos del servicio indicaron que:

> La gestión es un sistema que incluye liderazgo, administración, política, rendimiento normativas e incentivos; los activos organizativos son configuraciones activas de personas, procesos, aplicaciones e

> infraestructuras que implementan todas las actividades organizativas; los activos de procesos incluyen algoritmos, métodos, procedimientos y rutinas que facilitan las actividades e interacciones de implementación y gestión; los activos de conocimiento son logros, experiencias, información y propiedad intelectual; las personas representan la capacidad de creatividad, análisis, percepción, educación, liderazgo, comunicación, empatía y confianza, los activos de información son colecciones significativas de datos que se aplican en el contexto de clientes, contratos, servicios, proyectos y producción, los activos de aplicaciones incluyen artefactos, automatizaciones y herramientas para apoyar el rendimiento de otros tipos de servicios. (p. 29)

Esta dimensión permite que las organizaciones públicas y privadas puedan dar un servicio de calidad se conviertan en proveedores del servicio, esto quiere decir que el negocio cuenta con personas con las capacidades y competencias que responden de manera oportuna a las necesidades del cliente y del mercado. En esta dimensión el negocio toma el rol de proveedor del servicio con la finalidad de organizarse para que la organización funcione como un engranaje en la que todas las áreas están alineadas con un mismo horizonte, con el único objetivo de cumplir con la misión del negocio. Tiene la característica de apoyar de manera transversal en todos los procesos del negocio considerando los niveles estratégicos, operativos y técnicos.

Kaplan y Norton (2001) citado por Bauset y Rodenes (2013), sobre activos del servicio consideran: “Los activos intangibles como la mayor fuente de ventaja competitiva para una organización. La satisfacción del usuario se considera que formaría parte de dichos activos” (p. 60).

Dentro de los activos, existen dos tipos de activos los tangibles e intangibles. Los activos intangibles además de ser la mayor fuente de ventaja competitiva, se convierte como una estrategia del negocio que dependiendo cual sea el objetivo se tomaran las acciones pertinentes. La satisfacción del usuario es

importante porque se debe cumplir con lo que el usuario solicitó, como un producto y servicio debe tratar de superar las expectativas utilizando estrategias.

Gómez (2007) refiriéndose a activos del servicio dijo que:

> Las políticas de seguridad también deberían prestar atención al control de los equipos que pueden salir de la organización, como los ordenadores portátiles, agendas electrónicas. Como norma general, los equipos y medios informáticos de la organización no podrán ser sacados fuera de sus instalaciones por los empleados sin la correspondiente autorización. Para ello, se establecerán medidas, procedimientos y controles de seguridad para los equipos que deban usarse fuera de los locales de la empresa, de forma que estén sujetos a una protección equivalente a la de los equipos internos. (p. 51)

Cuando la organización implementa el sistema de gestión de seguridad de la información, en ella la alta dirección aprueba y publican las políticas de seguridad de información que se deben dar a conocer a los trabajadores, practicantes y proveedores. En ella están definidas de manera general las políticas de seguridad de la información que regirán la organización. Teniendo como base estas políticas se elaboran las directivas y circulares que normaran la seguridad informática entre ellas tenemos el uso de los equipos informáticos, servicios informáticos y plataformas tecnológicas, administración de las comunicaciones, backups de los sistemas de información, gestión de accesos e identidades.

San- José, Mata y Olalla (2012) citado por Bauset y Rodenes (2013), sobre activos del servicio destacaron: “Para que las tecnologías de información sean eficientes en costes, aportando valor, hay que focalizarse en gestión de los niveles de servicio, gestión de la demanda, capacidad, disponibilidad y control de los activos” (p. 55).

Las tecnologías de información eficientes se administran de manera adecuada hay que considerar tener con los proveedores niveles de servicio con tiempo de entrega, planificar presupuestos, planes de capacitación, planes de capacitación, monitoreo de cumplimiento de las políticas de seguridad en temas de activos.

Dimensión cultura:

Bon et al (2008) refiriéndose a la cultura indicaron que:

> Las organizaciones que desean cambiar (para mejorar la calidad de sus servicios, por ejemplo) se tendrán que enfrentar antes o después con la cultura de la organización, en la que deberán introducir los cambios necesarios para adaptarla al cambio general. La cultura organizativa o corporativa comprende la manera en que las personas se relacionan dentro de la organización, la forma en la que se adoptan e implementan decisiones y la actitud de los empleados hacia su trabajo, los clientes, los proveedores de servicios, los superiores y los compañeros. La cultura depende de los estándares y valores de las personas que forman la organización y no se puede controlar, aunque es posible influir en ella. (p.90)

Esta dimensión permite que las organizaciones públicas y privadas cuenten con los recursos y las capacidades para soportar la atención al cliente producto de la cartera de servicios que brindan las organizaciones, esta dimensión está soportada por personas, procesos, sistemas y tecnologías de información. Las capacidades viene hacer lo que las personas pueden hacer con los recursos destinados mediante los conocimientos adquiridos a través de la experiencia, capacitación y entrenamiento. Tiene la característica de apalancar los objetivos definidos en el plan anual de capacitación. Junto con la dimensión comunicación en organizaciones de servicios de tecnologías de información forman la base para el valor de un servicio, este valor está orientado a conseguir un determinado

objetivo. En el caso de una organización pública o privada, los recursos y capacidades deben estar definidas en las funciones del área de recursos humanos, en la que se tiene como una de las funciones la planificación y ejecución del plan de capacitación de los recursos considerando a todas las áreas de la organización mediante criterio de competencias además de otras.

Gómez (2007) refiriéndose a la cultura dijo que:

> La protección de datos y documentos sensibles deben contar con una política de seguridad relacionada con la protección de datos debe contemplar en primer lugar la clasificación de los documentos y los datos de la organización atendiendo a su nivel de confidencialidad. Una posible clasificación de los documentos y los datos que se podrían adoptar en una empresa sería la información sin clasificar o desclasificada: podría ser conocida por personas ajenas a la empresa, información de uso interno: conocida y utilizada sólo por empleados de la organización, así como por algún colaborador externo autorizado. No obstante, no conviene que ésta sea divulgada a terceros, información confidencial: sólo puede ser conocida y utilizada por determinado grupo de empleados. Su divulgación podría ocasionar daños significativos para la organización, información secreta o reservada. (p. 68)

Los datos de los clientes a través de lo política de seguridad de las organizaciones en la actualidad consideran la clasificación de los datos y documentos, esto es posible esto se fortalece con una directiva aprobada por la alta dirección, en la que los documentos clasificados deben tener el tratamiento de acuerdo a su clasificación de esta manera también se está protegiendo de la confiabilidad. Es importante que los conserjes se les capaciten para que tomen conciencia del tipo de documento que están transportando de esta manera no romper la custodia del documento, es necesario hacer un cargo de responsabilidad.

Según la Contraloría General (2006) en la Resolución N° 320 en que aprueban las Normas de Control Interno, refiriéndose a la cultura precisó:

> Las actividades de supervisión se realizan con respecto de todos los procesos y operaciones institucionales, posibilitando en su curso la identificación de oportunidades de mejora y la adopción de acciones preventivas o correctivas. Para ello se requiere de una cultura organizacional que propicie el autocontrol y la transparencia de la gestión, orientada a la cautela y la consecución de los objetivos del control interno. La supervisión se ejecuta continuamente y debe modificarse una vez que cambien las condiciones, formando parte del engranaje de las operaciones de la entidad. (p. 30)

La importancia de una cultura organizacional está basada fundamentalmente en las actitudes de los trabajadores y clientes de una organización y que se inicia desde el proceso del reclutamiento de personal y la afiliación de los clientes que la empresa quiere tener en la empresa. Periódicamente se debe concientizar en temas de autocontrol y transparencia, complementando esta con reforzamiento de los valores que ya están definidos en los planes estratégicos empresariales.

Beynon (2014) refiriéndose a la cultura dijo:

> La cultura de un grupo social consiste en un conjunto de expectativas de comportamiento asociadas con el grupo. La cultura normalmente se aplica a nivel de las sociedades, pero últimamente es común hablar de la cultura de la organización. La cultura de una organización puede afectar al diseño de los sistemas de información así como a su éxito. El sistema de información de una organización también puede contribuir a los cambios en la cultura de la organización. (p. 246)

Los planes estratégicos empresariales deben definir y dar prioridad a la cultura organizacional en el mismo nivel que los demás objetivos estratégicos,

como por ejemplo el objetivo de atención al cliente. Tener en consideración el sistema de información que se va a implementar ya que este ayudará a lograr los objetivos empresariales. La cultura organizacional es transversal al igual que la seguridad de la información y la calidad.

1.1.1 Bases teóricas de la variable Procedimientos de Seguridad Informática

Según cienciaes.com (s.f.) refiriéndose a la base teórica de la variable procedimientos de seguridad informática:

> Charles Babbage, creador de la primera computadora mecánica, nació en un mundo en el que todos los cálculos matemáticos se hacían a mano. A Babbage, que utilizaba continuamente las tablas matemáticas para sus cálculos y diseños, se lo llevaban los demonios cada vez que encontraba un error, y encontraba muchos. En 1822, Babbage construyó un modelo experimental de su máquina de calcular a la que llamó “máquina de diferencias”. El modelo animó al investigador a diseñar y construir una máquina a gran escala. Más de 10 años invirtió el científico en el diseño de su máquina. El tamaño y la complejidad eran descomunales, sus más de 25.000 piezas, una vez ensambladas, formarían un artefacto de dos metros de alto y pasaría varias toneladas. Babbage no se dio por vencido, al contrario, comenzó a trabajar en un proyecto aún más ambicioso al que denominó “máquina analítica” más que una calculadora, la máquina analítica era un ordenador que contenía los conceptos básicos de una computadora moderna: podía sumar, restar, multiplicar y dividir, era programable y contenía los rudimentos de la memoria y el procesador de los ordenadores actuales. Los bocetos de Babbage durmieron el sueño de los justos durante 135 años en la Biblioteca del Museo de las Ciencias de Londres. En 1985, un investigador de la Universidad de Sydney en

> Australia, llamado Allan G. Bromley, de visita en Londres, examinó los bocetos de Babbage y se convenció de que la Máquina de diferencias Nº 2 podría ser construida. Al fin, en 1991, cuando se cumplieron doscientos años desde el nacimiento de Babbage, la "Máquina de diferencias Nº 2" realizó sus primeros y ajustados cálculos demostrando al mundo la extraordinaria visión de un inventor meticuloso, un visionario excéntrico y científico genial: Charles Babbage.

Telefónica (2014) refiriéndose a la base teórica de la variable procedimientos de seguridad informática:

> Padre de las computadoras John von Neumann fue uno de los matemáticos más importantes de la historia moderna cuyo legado las máquinas autorreplicantes. Fue un niño prodigio en su Hungría natal que a los seis años dividía mentalmente números de ocho dígitos. Quizás su faceta más conocida es su participación en el equipo del **Proyecto Manhattan** que diseñó y fabricó las primeras bombas atómicas que fueron lanzadas sobre Japón a finales de la Segunda Guerra Mundial. En 1949 diseñó **su arquitectura de computadores** para resolver el problema de la necesidad de reconfiguración permanente de los primitivos ordenadores ENIAC; esta arquitectura es prácticamente **la misma que tienen todos los ordenadores actuales.** Y, en fin, fundó la Teoría de Juegos como una rama independiente de las matemáticas. Pero el genio inquieto de von Neumann también postuló teorías más futuristas para problemas que hoy en día todavía pertenecen a la ciencia ficción, como la explotación minera de la Luna o del cinturón de asteroides, la creación de satélites alimentados por energía solar o la construcción de fábricas en otros planetas. Para afrontar tareas de esta complejidad, **ideó conceptualmente la creación de las** *máquinas autor replicantes* con la capacidad de recoger materias primas de su entorno, elaborar las piezas adecuadas y ensamblarlas para generar copias de sí mismas.

Urbina (2012) refiriéndose a la base teórica de la variable procedimientos de seguridad informática:

> Norbert Wiener fundador de la cibernética. Acuñó el término en su libro Cibernética o el control y comunicación en animales y máquinas, publicado en 1948. Durante la Segunda Guerra Mundial trabajó para las Fuerzas Armadas de los Estados Unidos en un proyecto para guiar a la artillería antiaérea de forma automática mediante el empleo del radar. Como resultado de los descubrimientos realizados en este proyecto introduce en la ciencia los conceptos de feedback o retroalimentación, y de cantidad de información, con lo que se convierte en precursor de la teoría de la comunicación o la psicología cognitiva. La Cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. La unión de diferentes ciencias como la mecánica, electrónica, medicina, física, química y computación, han dado el surgimiento de una nueva doctrina llamada Biónica, La cual busca imitar y curar enfermedades y deficiencias físicas. A todo esto se une la robótica, la cual se encarga de crear mecanismos de control los cuales funcionen en forma automática. Todo esto ha conducido al surgimiento de los Cyborg, organismos Bio-mecánicos que buscan imitar la naturaleza humana. Entre los años 1920 y 1923, Wiener se preocupó por un fenómeno físico sin demasiada importancia en esta ciencia, el llamado movimiento browniano, que se refiere al movimiento perpetuo que tienen las partículas disueltas en un líquido (por ejemplo, raspaduras de roca en agua), movimiento irregular que no parece responder a ninguna ley física

Lamarca (2012) refiriéndose a la base teórica de la variable procedimientos de seguridad informática:

Tratándose de la Internet real, una de las influencias decisivas fue Vannevar Bush. En 1957, el gobierno de los Estados Unidos formó la agencia advanced

research projects agency (ARPA), un segmento del Departamento de Defensa encargado de asegurar el liderazgo de los Estados Unidos en la ciencia y la tecnología con aplicaciones militares. En 1962, Licklider la importancia del concepto de "trabajo en red". En 1971 Ray Tomlinson, crea el primer programa para enviar correo electrónico. En 1979 ARPA crea la primera comisión de control de la configuración de Internet y en 1981 se termina de definir el protocolo TCP/IP (transfer control protocol / internet protocol). La world wide web fue creciendo a medida que se desarrollaba nuevo software y nuevas tecnologías. En 1998 el entonces vicepresidente de los EE.UU. anunció a los medios de comunicación una revolución *"más importante que la invención de la imprenta".* Se trataba de Internet2. El proyecto está pensado para aplicaciones como bibliotecas digitales y laboratorios virtuales, telemedicina, teleinmersión, educación a distancia y otras aplicaciones que no serían posibles con la tecnología del Internet de hoy. Ya se han desarrollado proyectos como el protocolo Ipv6, el multicasting (transmisión de mensajes e información desde un ordenador central hacia los demás ordenadores conectados a la red) y la calidad de servicio (QoS) que harán posible una nueva generación de aplicaciones de Internet; pero existen otros muchos proyectos en marcha que tienen que ver con conexiones y redes avanzadas de comunicaciones, interoperatibilidad de tecnologías, conocimientos e inteligencia distribuida, etc.

En los últimos años, las ciberamenazas han ido incrementándose exponencialmente en las empresas de las diversas industrias. Los cibercriminales vulneran los sistemas de información, los sistemas informáticos y plataformas tecnológicas de las organizaciones utilizando técnicas y dispositivos avanzados que les permita comprometer la seguridad de la información de las empresas y sus clientes. La gerencia de informática en coordinación con la gerencia de riesgos y Planeamiento y desarrollo deben definir lineamientos para el desarrollo seguro de aplicaciones que resulta ser la principal línea de defensa contra los ataques dirigidos hacia los sistemas de información. En ella se debe considerar componentes seguros de la arquitectura del software, programación de código, comunicaciones, almacenamiento seguro de datos en los aplicativos,

principalmente los desarrollados en web y considerar periódicamente un análisis de vulnerabilidades de estas con el objetivo de que no representen una amenaza a los activos de una organización. Actualmente existe una ley de protección de datos personales de los clientes y es en ella en que los ciber delincuentes tienen como objetivo de vulnerar los datos personales, datos de clientes, indisponibilidad del servicio, daño a la marca, logos. Lo importante es tener adecuados controles de seguridad para minimizar las pérdidas a nivel económico y reputacional.

Definiciones de la variable Procedimientos de Seguridad Informática

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009) en la Circular N° G-140 sobre los procedimientos de seguridad informática, indico: “procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios” (p. 3).

Las organizaciones deben contar con normas internas en la que se definan claramente la gestión de accesos e identidades de los sistemas de información, servicios informáticos y plataforma tecnológicas donde se deslinden responsabilidades en la administración de roles y perfiles de los usuarios, esto quiere decir que todo acceso a los sistemas de información, sistemas informáticos y plataformas tecnológicas deben estar autorizados por el jefe del área a cargo, la metodología debe estar basada en roles y perfiles.

Costas (2011) refiriéndose a los procedimientos de seguridad informática dijo:

Con la proliferación de la informática en todos los ámbitos de la vida, el número de usuarios y profesionales de informática ha crecido exponencialmente en los últimos años, del mismo modo que las necesidades de comunicación y compartir recursos en red. El desarrollo de las telecomunicaciones en las décadas

de los noventa posibilitó la interconexión de las distintas redes existentes mediante la red global Internet. (p. 18)

La tendencia en este mundo globalizado es que cada día se incrementen los usuarios y mayor número de profesionales de informática, por lo que una forma de estar preparados a este crecimiento es el teletrabajo, que ya está presente y está ganando espacio en nuestra forma de trabajas, por lo que es necesario tener definidos los procedimientos de los trabajadores y clientes para ser colgados en la nube para que puedan tener acceso las personas autorizadas utilizando las telecomunicaciones con la seguridad informática correspondiente.

Según la Norma internacional ISO/IEC 27001 (2013), refiriéndose a los procedimientos de seguridad informática indicó: “Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable” (p. 29)

Los directivos luego de aprobar los procedimientos de seguridad informática, están en la obligación de programar periódicamente auditorías internas con el objetivo de velar el cumplimiento de las políticas de seguridad y del resultado obtenido de las mismas , priorizar las recomendaciones críticas e importantes para implementarlas definiendo planes de trabajo con plazos establecidos , Es importante informar las acciones a tomar a la gerencia de auditoria interna de las acciones que se han tomado con el objetivo de implementar lo recomendado por la auditoria.

Gómez (2013) refiriéndose a los procedimientos de seguridad informática dijo:

> Para gestionar la seguridad informática es preciso contemplar toda una serie de tareas y procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los

> riesgos no se pueden eliminar totalmente, pero si se pueden gestionar. En este sentido, conviene destacar que en la práctica resulta imposible alcanzar la seguridad al 100%. (p. 30)

La actividades de desarrollo, soporte de plataformas y tecnologías de información que se ejecutan en una organización que tiene un área de informática deben estas plasmadas en procedimientos de seguridad informática, estos a su vez alineados a un proceso y subproceso, definir si es crítico para el negocio , quienes son sus clientes y usuarios internos y externos internos y externos , la fecha de aprobación y publicación, este procedimiento debe contar con el visto de los jefes de las áreas involucradas y la aprobación de la gerencia de informática y como últimas acciones publicarla y difundirla a todo el personal involucrado.

Beynon (2014) refiriéndose a los procedimientos de seguridad informática dijo:

> Una estrategia informática define la estructura en la que la información, los sistemas de información y las tecnologías de la información se van a aplicar en una organización en el marco de un tiempo futuro. El término estrategia implica una referencia futura. La planificación informática, el proceso de definir una estrategia informática, está guiada por la organización o planificación empresarial. Por tanto, idealmente, una estrategia informática debería estar muy alineada con la estrategia de la organización. (p. 430)

Para lograr que la estrategia informática este alineada a la empresa se debe hacer a través del plan estratégico de tecnologías de información definiendo los objetivos de tecnologías de información fortaleciéndolo las plataformas tecnológicas, los sistemas de información, los sistemas informáticos y es necesario que con un periodo razonable la gerencia de informática debe reportar el estado al alta dirección el estado de los proyectos. Si el plan estratégico de tecnologías de información está conformado por más de diez proyectos es

conveniente trabajarlo por gestión de portafolio, esto quiere decir que se agrupa por proyectos que tengan las mismas características, actividades y objetivos.

García Moran (2013) refiriéndose a los procedimientos de seguridad informática dijo:

> Los ataques internos son una realidad y representan una gran parte de los ataques informáticos según el FBI. Para poder mejorar la seguridad interna, se deberán hacer políticas más estrictas sobre acceso a recursos de información por parte de los usuarios. No hay motivo alguno para que la secretaria del jefe tenga acceso a la base de datos de cliente desde su ordenador si es que ella no trabaja con estos. (p. 273)

Los accesos a los recursos de información deben estar definidos en un procedimiento de gestión de accesos e identidades de los sistemas de información, sistemas informáticos y plataformas tecnológicas, en la que se definen claramente las responsabilidades de cada trabajador, usuario y cliente. Asimismo, los jefes deben ser concientizados en temas de seguridad de informática para que sepan el riesgo que están asumiendo al momento de dar su contraseña a otras personas. Con la concientización se mitigan los ataques internos que cada día van en aumento.

Consejo Nacional para la Enseñanza y la Investigación de las Ciencias de la Comunicación (2011) refiriéndose a los procedimientos de seguridad informática dijeron:

> La gestión forma parte de procedimientos de seguridad informática que deben llevar a cabo algunas organizaciones, ya sea formal o informal y que les permita salvaguardar los activos de la empresa, en sus prácticas organizativas, así como la información con la que cuente y lo integre, de manera que esta deba ser llevada a cabo con un control en el cumplimiento de estos procedimientos dependiendo el área de trabajo y siempre considerando su cultura organizacional, sus objetivos, riesgos y soluciones. (p. 1040)

Los directivos y las gerencias de las organizaciones deben definir lineamientos y darles los recursos necesarios que permitan salvaguardar los activos de empresa, entre otros tenemos activos de personas, procesos, aplicación, conocimiento, infraestructura, plataformas, información, comunicaciones, cada activo conformado por otros activos, estos conforman la administración de las tecnologías de información. Para salvaguardar estos activos es vital concientizar a los clientes y trabajadores de una organización como ocurre la fuga de la información por ejemplo preguntándose dónde está el dispositivo USB, si este está cifrado y si todos los trabajadores deben tener libre este puerto, evitar dejar documentos en el escritorio, tener en consideración a quién se acepta en el Facebook, dónde se apunta las contraseñas para recordarlas y por ningún motivo compartir la contraseña ya que es personal e intransferible, considerar que los equipos en el que uno accede debe contar con una clave de acceso.

Schmarzo (2014) refiriéndose a los procedimientos de seguridad informática dijo:

> El usuario profesional es el responsable de definir sus procesos empresariales clave, así como identificar la métrica y los indicadores de rendimiento clave utilizados para medir estos procesos empresariales. El usuario profesional es el único que conoce las preguntas que intentan responder y las decisiones que intentan tomar. Es el único que intenta aprovechar los datos y conocimientos disponibles para responder a estas preguntas y tomas las decisiones. (p.66)

Hoy en día las organizaciones recopilan demasiada información en este mundo globalizado y la capacidad operativa no se abastece para analizar la cantidad de data que existe, por lo que existe el termino Big Data que va ser una época en el que el mundo de las tecnologías de información un gran paso. Porque hoy en día hay que estar analizando las redes sociales, análisis de datos en tiempo real, análisis de grandes repositorios de datos. Para pensar en Big Data, se tiene que saber que actualmente se vive en la era de la información, con un

teléfono móvil en cada bolsillo, un ordenador portátil en cada mochila y grandes sistemas de tecnología funcionando diariamente mandando datos y datos cada segundo, se ve claramente que el mundo tiene más datos que nunca, pero esto no es todo, ya que día a día crece aún más. Un ejemplo claro de esto es el del telescopio Sloan Digital Sky Survey construido en el año 2000 en Nuevo México. Durante las primeras semanas este telescopio recopiló más información de los que se habían acumulado en toda la historia de la astronomía, pero esto no es más que un pequeño ejemplo de la gran avalancha que sufrimos en la actualidad. Gracias a esto Big Data se está revolucionando el mundo, organizaciones, personas y tecnología.

Dimensiones de la variable Procedimientos de Seguridad Informática:

Dimensión Seguridad de la Información:

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009) en la Circular N° G-140 sobre la Gestión de la Seguridad de la Información, preciso que: “Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad” (p.2).

La seguridad de la información, es la protección de los activos de información fundamentales para el éxito y viabilidad de los negocios mediante un sistema de gestión de la seguridad de la información que administre los riesgos que atentan la confidencialidad, la integridad y la disponibilidad de la información. El mismo que debe estar formando parte del plan estratégico institucional. Resguardar el cumplimiento de las normativas vigentes. Asimismo, promover la

concientización y capacitación al personal para apoyar el cumplimiento de las políticas y procedimientos de seguridad de la información.

Según la Contraloría General (2006) en la Resolución N° 320 en que aprueban las Normas de Control Interno, refiriéndose a la seguridad de la información precisó:

> La seguridad de la información debe haber un responsable por cada proceso, actividad o tarea organizacional y debe ser claramente definida, específicamente asignada y formalmente comunicada al funcionario Respectivo. La ejecución de los procesos, actividades, o tareas debe contar con la autorización y aprobación de los funcionarios con el rango de autoridad respectivo. (p. 20)

Las organizaciones que se preparan para mantenerse en el mercado tienen que tener seguridad, por lo que implementan un sistema de gestión de seguridad de la información, este sistema está conformado por procesos, procedimientos, estos por actividades, tareas y guías. Lo importante en el sistema de gestión de seguridad de la información es que los procesos deben contar con un dueño o propietario, es importante señalar que en un proceso participan varios actores, pero es responsabilidad de la alta dirección designar a un deño del proceso, siendo recomendable que sea el mismo que se desempeña como gestor del riesgo del proceso.

Bauset y Rodenes (2013) refiriéndose a la Seguridad de la información dijeron que “para reducir el número de incidentes influyen el grado de cumplimiento de requisitos de seguridad y si los proveedores cubren las necesidades del servicio” (p. 59).

Los incidentes de seguridad de información en las organizaciones cada vez incrementa por lo que es necesario que la alta dirección planifique revisiones periódicas del cumplimiento de las políticas de la seguridad de la información de las normas ISO 27001 para determinar el grado de cumplimiento de los controles definidos en dicha norma. Asimismo, motivar a los clientes, proveedores y

trabajadores a identificar las oportunidades de mejoras de esta manera se fortalecerá la mejora continua del sistema de la gestión de seguridad de la información.

Costas (2011) refiriéndose a la seguridad de la información dijo “La política de seguridad que se desarrolló respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos especificando las consideraciones necesarias para el establecimiento de perfiles de usuario” (p. 97).

Cada vez que se habla de seguridad lógica es importante considerar la gestión de accesos e identidades, basada en una metodología por roles esto quiere decir que un usuario para acceder a los sistemas de información puede tener uno o varios roles, estos van a surgir por un cambio organizacional, nuevas funciones, nuevos o modificaciones de los sistemas informáticos o también por regulaciones o auditorías internas o externas.

Dimensión Confidencialidad:

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009) en la Circular N° G-140 sobre la confidencialidad, preciso: “La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados” (p. 2).

Esta dimensión permite la protección de la información frente a posibles accesos no autorizados, con independencia del lugar en que reside o la forma en que se almacena. Tiene la propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados. Junto con las dimensiones de integridad y disponibilidad forman los criterios de la seguridad de la información. En el caso de una organización pública o privada, la confidencialidad debe realizarse mediante informes periódicos cortos para verificar el cumplimiento de la misma.

Gómez (2013) refiriéndose a la Confidencialidad dijo:

> Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. (p. 20)

Hoy en día las empresas cuidan mucho su reputación e imagen y este prestigio se demuestra en la confidencialidad que hay al momento de prestar los servicios. Entonces se debe asegurar que la base de datos que contiene los datos de los clientes esté encriptados. Asimismo, asegurar el medio por donde se realiza el transporte de dicha data y si el usuario accede a los servidores de las base de datos vía remoto se realice mediante una red de comunicaciones segura desde el punto remoto de donde se va acceder hasta el servidor.

García- Moran (2013) refiriéndose a la Confidencialidad dijo:

> Contempla que el acceso a los datos lo realizan las personas o usuarios autorizados para ello. Al crear una comunicación entre dos puntos, es tremendamente complicado determinar con absoluta seguridad que no está siendo captada por otros. Esto podría ser posible debido a que hay una ausencia de control de la comunicación por las partes que la establecen, con lo cual la única posibilidad factible para establecer seguridad en la comunicación es encriptándola. (p. 494)

Para que una comunicación entre dos puntos sea efectiva y segura el transporte de los datos debe ser encriptado eso quiere decir que el que envía un mensaje tiene dos llaves una publica y otra privada, de igual manera el que recibe el mensaje también tiene dos llaves con la publica recibe el mensaje y con la llave privada abre el mensaje y podrá tener acceso al contenido, de esta manera se

está asegurando que el acceso a la información lo realizan las personas o usuarios autorizados.

Dimensión Integridad:

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009) en la Circular N° G-140 sobre la integridad, preciso: “La información debe ser completa, exacta y válida” (p.2).

Esta dimensión permite la protección de la información, datos, sistemas y otros activos relacionados contra cambios o alteraciones en su estructura o contenido, sea intencionada, no autorizada o casual. Tiene la propiedad de salvaguardar la exactitud y completitud de los activos. En el caso de una organización pública o privada, la integridad debe ser monitoreada ya que estas son las mantiene la imagen de una organización a través de los usuarios, medios de prensa y comunicación.

Costas (2011) refiriéndose a la integridad dijo “Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original” (p. 25).

Las organizaciones que implementan el sistema de gestión de seguridad de la información, consideran en uno de sus pilares fundamentales la integridad de la información en la que describe el tratamiento y responsabilidad de las personas que utilizan la información. Asimismo, para minimizar los riesgos de integridad las organizaciones se apoyan en los sistemas de información en los sistemas informáticos y plataformas tecnológicas.

García-Moran (2014) refiriéndose a la integridad dijo:

No se deben permitir alteraciones en la información que se está transmitiendo, ya que su integridad es fundamental, imaginemos un mensaje totalmente alterado, donde se informa de un cantidad de dinero que es el doble de la original, números de tarjetas de red. (p. 494)

Los datos y la información son solicitados por usuarios y clientes, los mismos que sirven como entrada o salida de un proceso. Este insumo o resultado debe estar encriptado en el momento de la recepción o entrega y tener en consideración que el medio de transporte se encuentre encriptado de esta manera no existe alteración de la data o información y como está encriptado no podrán hacer snifing escucha del tráfico de la información que en ese momento está pasando.

Dimensión Disponibilidad:

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009) en la Circular N° G-140 sobre la disponibilidad, preciso: “La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida” (p.2).

Esta dimensión tiene la garantía de que los usuarios autorizados puedan acceder a la información cuando los necesiten. Tiene la propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada. Junto con las dimensiones de confidencialidad e integridad forman los criterios de la seguridad de la información. En el caso de una organización pública o privada, la disponibilidad debe ser adecuada razonable, es decir, para esta dimensión es mantenar la disponibilidad de la información.

Bauset y Rodenes (2013) refiriéndose a la disponibilidad dijeron “para aportar valor a una organización los servicios de tecnologías de información deben gestionar eficientemente la disponibilidad, continuidad y capacidad de los equipos, mejorar los tiempos de respuesta de resolución de los incidentes, y procurar la satisfacción del cliente” (p. 54).

Para garantizar la disponibilidad y continuidad de la información las organizaciones se apoyan en las tecnologías de información y de esta manera garantizan que la información esté disponible cada vez que un usuario quiera tener acceso. Una de las medidas es el monitoreo de 24 por 7 de los servicios y procesos críticos de la organización con un monitoreo tipo semáforo amarillo, azul y rojo, eso quiere decir que cuando se observa un mensaje amarillo es que se ha iniciado una alerta, si la alerta es azul y la probabilidad es mayor para convertirse en un incidente y si la alerta es roja quiere decir que se ha materializado el incidente , por eso es recomendable tomar acciones cuando la alerta es amarillo y minimizar los incidentes de esta manera no se interrumpe la atención a los clientes .

Costas (2011) refiriéndose a la disponibilidad dijo “se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios autorizados cuando estos lo requieran” (p. 26).

Las organizaciones modernas en sus estructuras organizacionales deben considerar un área de operaciones y control de plataformas, definiendo la función de mantener la disponibilidad de los sistemas de información, sistemas informáticos y plataformas tecnológicas para el uso de los clientes y usuarios.

Gómez (2013) refiriéndose a la disponibilidad dijo que:

> La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de

> manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios. (p. 21)

Los planes estratégicos empresariales definen los proyectos, actividades y procesos que se van a realizar en un determinado tiempo y este a su vez se ejecutan mediante los planes estratégicos operativos que tienen una duración de un año y en este plan está incluido el plan estratégico de tecnologías de información en la cual están los proyectos de tecnologías de información y uno de ellos debe ser el plan de contingencia de tecnologías de información, este plan tiene como objetivo principal mantener la disponibilidad de los sistemas de información, sistemas informáticos y plataformas tecnológicas para que estén disponibles en el momento que los usuarios y clientes desean acceder a sus servicios.

1.3 Justificación

Hernández, et al (2014) refiriéndose a la justificación de la investigación afirman que:

> Justificación de la investigación indica el porqué de la investigación exponiendo sus razones. Por medio de la justificación debemos demostrar que el estudio es necesario e importante. Además de los objetivos y las preguntas de investigación, es necesario justificar el estudio mediante la exposición de sus razones (el para qué del estudio o por qué debe efectuarse). La mayoría de las investigaciones se ejecutan con un propósito definido, pues no se hacen simplemente por capricho de una persona, y ese propósito debe ser lo suficientemente significativo para que se justifique su realización. (p. 40)

1.3.1 Justificación teórica

La presente investigación fundamenta y resalta el conocimiento de la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática. El conocimiento está estructurado desde las bases teóricas, antecedentes y citas .Aporta conocimientos científicos recolectados de una manera organizada en el marco internacional, nacional y local de las variables y dimensiones de la administración de tecnologías de información y de los procedimientos de seguridad informática. El aporte teórico de esta investigación está enfocada en los resultados obtenidos que demuestran que existe incidencia de las tecnologías de información en los procedimientos de seguridad informática, por lo que es importante que las gerencias de las empresas deben darle la importancia y prioridad a la administración de tecnologías de información ya que el conocimiento obtenido en esta investigación es que la única constante es el cambio por lo tanto se debe estar preparado para los cambios tecnológicos.

Se resalta la importancia de la seguridad de informática de una forma transversal en todos los procesos de la organización, así mismo el conocimiento de los procedimientos de seguridad informática, resalta las tendencias en el mercado como big data, cibernética que son tendencia, estos conocimientos están en todo el desarrollo de la investigación. Conocimientos necesarios que los clientes y usuarios de las organizaciones deban tener presente en el momento de usar los sistemas informáticos, los servicios informáticos y plataformas tecnológicas. También es importante tener en consideración los lineamientos de la seguridad informática para minimizar los riesgos, fraudes y fuga de información.

1.3.2 Justificación Práctica

La presente investigación fundamenta y resalta la incidencia que juega la administración de tecnologías de información en los procedimientos de seguridad informática en el desarrollo integral de los profesionales. El aporte práctico de esta investigación, es fundamental para comprender que los directivos de la administración de tecnologías de información, deben desarrollar sus estrategias y métodos en función de la realidad en que la información se incrementa

exponencialmente en las organizaciones estatales y públicas y que es de vital importancia incidir en los profesionales de seguridad informática.

La presente investigación, resalta la cultura de los profesionales de seguridad informática que debe cumplir como parte de su desarrollo de las funciones encomendadas, sostiene que es necesario que el trabajador tome conciencia de la importancia de tener actualizados y elaborar nuevos procedimientos de seguridad informática. Se busca con este trabajo incentivar las buenas prácticas que se describen en las normas de regulación y control interno y externo. Además desde la incorporación de los trabajadores a las organizaciones estatales y privadas se debe realizar en la inducción conocimientos de buenas prácticas de la administración de tecnologías de información y su incidencia en los procedimientos de seguridad informática.

1.3.3 Justificación Metodológica

Los motivos de la presente investigación es que estamos viviendo la era de la información y del conocimiento, asimismo, tenemos la generación de los milenios y de pronto tenemos que estamos siendo atacados por ciber delincuentes que están continuamente jaqueando las organizaciones tratando de buscar puntos por donde vulnerar o hacer phishig. Uno de los beneficios de la presente investigación es la importancias de la gestión de servicios de tecnologías de información a través de los activos de información, las mismas que se realizan un inventario, se clasifica y se dan el tratamiento según su clasificación con los controles de seguridad informática respectivamente, de esta manera las organizaciones cuando llegue el momento de que han vulnerado cualquiera de los activos de información el impacto va ser mínimo ya que podrán tener el activo pero no podrán acceder a la información por estar encriptado, por eso es importante concientizar en el temas de las políticas de seguridad de la información con sus tres pilares, la confidencialidad, la integridad y la

disponibilidad porque de esta manera estamos asegurando una atención razonable para el cliente y el usuario.

Las tecnologías de información cambian constantemente y la cantidad de información que se tiene, cada vez incrementa exponencialmente. El aporte metodológico de la presente investigación es la utilización de instrumentos para recopilar información, las cuales fueron realizadas al personal de tecnologías de información.La presente investigación si es factible su aplicación ya que los aportes entregados ayudan mucho a los gerentes para la toma de decisiones y el beneficio es a los clientes y usuarios. Las conclusiones a donde se ha llegado servirán como un aporte de la investigación a otras investigaciones así como la estadística utilizada

1.4 Problema

En los últimos años, los procedimientos de seguridad informática no han sido documentados adecuadamente y la información cada día es cada vez mayor. A pesar de innumerables instituciones nacionales e internacionales han manifestado su preocupación y están emprendiendo acciones para superar este problema mediante una razonable administración de tecnologías de información, las mejoras aún no son evidentes.

En los últimos 5 años los procedimientos de seguridad informática en América Latina se ha incrementado exponencialmente, esto trae como consecuencia procedimientos desactualizados y nuevos por elaborar. Se requiere con suma urgencia solucionar estos problemas, se debe generar una nueva cultura organizacional en las organizaciones, es decir se requiere de una adecuada cultura orientada a los trabajadores de que cada uno debe elaborar sus

procedimientos de seguridad informática en las funciones que desempeña, concientizándolos para crear una actitud para documentar y mantener actualizados los procedimientos de seguridad informática y ellos a su vez sean los portadores de esta buena práctica a los demás trabajadores de otras áreas.

La administración de tecnologías de información, surge nuevamente como medio para solucionar estos problemas, así pues la administración de tecnologías de información no es nueva en el mundo, sin embargo es nuestro país, no es efectiva, pues no se basa en programas efectivos o que consideren la realidad individual de cada una de las instituciones de nuestro país, debido probablemente a que los directivos o administradores de las tecnologías de información, desconocen la implicancia que estas carencias tienen en el desarrollo integral de las instituciones que se administra. Por lo tanto es muy necesario que los directivos que están a cargo de la administración de las tecnologías de información, deben tener claro estos problemas para que puedan estrategias para desarrollar actitudes para actualizar y elaborar los procedimientos de seguridad informática.

En las organizaciones estatales y particulares, se forman generaciones de recursos humanos que cada día ven en las actividades cotidianas de su trabajo, recarga laboral, los requerimientos han superado la capacidad operativa y no se motiva la cultura de actualización y elaboración de procedimientos de seguridad informática, todo esto por la indiferencia de sus directivos por falta de conocimiento de la administración de tecnologías de información.

En la actualidad las instituciones del Estado, afronta serios problemas de debido que no cuentan con procedimientos de seguridad informática y si es que existen están desactualizados. Esta situación puede explicarse en parte por la falta de conocimiento o de información para documentar los procedimientos de seguridad informática, el desinterés de las gerencias de tecnologías de información, así como la actitud negativa de los trabajadores que no estiman la importancia de documentar los procedimientos de seguridad informática, realizando las funciones indicadas sin contar son un documento formal que los

oriente. Todo lo descrito pone en evidencia que en la institución de estudio se carece de una cultura de actualización y elaboración de procedimientos de seguridad informática, sobre todo la orientada a los trabajadores de las áreas de tecnologías de información y riesgos.

Así mismo, en la institución financiera del Estado, se observa que los directivos y trabajadores no se encuentran comprometidos con el desarrollo de actividades relacionadas con el la cultura de documentar procedimientos de seguridad informática o que estén encaminadas a desarrollar actitudes de actualización y elaboración de los procedimientos de seguridad informática en sus trabajadores. Todo esto debido fundamentalmente al escaso conocimiento que se posee acerca de las implicancias de no tener los procedimientos de seguridad informática actualizados y los nuevos a elaborar, ya que esto implica incumplimiento con las auditorías internas, auditorías externas, entidades reguladoras , certificaciones ISOs y normas técnicas peruanas.

Los factores antes mencionados, generaron en el investigador una actitud de preocupación frente a estas carencias, las mismas que afectan el desarrollo integral de las funciones de los trabajadores de las áreas de seguridad informática, por lo que considero muy importante intervenir metodológicamente y aprovechar la capacidad de asimilación que tiene los profesionales de seguridad informática. Los trabajadores durante las primeras etapas de formación profesional, se encuentran en una etapa formativa clave para la enseñanza de buenos hábitos y es el mejor momento para transmitir conceptos, conocimientos con mensajes conservacionistas orientados a la participación activa, consiente y responsable en el individuo.

La administración de tecnologías de información debe fomentar el desarrollo de la conciencia y valores necesarios para mejorar la calidad de los procedimientos de seguridad informática, razón por la cual, planteo en este trabajo de investigación, medir la incidencia que tiene el uso de una administración de tecnologías de información sobre el desarrollo de

procedimientos de seguridad informática en los profesionales que se encuentran en las áreas de tecnologías de información y seguridad.

El área de la seguridad de la información inicio sus funciones en la gerencia de riesgos, luego de una restructuración se dividieron las funciones naciendo seguridad informática dentro de la gerencia informática en el Banco de la Nación. Por lo tanto las normas y procedimientos estaban orientados a la seguridad de la información y debido a esta segregación de funciones la administración de tecnologías de información en los procedimientos de seguridad informática también deberían ser actualizados, los procedimientos son desarrollados funcionalmente y no orientados a procesos y no tienen como base un marco referencial de negocio para el gobierno y la gestión de tecnologías de la empresa, que se ayudará a crear valor optimo desde las tecnologías de información, satisfacer las necesidades de los stakeholder internos y externos, optimizar los recursos, separar el gobierno de la administración.

1.4.1 Formulación del Problema:

Para realizar la presente investigación, se han planteado los siguientes problemas:

Problema General

¿Cuál es la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016?

Problemas específicos:

Problema específico 1

¿Cuál es la incidencia de la administración de tecnologías de información en la seguridad de la información del Banco de la Nación, 2016?

Problema específico 2

¿Cuál es la incidencia de la administración de tecnologías de información en la confidencialidad del Banco de la Nación, 2016?

Problema específico 3

¿Cuál es la incidencia de la administración de tecnologías de información en la Integridad del Banco de la Nación, 2016?

Problema específico 4

¿Cuál es la incidencia de la administración de tecnologías de información en la disponibilidad del Banco de la Nación, 2016?

1.5 Hipótesis:

Hipótesis general

La administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016.

Hipótesis específicas:

Hipótesis especifica 1

La administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016.

Hipótesis especifica 2

La administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016.

Hipótesis especifica 3

La administración de tecnologías de información incide en la Integridad del Banco de la Nación, 2016.

Hipótesis especifica 4

La administración de tecnologías de información incide en la disponibilidad del Banco de la Nación, 2016.

1.6 Objetivos

Objetivo General

Determinar la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016.

Objetivos Específicos:

Objetivo específico 1

Determinar la incidencia de la administración de tecnologías de información en la seguridad de la información del Banco de la Nación, 2016.

Objetivo específico 2

Determinar la incidencia de la administración de tecnologías de información en la confidencialidad del Banco de la Nación, 2016.

Objetivo específico 3

Determinar la incidencia de la administración de tecnologías de información en la Integridad del Banco de la Nación, 2016.

Objetivo específico 4

Determinar la incidencia de la administración de tecnologías de información en la disponibilidad del Banco de la Nación, 2016.

II. MARCO METODOLÓGICO

2.1. Variables:

Hernández, et al (2014) refiriéndose a la variable afirman que: “una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse” (p.93).

Definición conceptual:

Definición conceptual de la variable: Administración de tecnologías de información

Según Bon et al (2008) refiriéndose a la administración de tecnologías de información indicaron que:

> La administración de servicios de tecnologías de información ha pasado a ser el enfoque centrado en servicios y procesos de lo que anteriormente se llamó gestión de las tecnologías de la información. El desplazamiento de la gestión desde la infraestructura hasta los procesos ha llevado a la aparición de la gestión de servicios de tecnologías de información como una disciplina centrada en servicios y procesos. Los procesos siempre deben tener un objetivo definido. El objetivo de los procesos de gestión de servicios de tecnologías de información es contribuir a la calidad de los servicios. La gestión de la calidad y el control de procesos forman parte de la organización y sus políticas. (p. 86)

Definición conceptual de la variable: Procedimientos de seguridad informática

Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009), en la Circular N° G-140 sobre los procedimientos de seguridad informática, indico que: “procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios” (p. 3).

Definición operacional:

Hernández, et al (2014) refiriéndose a la definición operacional, afirman que:

> Constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar para recibir las impresiones sensoriales, las cuales indican la existencia de un concepto teórico en mayor o menor grado (Reynolds, 1986, p.52). En otras palabras, especifica qué actividades operaciones deben realizarse para medir una variable e interpretar los datos obtenidos. Una decisión operacional nos dice que para recoger datos respecto de una variable, hay que hacer esto y esto otro, además articula los procesos o acciones de un concepto que son necesarios para identificar ejemplos de éste (MacGregor, 2006). (p. 120)

La operacionalización de presente investigación, utilizó este proceso metodológico que consiste en descomponer deductivamente las variables que lo componen el problema de investigación, partiendo desde lo más general a lo más específico; es decir que estas variables se dividen en dimensiones, indicadores e ítems.

Definición operacional de la variable: Administración de tecnologías de información

Operacionalmente la variable administración de tecnologías de información se define mediante las dimensiones: gestión de servicios de tecnologías de información y procesos, funcionalidad y garantía, recursos y capacidades, activos de servicio y cultura. Asimismo cada dimensión tiene sus indicadores y a estos se les formuló dos ítems por cada indicador.

Definición operacional de la variable: Procedimientos de seguridad informática

Operacionalmente la variable procedimientos de seguridad informática se define mediante las dimensiones: seguridad de la información, confidencialidad, integridad y disponibilidad. Asimismo cada dimensión tiene sus indicadors y a estos se les formuló dos ítems por cada indicador.

2.2. Operacionalización de las variables:

Hernández, et al (2014) refiriéndose a la operacionalidad de las variables, afirma que:

> El paso de una variable teórica a indicadores empíricos verificables y medibles e ítems o equivalentes se le domina operacionalización (Solis, 2013). La operacionalización se fundamenta en la definición conceptual y operacional de la variable. El proceso más lógico para hacerlo es transitar de la variable a sus dimensiones o componentes, luego a los indicadores y finalmente a los ítems o reactivos o sus categorías. (p.211)

La tabla de operacionalización de presente investigación, sirve para establecer la consistencia interna entre las dimensiones, indicadores, ítems, escala y valores, niveles y rangos.

Tabla 1

Operacionalización de la variable administración de tecnologías de información

Dimensiones	Indicadores	Cantidad de ítems	Ítems	Escala y valores	Niveles	Rango o intervalo
Gestión de servicios de tecnologías de información y procesos	Coherencia y organización Estructura de procesos Calidad de los servicios de tecnologías de información	6	1 - 6		Malo Regular Bueno	(6 - 14) (15 - 22) (23 - 30)
Funcionalidad y garantía	Resultados del negocio Percepción del usuario Valor económico Riesgo		7 - 14		Malo Regular Bueno	(8 - 19) (20 - 30) (31 - 40)
Recursos y capacidades	Crear valor Habilidad de la organización Experiencia adquirida	8	15 - 20	Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)	Malo Regular Bueno	(6 - 14) (15 - 22) (23 - 30)
Activos de servicio	Actividades de organización Actividades de proceso Actividades de conocimiento Actividades de información Actividades de aplicaciones	10	21 - 30		Malo Regular Bueno	(10 - 23) (24 - 36) (37 - 50)
Cultura	Actitud de los empleados Valores de las personas Adaptar al cambio	6	31 - 36		Malo Regular Bueno	(6 - 14) (15 - 22) (23 - 30)
Administración de tecnología de información		36	36			

Tabla 2

Operacionalización de la variable procedimientos de seguridad informática:

Dimensiones	Indicadores	Cantidad de ítems	Ítems	Escala y valores	Niveles	Rango o intervalo
Seguridad de la información	Políticas de seguridad de la información				Bajo	(8 - 19)
	Procedimientos de seguridad informática		1 - 8		Moderado	(20 - 30)
	Estructura organizacional				Alto	(31 - 40)
	Herramientas informáticas					
		8				
Confidencialidad	Gestión de accesos				Bajo	(8 - 19)
	Cuentas no permitidas				Moderado	(20 - 30)
	Duplicidad de roles		9 - 16		Alto	(31 - 40)
	Cuentas no conformes			Nunca (1)		
		8		Casi nunca (2)		
Integridad	Gestión de clientes			A veces (3)	Bajo	(4 - 9)
	Gestión de Vulnerabilidades			Casi siempre (4)	Moderado	(10 - 14)
			17 - 20	Siempre (5)	Alto	(15 - 20)
		4				
Disponibilidad	Gestión de roles				Bajo	(8 - 19)
	Usuarios atendidas durante el plazo				Moderado	(20 - 30)
	Requerimientos enviadas fuera del plazo		21 - 28		Alto	(31 - 40)
	Usuarios atendidos fuera del plazo					
		8				
Procedimientos de seguridad informática		28	28			

2.3. Metodología:

2.4. Tipo de estudio

El tipo de estudio en este caso está dentro de la Investigación básica, al respecto, Valderrama expresa que la investigación básica:

> Es conocida también como investigación teórica, pura o fundamental. Está destinada a aportar un cuerpo organizado de conocimientos científicos y no produce necesariamente resultados de utilidad práctica inmediata. Se preocupa por recoger información de la realidad para enriquecer el conocimiento teórico científico, orientado al descubrimiento de principios y leyes (2013, p.164).

La presente investigación es básica, este tipo de estudio pretende profundizar en el conocimiento teórico de las variables a administración de tecnologías de información y procedimientos de seguridad informática.

Enfoque cuantitativo

Hernández, et al (2014) refiriéndose al enfoque cuantitativo, afirma que:

> El enfoque cuantitativo, que representa como dijimos, un conjunto de procesos, es secuencial y probatorio .Cada etapa precede a la siguiente y no podemos brincar o eludir pasos. El orden es riguroso, aunque desde luego, podemos redefinir alguna fase. Parte de una idea que va acotándose y una vez limitada , se derivan objetivos y preguntas de investigación , se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y se determinan variables; se traza un plan para probarlas (diseño), se miden las variables en un determinado contexto; se analizan las mediciones obtenidas utilizando métodos estadísticos se extrae una serie de conclusiones respecto de la o de las hipótesis. (p. 4)

La presente investigación ha utilizado un enfoque cuantitativo, ya que se ha utilizado los procedimientos del método científico como un método general y unitario. Además se ha utilizado la estadística como una herramienta para el recojo de los datos, su procesamiento, análisis y presentación de los resultados.

2.5. Diseño

Hernández, et al (2014) refiriéndose al diseño, afirman que:

> El término diseño se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema. En el enfoque cuantitativo el investigador utiliza sus diseños para analizar la certeza de las hipótesis formuladas en un contexto en particular o para aportar evidencias respecto de los lineamientos de la investigación, si es que no se tiene hipótesis. (p.128)

El diseño de la presente investigación es no experimental, transeccional o transversal, correlacional causal para ello establecemos las siguientes definiciones:

Diseño no experimental

Hernández, et al (2014) refiriéndose al diseño no experimental, afirman que "Estudios que se realizan sin la manipulación deliberada de variables y en los que solo se observan los fenómenos en su ambiente natural para analizarlos". (p. 152)

Este tipo de diseño se ajusta a la presente trabajo debido a que el desarrollo de la investigación tiene un tiempo limitado y toda la información que se analizado fue obtenida en un solo instante. No ha existido manipulación de los datos de las variables.

Diseño correlacional - causal:

Hernández, et al (2014) refiriéndose al diseño correlacional - causal, afirman que:

> Este tipo de estudio descriptivo tiene como finalidad determinar el grado de relación o asociación no causal existente entre dos o más variables. Se caracterizan porque primero se miden las variables y luego, mediante pruebas de hipótesis correlacionales y la aplicación de técnicas estadísticas, se estima la correlación. Aunque la investigación correlacional no establece de forma directa relaciones causales, puede aportar indicios sobre las posibles causas de un fenómeno. (2010, p.201).

Este tipo de diseño busca determinar el grado de causalidad de la variable administración de tecnologías de información en los procedimientos de seguridad informática.

2.6. Población, muestra y muestreo:

Población.

Hernández, et al (2014) refiriéndose a la población, afirman que:

> Una vez que se ha definido cuál es la unidad de muestreo se procede a delimitar la población que va hacer estudiada y sobre la cual se pretende generalizar los resultados. Así, una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones. (p.174)

Es importante describir de manera clara y precisa las características de la población, en este estudio la población está constituida por 154 profesionales en tecnologías de información del Banco de la Nación.

Muestra.

Hernández, et al (2014) refiriéndose a la muestra, afirman que:

> Para el proceso cuantitativo, la muestra es un subgrupo de la población de interés sobre el cual se recolectaran datos, y que tiene que definirse y delimitarse de antemano con precisión, además de que debe ser representativo de la población. El investigador pretende que los resultados encontrados en la muestra se generalicen o extrapolen a la población. El interés es que la muestra sea estadísticamente representativa. (p.173)

Con el objetivo de que los resultados encontrados en la muestra se generalicen o extrapolen a la población, en la presente investigación se recolectaron los datos a través de la aplicación de dos cuestionarios a 110 trabajadores del Banco de la Nación.

Según Bernal (2006), "la muestra es la parte de la población que se selecciona, de la cual realmente se obtiene la información para el desarrollo del estudio y sobre la cual se efectuarán la medición y la observación de las variables objeto de estudio" (p.165).

La muestra seleccionada es aleatoria simple; y su tamaño(n), según Bernal (2006:171), se puede calcular aplicando la siguiente fórmula:

$$n = \frac{Z^2 P.Q.N}{\varepsilon^2 (N-1) + Z^2.P.Q}$$

Dónde:

Z (1,96): Valor de la distribución normal, para un nivel de confianza de (1 – α)
P (0,5): Proporción de éxito.
Q (0,5): Proporción de fracaso (Q = 1 – P)
ε (0,06): Tolerancia al error
N (154): Tamaño de la población.

N: Tamaño de la muestra.

Reemplazando tenemos:

$$n = \frac{(1{,}96)^2(0{,}5)(0{,}5)\times 154}{0{,}06^2(154-1)+1{,}96^2.(0{,}5)(0{,}5)} = 110$$

Es decir, para el desarrollo de la presente investigación, aplicaremos los cuestionarios a 110 trabajadores del Banco de la Nación

Muestreo Probabilístico

Hernández, et al (2014) refiriéndose al muestreo probabilístico, afirman que:

> En las muestras probabilísticas, todos los elementos de la población tienen la misma posibilidad de ser escogidos para muestra y se obtienen definiendo las características de la población y el tamaño de la muestra, y por medio de una selección aleatoria o mecánica de las unidades de muestreo. (p.175)

Las muestras probabilísticas nos aseguran que la muestra que se ha elegido tiene inferencia en la población, quiere decir que cualquier individuo tiene la misma posibilidad de ser elegido para formar parte de la muestra. Es un procedimiento que se utiliza para determinar la muestra.

2.7. Técnicas e instrumentos de recolección de datos:

Técnicas:

Morone (2012), refiriéndose a las técnicas de investigación afirma que “Las técnicas son los procedimientos e instrumentos que utilizamos para acceder al conocimiento. Encuestas, entrevistas, observaciones y todo lo que se deriva de ellas” (2012, p.3).

En el presente estudio se utilizó la técnica de encuesta.

Técnica la encuesta

Asimismo Morone (2012), sobre la encuesta afirma que “Se utiliza el término encuesta para referirse a la técnica de recolección de datos que utiliza como instrumento un listado de preguntas que están fuertemente estructuradas y que recoge información para ser tratada estadísticamente, desde una perspectiva cuantitativa (p.17).

La presente investigación ha utilizado la técnica de la encuesta para la recolección de datos. Por lo que a la muestra de trabajadores del Banco de la Nación se administraron dos cuestionarios con escala de medición tipo Likert.

Medición tipo Likert

Hernández, et al (2014) refiriéndose a la medición tipo Likert, afirman que:

> El método fue desarrollado por Rensis Likert en 1932; sin embargo, se trata de un enfoque vigente y bastante popularizado. Consistente en un conjunto de ítems presentados en forma de afirmaciones o juicios, ante los cuales se pide la reacción de los participantes. Es decir, se presenta cada afirmación y se solicita al sujeto que externe su reacción eligiendo uno de los cinco puntos o categorías de la escala. A cada punto se le asigna un valor numérico. Así el participante obtiene una puntuación respecto de la afirmación y al final su puntuación total, sumando las puntuaciones obtenidas en relación con todas las afirmaciones. (p. 238)

La presente investigación ha utilizado la medición tipo Liker y como fue dirigida a profesionales en tecnologías de información técnica los dos cuestionarios tuvieron la escala de nunca (1), casi nunca (2), a veces (3), casi siempre (4) y Siempre (5).

Instrumento:

Hernández, et al (2014) refiriéndose a la muestra, afirman que “En la investigación disponemos de múltiples tipos de instrumentos para medir las variables de interés y en algunos casos llegan a combinarse varias técnicas de recolección de datos” (p.217).

La formulación de los instrumentos de evaluación aplicada en la presente investigación se elaboró de tal manera que tengan la calidad adecuada y razonable para obtener una acertada realidad de las variables investigadas. En la presente investigación se utilizó un cuestionario para cada variable a medir.

Cuestionario:

Las preguntas que se elaboraron fueron cuidadosamente dirigidas y contestadas por personal profesional en tecnologías de información del Banco de la Nación

Cuestionario sobre la administración de tecnologías de información

Datos generales	
Título:	Cuestionario sobre la administración de tecnologías de información
Autor:	Br. Pérez Castillo, María Rosario
Procedencia:	Lima – Perú, 2016
Objetivo:	Describir las características de la variable administración de tecnologías de información en el Banco de la Nación – 2016
Administración:	Individual
Duración:	15 minutos

Significación:	El cuestionario está referido a determinar la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática
Estructura:	La escala consta de 36 ítems, con 05 alternativas de respuesta de opción múltiple, de tipo Likert, como: Nunca (1), Casi nunca (2), A veces (3), Casi siempre (4) y Siempre (5). Asimismo, la escala está conformada por 04 dimensiones, donde los ítems se presentan en forma de proposiciones con dirección positiva y negativa sobre la administración de tecnologías de información

Cuestionario sobre los procedimientos de seguridad informática

Datos generales

Título:	Cuestionario sobre los procedimientos de seguridad informática
Autor:	Br. Pérez Castillo, María Rosario
Procedencia:	Lima – Perú, 2016
Objetivo:	Describir las características de la variable procedimientos de seguridad informática en el Banco de la Nación – 2016
Administración:	Individual
Duración:	15 minutos
Significación:	El cuestionario está referido a determinar la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática
Estructura:	La escala consta de 28 ítems, con 05 alternativas de respuesta de opción múltiple, de tipo Likert, como: Nunca (1), Casi nunca (2), A veces (3), Casi

> siempre (4) y Siempre (5). Asimismo, la escala está conformada por 04 dimensiones, donde los ítems se presentan en forma de proposiciones con dirección positiva y negativa sobre los procedimientos de seguridad informática

Validación y confiabilidad del instrumento:

Validez

Hernández, et al (2014) refiriéndose a la validez, afirman que “La validez, en términos generales, se refiere al grado en que un instrumento mide realmente la variable que pretende medir” (p.200).

Validez de expertos

Hernández, et al (2014) refiriéndose a la validez, afirman que “Grado en que un instrumento realmente mide la variable de interés, de acuerdo con expertos en el tema” (p. 204)

Validez de contenido

Hernández, et al (2014) refiriéndose a la validez, afirman que:

> Grado en que un instrumento refleja un dominio especifico de contenido de lo que se mide. El dominio de contenido de una variable normalmente está definido o establecido por la literatura (teoría y trabajos antecedentes). En indagaciones exploratorias en las que las fuentes previas son escasas, el investigador empieza a adentrarse al problema de estudio y a proponer cómo puede estar constituido tal dominio. De cualquier manera, en cada investigación uno debe probar que el instrumento utilizado es válido. (p.201)

La consistencia de los resultados de una investigación representan un valor científico, los instrumentos de medición deben ser confiables y válidos, por ese motivo, para obtener la validez de los instrumentos antes de aplicarlos se sometieron a un proceso de validación de contenido

En la investigación del presente trabajo se ha realizado el proceso de validación de contenido, en donde se han tenido en cuenta tres aspectos: relevancia, pertinencia y claridad de cada uno de los ítems de los instrumentos.

Tabla 03

Jurados expertos

Experto	**Experto**	**Aplicabilidad**
	Metodólogo	Aplicable
	Temático	Aplicable
	Temático	Aplicable

Los cuestionarios sobre la administración de tecnologías de información y procedimientos de seguridad informática fueron sometidos a criterio de un grupo de Jueces expertos, integrado por profesores: Doctores que laboran en la Escuela de Posgrado de la Universidad Cesar Vallejo, quienes informaron acerca de la aplicabilidad de cada uno de los cuestionarios de la presente investigación. Asimismo, en el proceso de validación de cada uno de los cuestionarios del presente estudio, se tendrá en cuenta para cada ítem, la validez de contenido y para tal efecto se consideraran tres aspectos: pertinencia, relevancia y claridad.

Tabla 04

Validez del cuestionario sobre administración de tecnologías de información

Expertos	**Suficiencia del instrumento**	**Aplicabilidad del instrumento**
	Hay Suficiencia	Es aplicable

	Hay Suficiencia	Es aplicable
	Hay Suficiencia	Es aplicable

Tabla 05

Validez del cuestionario sobre procedimientos de seguridad informática

Expertos	**Suficiencia del instrumento**	**Aplicabilidad del instrumento**
	Hay Suficiencia	Es aplicable
	Hay Suficiencia	Es aplicable
	Hay Suficiencia	Es aplicable

Confiabilidad

Hernández, et al (2014) refiriéndose a la confiabilidad, afirman que “Grado en que un instrumento produce resultados consistentes y coherentes” (p.200)

Para establecer la confiabilidad de los cuestionarios, se aplicó la prueba estadística de fiabilidad Alfa de Crombach, a un piloto de 20 profesionales en tecnologías de información del Banco de la Nación que no participaron en la muestra. Luego se procesaran los datos, haciendo uso del Programa Estadístico SPSS versión 21.0.Los instrumentos han sido medidos con escala ordinal o politómica, esta estadística está reservada para este tipo de escala.

Tabla 06

Interpretación del coeficiente de confiabilidad

Rangos	Magnitud
0,81 a 1,00	Muy Alta
0,61 a 0,80	Moderada
0,41 a 0,60	Baja

0,01 a 0,20	Muy baja

Fuente: Ruíz (2007).

Como podemos observar, la tabla 06 nos permite analizar los resultados de la prueba Alfa de Crombach para cada una de las variables en estudio y sus correspondientes dimensiones.

Tabla 07

Resultados del análisis de confiabilidad del instrumento que mide la variable administración de tecnologías de información

Dimensión/variable	**Alfa de Crombach**	**N° de ítems**
Gestión de servicios de tecnologías de información y procesos	0,668	6
Funcionalidad y garantía	0,884	8
Recursos y capacidades	0,793	6
Activos de servicio		
Cultura	0,889	10
	0.924	6
Administración de tecnologías de información	**0,965**	**36**

Como se observa en la tabla 07, se muestra los resultados del análisis de confiabilidad de la variable administración de tecnologías de información. Las dimensiones gestión de servicios de tecnologías de información y procesos y recursos y capacidades, presentan confiabilidad moderada. Asimismo podemos observar que las dimensiones: Funcionalidad y garantía, activos de servicio, cultura y la variable administración de tecnologías de información, tienen confiabilidad muy alta.

Por lo tanto el instrumento que mide la variable administración de tecnologías de información, es confiable.

Tabla 08

Resultado de análisis de confiabilidad del instrumento que mide la variable procedimientos de seguridad informática

Dimensión / variable	**Alfa de Crombach**	**N° de ítems**
Seguridad de la información	0,856	8
Confidencialidad	0,766	8
Integridad	0,730	4
Disponibilidad	0,702	8
Procedimientos de seguridad Informática	**0,924**	**28**

Como se observa en la tabla 08, se muestra los resultados del análisis de confiabilidad de la variable procedimientos de seguridad informática. Las dimensiones confidencialidad, integridad y disponibilidad, presentan confiabilidad moderada. Asimismo podemos observar que la dimensión seguridad de la información y la variable procedimientos de seguridad informática, tienen confiabilidad muy alta.

Por lo tanto el instrumento que mide la variable procedimientos de seguridad informática, es confiable

Procedimientos de recolección de datos:

Se realizó un estudio piloto con la finalidad de determinar la confiabilidad de los instrumentos, en 20 profesionales en tecnologías de información del Banco de la Nación con las mismas características de la muestra de estudio, quienes fueron seleccionados al azar y a quienes se les aplicaron los cuestionarios con escala tipo Likert sobre las variables administración de tecnologías de información y los procedimientos de seguridad informática.

La confiabilidad de los instrumentos a partir de la muestra piloto, se estableció por dimensiones y por variables, cuyos resultados han sido mostrado e interpretados en las tablas 07 Y 08.

Una vez probada la validez y confiabilidad de los instrumentos de estudio, se procedió a aplicarlos a la muestra de 90 trabajadores del Banco de la Nación. Quienes respondieron en un tiempo aproximado de 30 minutos.

Luego, se analizaron los datos obtenidos de la muestra de 110 trabajadores, a través del programa estadístico SPSS versión 21.0 en español. Asimismo los resultados pertinentes al estudio, han sido mostrados mediante tablas y figuras, con su correspondiente interpretación, de acuerdo a los objetivos e hipótesis planteados en la presente investigación.

Para la contrastación de la hipótesis general, e hipótesis específicas y teniendo en cuenta que los datos de las dos variables son ordinales, se ha prescindido del test de normalidad, dado que en este caso no es una condición necesaria. Por consiguiente se procedió a aplicar en cada caso la prueba de regresión logística para establecer su incidencia entre las variables y dimensiones en estudio.

Este estudio tiene como finalidad determinar la incidencia de la variable administración de tecnologías de información en los procedimientos de seguridad informática.

2.8. Método de análisis

La estadística utilizada para la presente investigación fue descriptiva, se emplea procedimientos empleados para organizar y resumir conjuntos de observaciones en forma cuantitativa. La cual va ser representada mediante tablas, gráficos o valores numéricos. Se trabaja con dos variables que permiten estudiar la relación o asociación que existe entre la variable administración de tecnologías de información en los procedimientos de seguridad informática.

La estadística inferencial, se utiliza este método para inferir algo acerca de |una población basándose en los datos obtenidos a partir de una muestra. Los datos estadísticos son cálculos aritméticos realizados sobre los valores obtenidos en una porción de la población, seleccionada según criterios rigurosos. Estadística para probar hipótesis.

Regresión logística ordinal

Aguayo (2012), refiriéndose a regresión logística ordinal afirma que:

> Cuando tengamos una variable dependiente que queramos evaluar la asociación o relación con otra variables independientes. A partir de los coeficientes de regresión de las variables independientes introducidas en el modelo se puede obtener directamente la OR que se obtiene representa la probabilidad del evento. Lo que se pretende mediante la RL es expresar la probabilidad de que ocurra el evento en cuestión como función de ciertas variables, que se presumen relevantes o influyentes. (p. 1)

Para este estudio se realiza la presentación de los coeficientes de la regresión logística ordinal de la administración de tecnologías de información incide en los procedimientos de seguridad informática.

Burgueñoa, García- Bastosb y González (1995), refiriéndose a regresión logística ordinal afirma que:

> La curva ROC es un gráfico en el que se observan todos los pares sensibilidad especificidad resultantes de la variación continua de los puntos de corte en todo el rango de resultados observados. La mayoría de las curvas ROC caen entre estos dos extremos. Cualitativamente, cuanto más próxima es una curva ROC a la esquina superior izquierda, más alta es la exactitud global de la prueba. De la misma forma, si se dibujan en un mismo gráfico las curvas obtenidas con distintas pruebas diagnósticas, aquella que esté situada más hacia arriba y hacia la izquierda tiene mayor exactitud: por simple observación se obtiene una comparación cualitativa. Ya se ha comentado que la variabilidad del muestreo puede dar lugar a distintos valores de sensibilidad y especificidad. (p. 663)

En el caso de estudio que se muestra en este trabajo se presenta los coeficientes de la regresión logística ordinal de la administración de tecnologías de información incide en la seguridad de la información, también presenta los coeficientes de la regresión logística ordinal de la administración de tecnologías de información incide en la confidencialidad. Asimismo, presenta los coeficientes de la regresión logística ordinal la administración de tecnologías de información incide en la integridad del Banco de la Nación y presenta los coeficientes de la regresión logística ordinal de administración de tecnologías de información influye en la disponibilidad del Banco de la Nación

Heredia, Rodríguez y Vivalta (2012), refiriéndose a regresión logística ordinal afirma que:

> La regresión logística ha tenido un extendido uso por su capacidad para tratar variables independientes tanto numéricas como categóricas, y por la utilidad de la información que se deriva del análisis del denominado “odds ratio”. Los modelos logísticos son adecuados para situaciones donde se quiere explicar la probabilidad “p” de ocurrencia de un evento de interés por medio de los valores de ciertas variables independientes o explicativas McCullagh (1980) plantea que la unión con Logit es más adecuada para analizar datos ordinales cuya distribución de frecuencia es uniforme a lo largo de todas las categorías. (p. 252)

En el caso de estudio que se muestra en este trabajo si los valores de la variable ordinal representan la administración de las tecnologías de información incide en los procedimientos de seguridad informática son como de media a alta, por ende es posible considerar la unión logit como la más satisfactoria para este caso.

2.9. Aspectos éticos

Este trabajo de investigación ha cumplido con los criterios establecidos por el diseño de investigación cuantitativa de la Universidad César Vallejo, el cual sugiere a través de su formato el camino a seguir en el proceso de investigación. Asimismo, se ha cumplido con respetar la autoría de la información bibliográfica, por ello se hace referencia de los autores con sus respectivos datos de editorial y la parte ética que éste conlleva.

Las interpretaciones de las citas corresponden al autor de la tesis, teniendo en cuenta el concepto de autoría y los criterios existentes para denominar a una persona “autor” de un artículo científico. Además de precisar la autoría de los instrumentos diseñados para el recojo de información, así como el proceso de revisión por juicio de expertos para validar instrumentos de investigación, por el cual pasan todas las investigaciones para su validación antes de ser aplicadas.

III. RESULTADOS

3.1 Descripción de resultados

3.1.1 Descripción de la variable administración de tecnologías de información

Tabla 09

Niveles de la administración de tecnologías de información del Banco de la Nación

Niveles	Frecuencia	Porcentaje
Malo	0	0,0
Regular	38	34,5
Bueno	72	65,5
Total	110	100,0

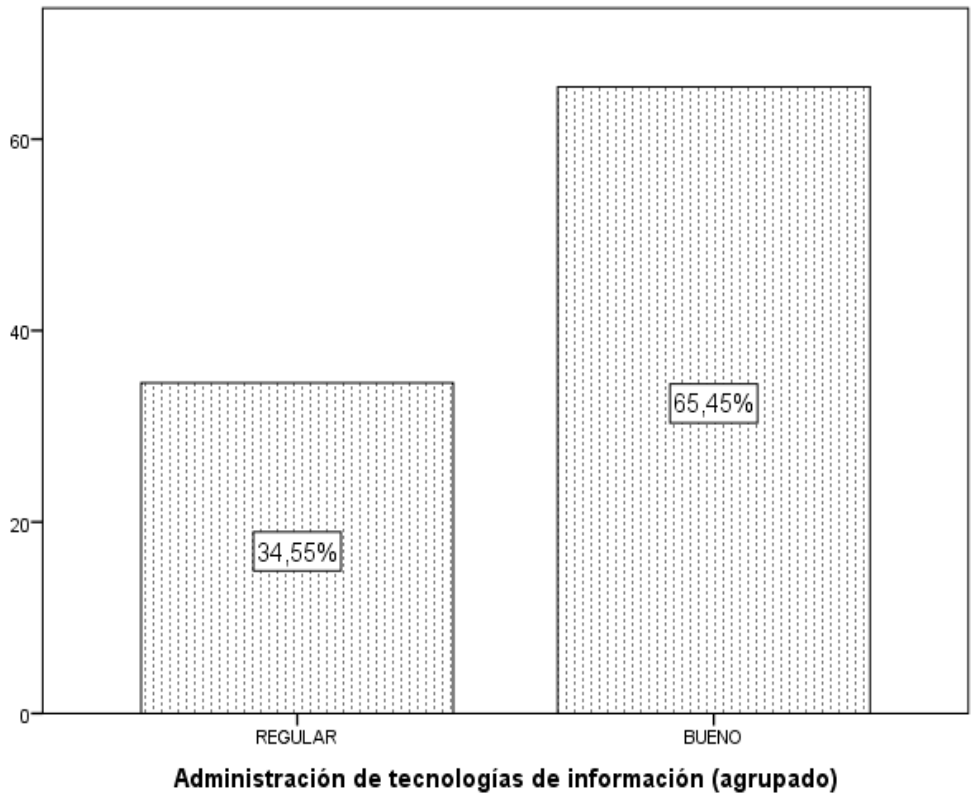


Figura 1. Niveles de frecuencias de la administración de tecnologías de información del Banco de la Nación

En cuanto al resultado que se muestran por niveles de la administración de tecnologías de información del Banco de la Nación, donde se aprecia que el 34.55% de los encuestados manifiestan que el nivel de la administración tecnológica es regular, mientras que el 65.45% perciben que el nivel de la administración tecnológica es bueno en el Banco de la Nación

De los resultados se tiene que la predominancia en cuanto al nivel de la administración de tecnologías de información del Banco de la Nación es buena.

Tabla 10

Niveles de los procedimientos de seguridad informática del Banco de la Nación

Niveles	Frecuencia	Porcentaje
Bajo	1	,9
Moderado	23	20,9
Alto	86	78,2
Total	110	100,0

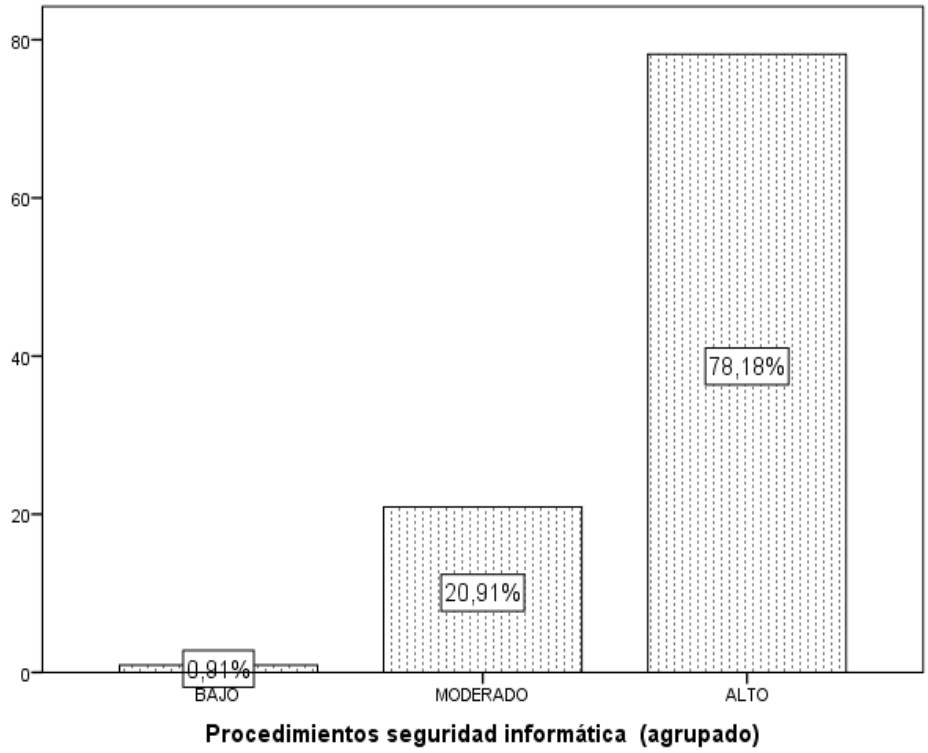


Figura 2. Distribución porcentual de la seguridad informática del Banco de la Nación

Así mismo en cuanto al resultado que a continuación se muestran por niveles de la seguridad informática del Banco de la Nación, se tiene la percepción que el 0.91% de los encuestados, perciben que seguridad informática del Banco de la Nación es bajo, mientras el 78.18% de los encuestados perciben que el

nivel de la seguridad informática del Banco de la nación es alto, implica que la seguridad si es muy adecuado en el Banco de la Nación. De los resultados se tiene que la predominancia en cuanto al nivel de la seguridad informática del Banco de la Nación es alta.

Resultados previos al análisis de los datos

En cuanto a los resultados obtenidos a partir del cuestionario con escala ordinal se asumirá prueba no paramétrica que muestra incidencia entre la variable independiente frente a la variable dependiente posteriores a la prueba de hipótesis se basaran a la prueba de regresión logística, ya que los datos para el modelamiento son de carácter cualitativo ordinal, orientando al modelo de regresión logística ordinal, para el efecto asumiremos el reporte del SPSS.

Tabla 11

Determinación del ajuste de los datos para el modelo de la administración de tecnologías de información en los procedimientos de seguridad informática del banco de la nación

Información de ajuste de los modelos

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	36,352			
Final	9,731	26,620	1	,000

Función de enlace: Logit.

En cuanto al reporte del programa a partir de los datos, se tienen los siguientes resultados donde los datos obtenidos estarían explicando la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, los resultado de la tabla de

acuerdo al Chi cuadrado es de 26.62 y p-valor (valor de la significación) es igual a 0.000, frente a la significación estadística α = 0.05 (p-valor < α), significa que los datos obtenidos se presta para la mostrar la incidencia de las variables de estudio.

Tabla 12

Determinación de las variables para el modelo de regresión logística ordinal

Bondad de ajuste

	Chi-cuadrado	gl	Sig.
Pearson	,149	1	,700
Desvianza	,274	1	,601

Función de enlace: Logit.

Así mismo se muestran los resultados de la bondad de ajuste de la variable el cual se rechaza la hipótesis nula; por lo que con los datos de la variable es posible mostrar la incidencia gracias a las variables y el modelo presentado estaría dado por el valor estadística de p -valor = 0.700 frente al α = 0.05. Por tanto el modelo y los resultados están explicando la incidencia de una variable sobre la otra.

Tabla 13

Presentación de los coeficientes de la regresión logística ordinal de la administración de tecnologías de información incide en los procedimientos de seguridad informática

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[nproced = 1]	-6,349	1,107	32,912	1	,000	-8,518	-4,180
	[nproced = 2]	-2,597	,464	31,336	1	,000	-3,506	-1,688
Ubicación	[adm_tic=2]	-2,604	,566	21,183	1	,000	-3,713	-1,495
	[adm_tic =3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados representan los coeficientes de la expresión de la regresión con respecto a la administración de tecnologías de información incide en los procedimientos de seguridad informática, se presentarán las comparaciones entre el nivel de la administración de tecnologías de información comparando entre el nivel alto de los procedimientos de seguridad, de los cuales se tienen al exp(-

2.604) = 0.07398, representando a la tasa de solo el 7.397% de los que perciben que el nivel de la administración de la tecnología es de la información es bueno, se debe a que los procedimientos de seguridad es alto en el Banco de la Nación, siendo esta afirmación asertiva en cuanto al valor de p = 0.000 < 0.05 de significación estadística.

3.2 Contrastación de hipótesis

Hipótesis general

H_o: La administración de tecnologías de información no incide en los procedimientos de seguridad informática del Banco de la Nación, 2016.

H_1: La administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016.

Regla de decisión:

Si p – valor < 0.05, rechazar H_0

Si p – valor > 0.05, aceptar H_0

Tabla 14

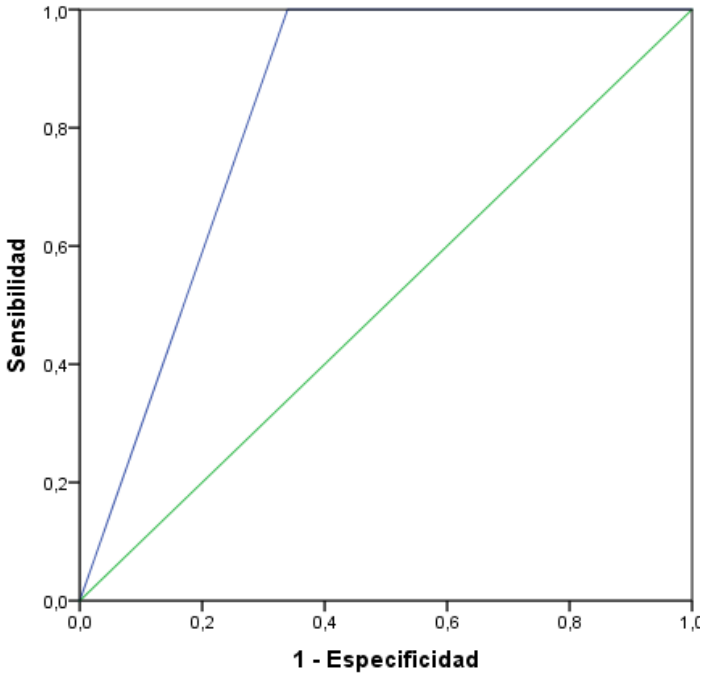
Pseudo coeficiente de determinación de las variables.

	Pseudo R-cuadrado

	Cox y Snell	Nagelkerke	McFadden.
resultado	,215	,318	,215

Función de vínculo: Logit.

En referencia, se tiene los pseudo R - cuadrado, lo que se estarían presentando es la incidencia porcentual de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación. El cual se tiene el resultado de Cox y Snell igual a 0.215, significaría que la seguridad informática del Banco de la Nación se debe al 21.5% la administración de tecnologías de información, sin embargo la dependencia más estable es el coeficiente de Nagalkerke, el cual se tiene que la seguridad informática del Banco de la Nación se debe al 31.8% la administración de tecnologías de información



Los segmentos de diagonal se generan mediante empates.

Área 0.830

Figura 3. Representación del área COR como incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática.

A consecuencia de lo explicado, se tiene el área representado por los datos incidencia de la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, el cual se muestra el reporte del mismo con 83.0% de área bajo la curva COR; implica que la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016.

La administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016.

Tabla 15

Presentación de los coeficientes de la regresión logística ordinaria de la administración de tecnologías de información incide en la seguridad de la información

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[Seguri = 1]	-7,527	1,245	36,548	1	,000	-9,968	-5,087
	[Seguri = 2]	-3,556	,717	24,574	1	,000	-4,962	-2,150
Ubicación	[adm_tic=2]	-3,877	,789	24,150	1	,000	-5,423	-2,331
	[adm_tic =3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados representan los coeficientes de la expresión de la regresión con respecto a la administración de tecnologías de información incide en la seguridad de la información, se presentarán las comparaciones entre el nivel de la administración de tecnología de información en comparación entre el nivel alto de la seguridad de la información, de los cuales se tienen al exp(-3.877) = 0.0207 representando a la tasa de solo el 2.07% de los que perciben que el nivel de la administración de la tecnología de información es bueno se debe a que la seguridad de la información es alto en el banco de la Nación, siendo esta afirmación asertiva en cuanto al valor de p = 0.000 < 0.05 de significación estadística.

Hipótesis especifica 1

H_o: La administración de tecnologías de información no incide en la seguridad de la información del Banco de la Nación, 2016.

H_1: La administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016.

Regla de decisión:

Si p – valor < 0.05, rechazar H_0

Si p – valor > 0.05, aceptar H_0

Tabla 16

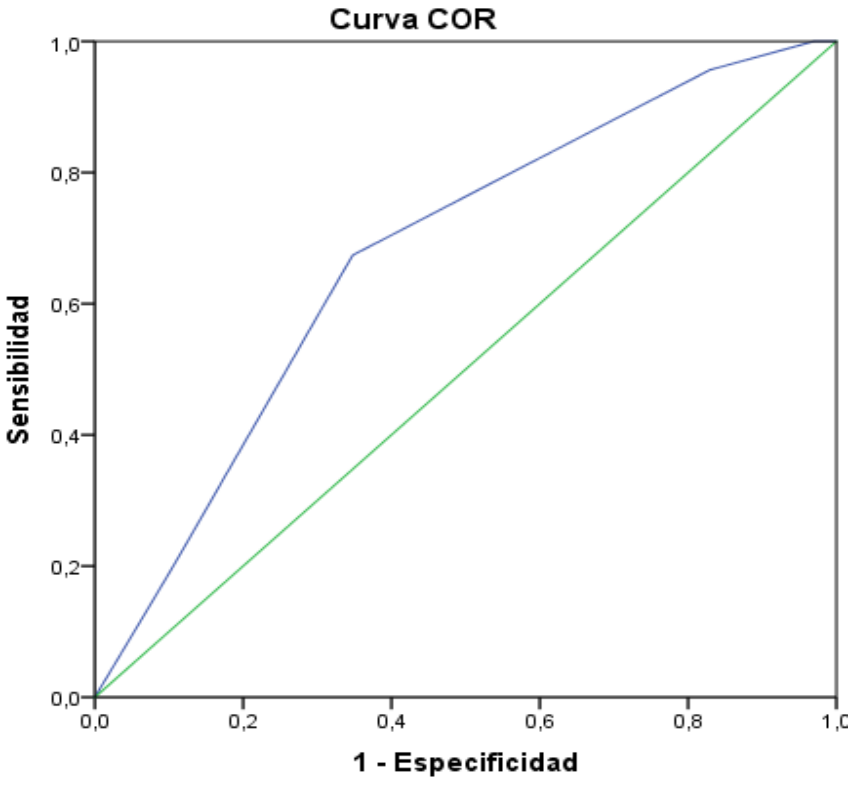
Pseudo coeficiente de determinación de las variables.

Pseudo R-cuadrado		
Cox y Snell	Nagelkerke	McFadden.

Resultado	,339	,502	,368

Función de vínculo: Logit.

En referencia, se tiene los pseudo R cuadrado, lo que se estaría presentando la incidencia porcentual de la administración de tecnologías de información en la seguridad de la información del Banco de la Nación. El cual se tiene el resultado de Cox y Snell igual a 0.339 significaría que la seguridad de la información del Banco de la Nación se debe al 33.9% la administración de tecnologías de información, sin embargo la dependencia más estable es el coeficiente de Nagalkerke, el cual se tiene que en la seguridad de la información del Banco de la Nación se debe al 50,2% la administración de tecnologías de información.



Los segmentos de diagonal se generan mediante empates.

Área 0.677

Figura 4. Representación del área COR de la administración de tecnologías de información en la seguridad de la información del Banco de la Nación

A consecuencia de lo explicado, se tiene el área representado por los datos incidencia de la administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, el cual se muestra el reporte del mismo con 67.7% de área bajo la curva COR; el cual la administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016.

La administración de tecnologías de información inciden en la confidencialidad del Banco de la Nación, 2016.

Tabla 17

Presentación de los coeficientes de la regresión logística ordinaria de la administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[nproced = 1]	-7,602	1,202	40,013	1	,000	-9,958	-5,247
	[nproced = 2]	-3,259	,588	30,662	1	,000	-4,412	-2,105

Ubicación	[adm_tic=2]	-4,229	,720	34,482	1	,000	-5,640	-2,817
	[adm_tic =3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados representan los coeficientes de la expresión de la regresión con respecto a la administración de tecnologías de información incide en la confidencialidad, se presentarán las comparaciones entre el nivel de la administración de tecnologías de información en comparación entre el nivel alto de la confidencialidad, de los cuales se tienen al exp(-4.229) = 0.0145 representando a la tasa de solo el 1.44% de los que perciben que el nivel de la administración de la tecnología de información es bueno se debe a que la confidencialidad es alto en el Banco de la Nación, siendo esta afirmación asertiva en cuanto al valor de p = 0.000 < 0.05 de significación estadística.

Hipótesis específica 2

H_o: La administración de tecnologías de información no incide en la confidencialidad del Banco de la Nación, 2016.

H_1: La administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016.

Regla de decisión:

Si p – valor < 0.05, rechazar H_0

Si p – valor > 0.05, aceptar H_0

Tabla 18

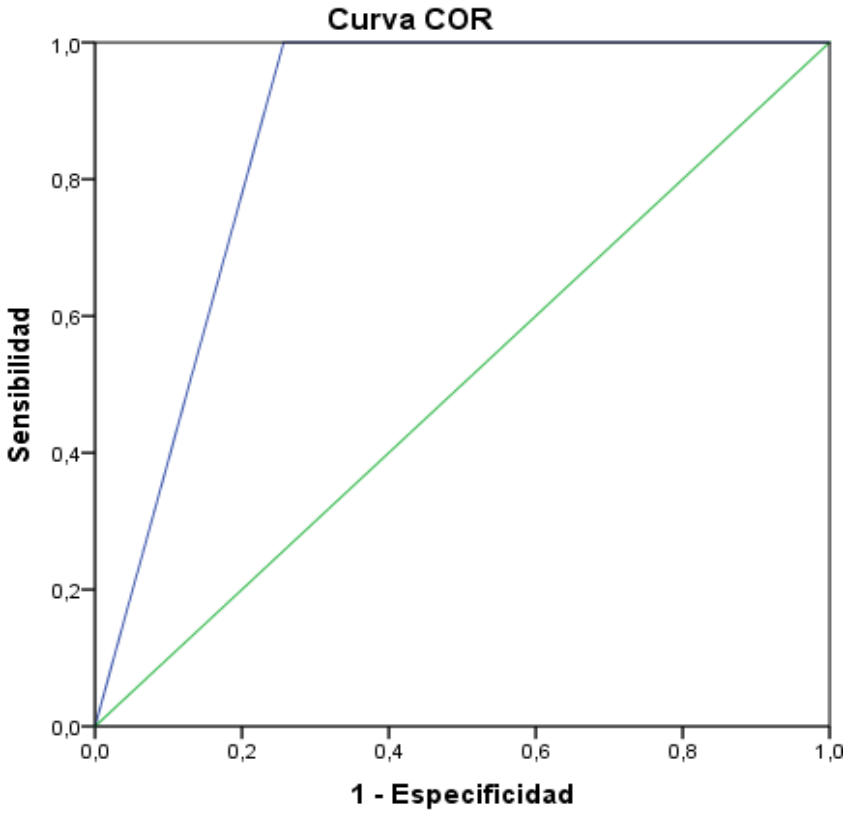
Pseudo coeficiente de determinación de las variables.

Pseudo R-cuadrado

	Cox y Snell	Nagelkerke	McFadden.
Resultado	,398	,589	,451

Función de vínculo: Logit.

En referencia, se tiene los pseudo R cuadrado, lo que se estarían presentando es la dependencia porcentual de la administración de tecnologías de información en la confidencialidad del Banco de la Nación. El cual se tiene el resultado de Cox y Snell igual a 0.398 significaría que la confidencialidad del Banco de la Nación se debe al 39.8% de la administración de tecnologías de información, sin embargo la dependencia más estable es el coeficiente de Nagalkerke, el cual se tiene la confidencialidad del Banco de la Nación se debe al 58.9% la administración de tecnologías de información.



Los segmentos de diagonal se generan mediante empates.

Área 0.872

Figura 5. Representación del área COR de la administración de tecnologías de información incide en la confidencialidad del Banco

A consecuencia de lo explicado, se tiene el área representado por los datos incidencia de tecnologías de información incide en la confidencialidad del Banco de la Nación, el cual se muestra el reporte del mismo con 87.2% de área bajo la curva COR; por lo que la administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016.

La administración de tecnologías de información incide en la integridad del Banco de la Nación, 2016.

Tabla 19

Presentación de los coeficientes de la regresión logística ordinaria la administración de tecnologías de información incide en la integridad del Banco de la Nación, 2016.

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[nproced = 1]	-26,239	1,225	458,983	1	,000	-28,639	-23,838

Ubicación	[nproced = 2]	-2,927	,593	24,391	1	,000	-4,088	-1,765
	[adm_tic=2]	-25,546	,000	.	1	.	-25,546	-25,546
	[adm_tic =3]	-2,416	,663	13,263	1	,000	-3,716	-1,116

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados representan los coeficientes de la expresión de la regresión con respecto a la administración de tecnologías de información en la integridad, se presentarán las comparaciones entre el nivel de la tecnología de información en comparación entre el nivel alto de la integridad, de los cuales se tienen al exp(-25.546) = 8.04476E-12 representando una tasa bastante pequeña del nivel de la administración de la tecnología de la información es bueno se debe a que la integridad es alto en el Banco de la Nación, siendo esta afirmación asertiva en cuanto al valor p=0.000<0.05 de significancia estadística.

Hipótesis específica 3

H_o: La administración de tecnologías de información incide en la integridad del Banco de la Nación, 2016.

H_1: La administración de tecnologías de información incide en la integridad del Banco de la Nación, 2016.

Regla de decisión:

Si p – valor < 0.05, rechazar H_0

Si p – valor $>$ 0.05, aceptar H_0

Tabla 20

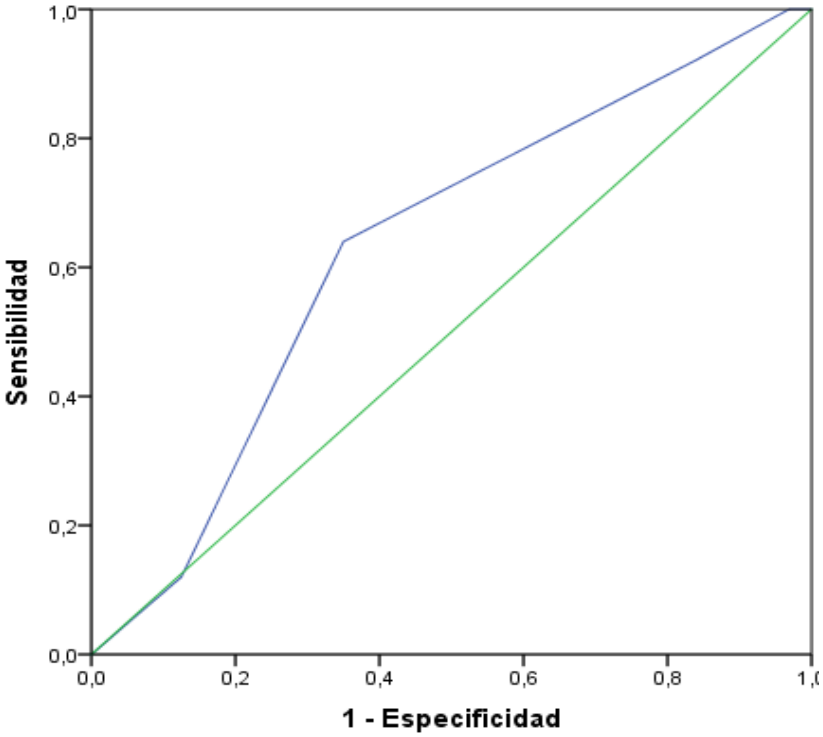
Pseudo coeficiente de determinación de las variables.

Pseudo R-cuadrado

	Cox y Snell	Nagelkerke	McFadden.
Resultado	,257	,381	,264

Función de vínculo: Logit.

En referencia, se tiene los pseudo R cuadrado, lo que se estarían presentando es la dependencia porcentual de la administración de tecnologías de información en la integridad del Banco de la Nación. El cual se tiene el resultado de Cox y Snell igual a 0.257 significaría que la integridad del Banco de la Nación se debe al 25.7% de la administración de tecnologías de información, sin embargo la dependencia más estable es el coeficiente de Nagalkerke, el cual se tiene a la integridad del Banco de la Nación se debe al 38.1% la administración de tecnologías de información



Los segmentos de diagonal se generan mediante empates.

Área 0.631

Figura 6. Representación del área COR La administración de tecnologías de información incide en la Integridad

Así mismo a consecuencia de lo explicado, se tiene el área representado por los datos incidencia de tecnologías de información incide en la integridad del Banco de la Nación, el cual se muestra el reporte del mismo con 63.1% de área bajo la curva COR; por lo que la administración de tecnologías de información incide en la Integridad del Banco de la Nación, 2016.

La administración de tecnologías de información incide en la disponibilidad del Banco de la Nación, 2016.

Tabla 21

Presentación de los coeficientes de la regresión logística ordinaria de administración de tecnologías de información incide en la disponibilidad del Banco de la Nación

Estimaciones de parámetro

							Intervalo de confianza al 95%	
		Estimación	Error estándar	Wald	gl	Sig.	Límite inferior	Límite superior
Umbral	[NDISPON = 1]	-23,772	1,013	550,239	1	,000	-25,758	-21,786
	[NDISPON = 2]	-22,618	,602	1413,542	1	,000	-23,797	-21,439
Ubicación	[adm_tic=2]	-20,161	,000	.	1	.	-20,161	-20,161

[adm_tic =3]	0[a]	.	.	0	.	.	.

Función de enlace: Logit.

a. Este parámetro está establecido en cero porque es redundante.

Los resultados representan los coeficientes de la expresión de la regresión con respecto a la administración de tecnologías de información en la disponibilidad, se presentarán las comparaciones entre el nivel de la tecnología de información en comparación entre el nivel alto de la disponibilidad, de los cuales se tienen al exp(-20.161) = 1.7546E-09 representando a la tasa bastante pequeña de los que perciben que el nivel de la administración de la tecnologías de la información es bueno se debe a que la disponibilidad es alto en el Banco de la Nación, siendo esta afirmación asertiva en cuanto al valor p=0.000<0.05 de significancia estadística.

Hipótesis específica 4

H_o: La administración de tecnologías de información no incide en la disponibilidad del Banco de la Nación, 2016.

H_1: La administración de tecnologías de información incide en la disponibilidad del Banco de la Nación, 2016.

Tabla 22

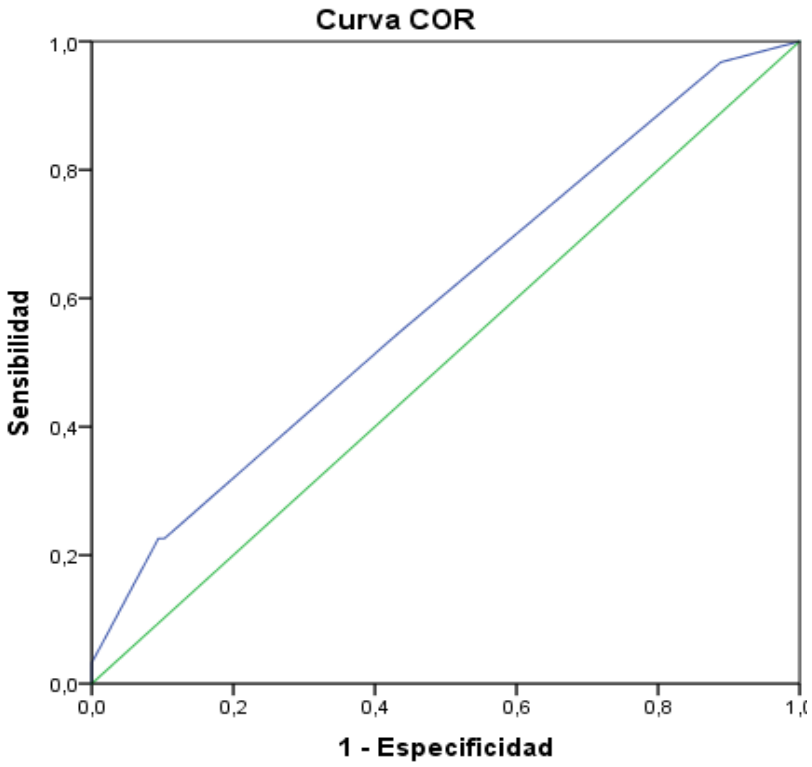
Pseudo coeficiente de determinación de las variables.

Pseudo R-cuadrado		
Cox y Snell	Nagelkerke	McFadden.

resultado	,184	,273	,181

Función de vínculo: Logit.

Finalmente, en referencia, se tiene los pseudo R cuadrado, lo que se estarían presentando es la dependencia porcentual de la administración de tecnologías de información en la disponibilidad del Banco de la Nación. El cual se tiene el resultado de Cox y Snell igual a 0.184 significaría que la disponibilidad del Banco de la Nación se debe al 18.4% de la administración de tecnologías de información, sin embargo la dependencia más estable es el coeficiente de Nagalkerke, el cual se tiene a la disponibilidad del Banco de la Nación se debe al 27.3% la administración de tecnologías de información.



Los segmentos de diagonal se generan mediante empates.

Área 0.596

Figura 7. Representación del área COR del programa de administración de tecnologías de información incide en la disponibilidad.

Finalmente, se tiene el área representado por los datos incidencia de tecnologías de información incide en la integridad del Banco de la Nación, el cual se muestra el reporte del mismo con 59.6% de área bajo la curva COR; la administración de tecnologías de información incide en la disponibilidad del Banco de la Nación, 2016.

IV DISCUSIÓN

4.1 Discusión de resultados

En el presente estudio se ha realizado el análisis estadístico regresión logística ordinal en el sentido que la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016.

Con referencia a la hipótesis general, los resultados indican que, a consecuencia de lo explicado, se tiene el área representado por los datos incidencia de la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, el cual se muestra el reporte del mismo con 83.0% de área bajo la curva COR; implica que la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016. Un resultado similar fue el de Barrionuevo y Ortiz (2015), los mismos que afirmaron que las instituciones financieras públicas tienen modelos de “Gestión de Servicios de TI” similares; y por consiguiente, es factible concebir un modelo estándar, que pueda ser aplicado en cualquiera de las entidades, el mismo que permita cumplir de una manera más eficiente las normativas establecidas por los organismos de supervisión y control, para las entidades financieras públicas, que existe duplicidad en los requerimientos entre las diferentes normativas; lo cual, es ineficiente ya que implica trabajo adicional, desperdicio de recursos (humanos, financieros y técnicos), duplicidad de esfuerzos durante los procesos de auditorías; y dificultad para implementar un modelo de “Gestión de Servicios de TI” estándar para dar cumplimiento a las exigencias de dichas normativas, del análisis realizado a los estándares y mejores prácticas de la industria, se determinó que para dar cumplimiento a los requerimientos de las normativas establecidas por los organismos de supervisión y control, se puede adoptar estándares de la industria; tales como: ITIL v3 (2011);Y, COBIT5 ; por tal motivo, resulta práctico determinar un modelo genérico, basado en esos estándares, el mismo que será aplicable a todas las empresas financieras públicas, y una adecuada taxonomía para los requerimientos de las normativas, así como para los procesos de los estándares y

mejores prácticas utilizados, permitirá generar un modelo más preciso y fácil de gestionar; logrando de esta manera incorporar al modelo características para mejora continua. Cobit es un framework un marco de negocio para el gobierno y la gestión de la TI de la empresa, que sirve para crear valor optimo desde las Tecnologías de información, satisfacer las necesidades de los Stakeholder: Internos (empleados, Gerentes y propietarios) y Externos (proveedores, sociedad, gobierno, acreedores, clientes), optimización de recursos, reducir los riesgos, obtener beneficios. Abarca a toda la empresa desde el principio a fin Gobierno Corporativo de TI. Uno de los principios es de separar el gobierno de la administración, El gobierno evalúa, dirige emite las directivas la gestión, planifica, construye, opera y monitorea lo que se resume en un modelo de referencia de procesos. Y habilitar un enfoque holístico. Lo que impulsa a utilizar este marco de trabajo es porque es un marco de negocio de las TI para que la gerencia conecte los requerimientos de control con los aspectos técnicos y riesgos de negocio, permite el desarrollo de políticas y buenas prácticas para el control de las TI en toda la empresa, cumplimiento regulatorio, ayuda a incrementar su valor a través de las tecnologías de información y permite su alineamiento con los objetivos del Negocio y permite enlazar y cuando sea el caso alinearse a otros marcos y estándares del mercado. Es importante mencionar que para implementar Cobit una forma es mapear los Objetivos del Negocio con los Objetivos de los Objetivos de TI y otra forma de implementar es mediante los 5 procesos, enunciar las excepciones mediante el modelo de referencia de procesos. ITIL en las entidades financieras los principales Servicios Corporativos de tecnologías de información comunes son: brindar servicios de alta disponibilidad con los principales aplicativos del “Core” del negocio asegurando la confiabilidad, integridad, los servicios de telefonía, redes y comunicaciones, soporte técnico, gestión de garantías de los equipos y servicios contratados a proveedores. Para aplicar el conocimiento y técnicas en los libros de ITIL: Estrategia, diseño, transición, operación y mejora continua a la producción y entrega de los servicios corporativos de tecnologías de información que brinda el área de informática, se debería tener en consideración de una buena estrategia tercer izar, la operación de los procesos que soportan la producción y prestación de servicios corporativos de TI, manteniendo la propiedad y administración de los mismos a cargo de funcionarios del propio banco bajo los roles y responsabilidades que establece

ITIL, para que garanticen el control y monitoreo de los procesos. La solicitud de los requerimientos de tecnologías de información debe ser canalizado a través de una mesa de ayuda, para ello es imprescindible contar con un catálogo de servicios. Contar con acuerdos de niveles de Servicio (SLAs) y que están reflejados en indicadores que miden la gestión de incidentes, firmar contratos los proveedores con las penalidades correspondientes. Es importante realizar encuestas de satisfacción de servicio a los usuarios atendidos. También es necesario establecer acuerdos de niveles operativos de servicios (OLAs) con las áreas involucradas en los servicios. El personal involucrado debe necesariamente contar con certificación ITIL en los diferentes niveles de acuerdo al rol que desempeñe. ITIL es el mejor lineamiento para brindar servicios de calidad que involucra un cambio cultural muy importante orientado a la gestión por resultados. La alta dirección de una empresa debe evaluar los beneficios de incorporar el marco ITIL en la gestión de servicios de Tecnologías de información. La taxonomía es como complemento de las noemas que indica su clasificación y la relación entre conceptos.

Otro resultado fue el Marchand (2013) quién afirmó conocer los lineamientos estratégicos de acuerdo a un Plan Estratégico Institucional, su relación con el soporte de TIC y la importancia estratégica de estos servicios de soporte. Conocer normas, estándares, buenas prácticas y metodologías relacionadas con la gestión estratégica de TIC es una organización. Conocer acerca del modelo de Balanced ScoreCard, procedimientos, herramientas y su utilidad para la gestión estratégica de TI. Desarrollar las fases de una metodología de implantación del modelo de Balanced ScoreCard (BSC) para la gestión estratégica de TI, y su validación aplicando al caso de estudio de la Universidad Nacional Agraria de la Selva. El objetivo del Balanced Scorecard es la creación de Valor para clientes, accionistas y empleados, llamada la trilogía del valor. En su inicio era solo medir los resultados tangibles e intangibles de una empresa, ahora es una herramienta de Implantación estratégica integral sirve para gestionar y en esta nueva era de la información y crea valor para los accionistas, clientes y empleados. Las empresas de la era de la información tendrán éxito si invierten en sus activos y los gestionan. La innovación y mejora de productos, servicios y

procesos será generada por empleados preparados, con tecnologías de la información y procedimientos, proporciona observar la tendencia y la evolución de los indicadores de la organización que permitirá anticipar y tomar decisiones estratégicas de manera óptima. Ahora, las organizaciones están compitiendo en ambientes complejos y es vital que tengan una exacta comprensión de sus objetivos y de los las estrategias a utilizar para alcanzarlos. Los indicadores financieros tienen el historial de hechos y acontecimientos pasados, Los objetivos e indicadores de BSC se derivan de la visión y estrategia de una organización; y contemplan la actuación de la organización desde las cuatro perspectivas la financiera, la del cliente, la de los procesos internos, aprendizaje y crecimiento. Se puede producir buenos resultados con limitados recursos que es una constante en las organizaciones. Los principios del BSC es convertir la estrategia a términos operativos, es decir no aplicarla si no de comprender, describirla, alinear la organización con estrategias para evitar los silos funcionales y tener objetivos en común, hacer que la estrategia sea el trabajo diario de todo el mundo, los empleados deben conocer los objetivos de la organización y BSC está orientado a trabajar en la comunicación y la formación de los objetivos personales se alinean a los objetivos de la organización. La estrategia un proceso continuo y movilizar el cambio a través del liderazgo directivo, donde la estrategia debe ser liderada por la alta dirección y participar activamente, reconocer que no es solo medir si no que es proyecto de cambio.

También Horna (2016), afirmó Elaborar propuestas de mejora de procesos según las mejoras prácticas e Implementar el piloto con las propuestas de mejora y realizar las evaluaciones correspondientes. El estándar se adaptada a las necesidades de cualquiera organización y se basa en dos principios fundamentales: Modularidad, acoplamiento de los procesos y la responsabilidad para cada proceso. Los procesos se clasifican en tres tipos: Procesos principales, procesos de soporte y procesos de la organización. El ciclo de vida del software describe el desarrollo de software, desde la fase inicial hasta la fase final. El propósito de este estándar es definir las distintas fases intermedias que se requieren para validar el desarrollo de la aplicación, es decir, para garantizar que el software cumpla los requisitos para la aplicación y verificación de los

procedimientos de desarrollo. El ciclo de vida permite que los errores se detecten y permite a los desarrolladores concentrarse en la calidad del software, en los plazos y en los costos asociados. Consta de los siguientes procedimientos entre otros definición de objetivos, análisis de los requisitos, diseño general, diseño en detalle, programación, prueba unitaria, integración, prueba de validación, documentación, implementación y mantenimiento. El modelo en cascada es una secuencia de fases donde al final de cada una de ellas se reúne la documentación para garantizar que cumple las especificaciones y los requisitos antes de pasar a la fase siguiente y el modelo V los procedimientos a probar ya deben haberse creado en la fase de diseño. Asimismo, Implementar el piloto con las propuestas de mejora y realizar las evaluaciones correspondientes, las pruebas piloto tiene por objetivo asegurar las condiciones apropiadas para la definición del diseño. Los componentes y las fases mínimas para el desarrollo de las pruebas piloto de un programa es que la responsabilidad por prueba estará a cargo de un coordinador de equipo con capacidad de convocatoria para el buen desempeño de la prueba. El desarrollo de toda prueba piloto requiere de un acta donde estén descritos los acuerdos generales.

Asimismo, estos resultados coinciden con los que sostiene teóricamente la a Norma internacional ISO/IEC 27001 (2013), refiriéndose a los procedimientos de seguridad informática que los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable. Los directivos luego de aprobar los procedimientos de seguridad informática, están en la obligación de programar periódicamente auditorías internas con el objetivo de velar el cumplimiento de las políticas de seguridad y del resultado obtenido de las mismas , priorizar las recomendaciones críticas e importantes para implementarlas definiendo planes de trabajo con plazos establecidos , Es importante informar las acciones a tomar a la gerencia de auditoria interna de las acciones que se han tomado con el objetivo de implementar lo recomendado por la auditoria.

Con respecto a la primera hipótesis específica, los resultados indican que a consecuencia de lo explicado, se tiene el área representado por los datos incidencia de la administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, el cual se muestra el reporte del mismo con 67.7% de área bajo la curva COR; el cual la administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016.Un resultado similar fue el de Gallegos y Murillo (2015), los mismos que afirmaron que el fraude en la industria de las telecomunicaciones y el estudio exploratorio de la gestión de la seguridad de la información en las empresas del Ecuador, se determina que las empresas por fraude a nivel mundial ascienden al 10% de su rentabilidad y en el Ecuador no es la excepción, debido a que las telecomunicaciones ecuatorianas carecen de una estrategia de gestión de seguridad de la información a nivel de toda la organización y se confunde la gestión de la seguridad de la información con el concepto de seguridad informática, y el resultado del proceso de selección de estándares y buenas prácticas realizado, que determinó la utilización de eTOM v12, COBIT 5 e ISO/IEC 27011 para el desarrollo de la metodología de gestión de seguridad de la información, fue exitoso, ya que existe una integración formal, específicamente entre COBIT 5 y la ISO/IEC 27002, que constituye la parte neurálgica y un sólido soporte conceptual para la metodología, de donde se desprenden las guías de implementación de procesos de la gestión de la seguridad de la información, contextualizadas a los procesos de las telecomunicaciones, para cubrir sus principales necesidades. La ISO 27011 aborda las directrices de gestión de seguridad para las organizaciones de telecomunicaciones basadas en la norma ISO 27002. La norma facilita controles y una orientación en qué hacer para la implementación en las empresas de telecomunicaciones. Pero no el cómo. Teniendo en cuenta la confidencialidad, disponibilidad e integridad de las infraestructuras y servicios. La información para las empresas de telecomunicaciones es un activo esencial, por eso es necesario tener la seguridad respectiva. La norma ISO27011 nos garantiza la seguridad de la información de las empresas a través de unos controles apropiados. Estos controles han de ser

implementados y auditados periódicamente proteger la integridad, confidencialidad y disponibilidad de las infraestructuras y servicios, asegurar la disminución de los riesgos de los servicios que las empresas de telecomunicaciones prestan, tener la capacidad de hacer que la moralidad de las personas y la confianza de las mismas mejoren. Por eso es fundamental comprender cuáles son los procesos críticos de un modelo de operaciones, para asegurarse que están bajo control. Los procesos que podemos calificar como críticos son aquellos que de alguna forma hacen que nuestro negocio siga funcionando. Los procesos estratégicos son los que hacen que nuestro modelo de negocios exista. Todos los procesos de alguna forma contribuyen al funcionamiento de la operación. Los procesos críticos son aquellos que “no pueden caer”. Los procesos críticos demandan no sólo mayor atención, sino además requieren un mayor nivel de inversión para asegurarse de que no fallen o incluso para evitar que su criticidad golpee a la operación. Es posible que, si se invierte lo suficiente, un determinado proceso deje de ser crítico. Pero nuevamente nos encontramos ante una decisión: cuánto riesgo estamos dispuestos a tolerar y cuánto queremos invertir para reducir ese riesgo. Los no identificados pueden significar una amenaza para el éxito de una auditoría. Es necesario entonces identificar los riesgos y la relación que tienen con los controles existentes. Una buena identificación de los riesgos involucra el examinar todas las fuentes de riesgo y las perspectivas de todos los entes participantes ya sean internos o externos. Las empresas de la Industria de las Telecomunicaciones y Tecnología son vulnerables y están expuestas al fraude. El fraude en redes fijas, los estafadores simplemente se enganchan a la red y adjuntan un dispositivo que les permite obtener el servicio. El servicio es facturado como cualquier servicio legítimo al propietario de la línea. Los estafadores comprendieron que las cabinas telefónicas funcionaban cuando las monedas eran insertadas y así se idearon un modo de hacer sus llamadas sin gastar el dinero. Era fácil inventar una técnica simple que permita depositar temporalmente monedas en el teléfono y luego recuperar las monedas después de que la llamada era colgada. Los estafadores ataban una cuerda o un cable a una moneda, depositaban la moneda, y después que la llamada era colgada daban un tirón y la moneda era recuperada. Gradualmente, los teléfonos que utilizaban monedas fueron diseñados de tal manera que tenían caminos de recolección de

monedas más complicados o de dirección única, impidiendo que esto sucediera. El servicio de prepago al principio fue pensado como la solución al fraude de la suscripción, por lo que el operador no se preocupó realmente quién era el cliente, o a donde fueron hechas las llamadas. Sin embargo, se han desarrollado métodos para cometer el fraude en estos servicios. El fraude de suscripción es utilizado por personas que no tienen el suficiente conocimiento técnico para incursionar en fraude de otro tipo, y funciona tanto en redes alámbricas como inalámbricas. Con la explosión de nuevos proveedores de servicio y revendedores de larga distancia, han aparecido proveedores de servicio ilegítimos y los revendedores de llamadas encuentran métodos de añadir sus gastos a una factura telefónica de suscriptores reales. La segunda, el fraude en redes inalámbricas ha empezado a ser mejor entendida y manejada recientemente. La estrategia de Gobierno en línea contribuye con la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC. Facilitar la eficiencia y la relación entre las entidades del Estado, así como con la sociedad. Fortalecer las condiciones para el incremento de la competitividad y el mejoramiento de la calidad de vida, contribuir al incremento de la transparencia en la gestión pública, promover la participación ciudadana haciendo uso de los medios electrónicos. La Estrategia de Gobierno en línea, se han establecido los siguientes elementos estratégicos, que se han organizado desde las dimensiones Cliente, Financiera, Procesos de Aprendizaje y Desarrollo. La comunicación es la forma en que el ser humano se puede comunicar, es un proceso que consta de tres elementos básicos que son el emisor, el medio y el receptor, si deja de existir alguno de estos elementos deja de llamarse comunicación.

Por otra parte, Carbajal (2013), afirmó que aplicar la normativa emitida por la Contraloría General de la República en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos, aplicar la normativa emitida por otras entidades del Estado Peruano en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos. La Contraloría General de la República es el ente rector del Sistema Nacional de Control, con autonomía administrativa, funcional, económica y financiera, cuya

misión es supervisar a las entidades públicas orientando su accionar a la transparencia de la gestión de las entidades. El Sistema Nacional de Control es el conjunto normas, métodos y procedimientos, que ayudan a desarrollar el ejercicio del control gubernamental en forma descentralizada. Su acción comprende todas las actividades administrativo, presupuestal, operativo y financiero de las entidades y alcanza al personal que presta servicios en ellas, independientemente del régimen que las regule. Tenemos como etapas del control al control previo que lo realizan las mismas áreas, concurrente donde puede estar presente el Órgano de Control Interno como veedor y posterior que lo realiza el órgano de control interno, la Contraloría o las Sociedades de Auditoría. El control interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúe correcta y eficientemente. Los titulares y funcionarios de las instituciones públicas sestan en la obligación de implementar los sistemas de control interno, debiendo emitir para ello la normativa de los lineamientos establecidos en las Normas de Control Interno, aprobados con Resolución de Contraloría N° 320-2006-CG, se encuentran obligados a documentar y difundir las políticas, normas y procedimientos de gestión y control interno. Su omisión genera responsabilidad administrativa funcional, así como responsabilidad civil o penal, de ser el caso. Los componentes del sistema de control interno están el ambiente de control que es el entorno de la organización. La evaluación de riesgos que debe identificar, analizar y realizar planes de acción para mitigar el riesgo de los riesgos que puedan afectar a las instituciones. El seguimiento de resultados es importante porque se monitorea el estado actual de las acciones a tomar para implementar las recomendaciones formuladas en los informes por los órganos del sistema nacional de control. Los compromisos de mejoramiento es que luego de haber evaluado las recomendaciones formuladas por el órgano de control interno la entidad se debe comprometer a implementar las mejoraras evidenciadas definiendo planes de acción con fechas propuestas de implementación de la misma. La auditoría de seguridad informática es necesario porque hay que proteger los sistemas informáticos las plataformas tecnológicas, los servicios informáticos y los activos de tecnologías de información en que las instituciones deben hacer inversiones para mantener operativa su entidades. En los cambios estructurales de las instituciones de las entidades es importante

incluir en ella las funciones y el área para que se encargue de la auditoria de organización informática. En el desarrollo de las auditorias de sistemas informáticos. Costas (2011) refiriéndose a la administración de tecnologías de información dijo que “Los elementos principales a proteger, en cualquier sistema informático son software, hardware y los datos. Habitualmente los datos constituyen el primer elemento a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar” (p. 26).

Los activos informáticos deben estar identificados en todos los procesos de información y esto se realiza a través de la clasificación de la información en la que se identifica los activos teniendo en cuenta los criterios de criticidad e importancia, y una vez identificados se realiza un tratamiento de la información a través del uso de sellos de agua identificándolo como confidencial, dándole la importancia en su almacenamiento, proceso y transporte. Las bases de datos de la organización deben ser protegidas, es decir encriptar la base de datos debido a que ella contiene

Estos resultados son coherentes con lo que sostiene teóricamente la Según la Superintendencia de Banca, Seguros y Administradores privadas de fondo de pensiones (2009), el mismo que la característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad. La seguridad de la información, es la protección de los activos de información fundamentales para el éxito y viabilidad de los negocios mediante un sistema de gestión de la seguridad de la información que administre los riesgos que atentan la confidencialidad, la integridad y la disponibilidad de la información. El mismo que debe estar formando parte del plan estratégico institucional. Resguardar el cumplimiento de las normativas vigentes. Asimismo, promover la concientización y capacitación al personal para apoyar el cumplimiento de las políticas y procedimientos de seguridad de la información.

En relación a la segunda hipótesis específica, los resultados indican que a consecuencia de lo explicado, se tiene el área representado por los datos incidencia de tecnologías de información incide en la confidencialidad del Banco de la Nación, el cual se muestra el reporte del mismo con 87.2% de área bajo la curva COR; por lo que la administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016. Un resultado similar fue el de Corletti (2011), el mismo que afirmó que el resultado de este análisis es "La acción retardante". Esta operación realmente se propone objetivos cuya semejanza al problema de seguridad en redes informáticas es llamativo. En virtud de esa similitud es que se comienza a investigar cómo se pueden aplicar los principios de redes de computadoras para organizar una "operación informática de acción retardante". Dando como resultado una operación Informático - Militar denominada "estrategia de seguridad informática por acción retardante", y que en definitiva propone cambiar la actual defensa estática por una nueva metodología de trabajo dinámica, basada en el concepto de dejar avanzar al enemigo, para poder observarlo, desgastarlo, aprender de él y erradicar el problema de raíz.

Asimismo, estos resultados coinciden con los que sostiene teóricamente Costas (2011), el mismo que sostiene que, sse trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. Uno de los pilares del sistema de gestión de seguridad de la información es la confidencialidad, en este contexto es importante considerar la protección y resguardo de documentos y datos sensibles de los clientes y trabajadores, que los que tengan acceso solamente deben ser las personas autorizadas. cabe señalar que se debe clasificar la información no solo decir que es confidencial si no que hay que identificarla con un sello de agua, con membretes de confidencialidad, si

es transportado en físico lacrarlo, de lo contrario el documento es tratada como información de uso interno y que puede ser conocida por los trabajadores.

Sobre la tercera hipótesis específica, los resultados indican que, así mismo a consecuencia de lo explicado, se tiene el área representado por los datos incidencia de tecnologías de información incide en la integridad del Banco de la Nación, el cual se muestra el reporte del mismo con 86.31% de área bajo la curva COR; por lo que la administración de tecnologías de información incide en la Integridad del Banco de la Nación, 2016. Un resultado similar fue el de Bullón (2010), el mismo que afirmó que el estudio de investigación fue dirigido a evaluar empíricamente el impacto de la TI en la ventaja competitiva, y el análisis por sesgo común no arrojó evidencias suficientes de que existiera un sesgo común entre estos dos tipos de variables independientes y dependientes. El rápido cambio tecnológico por el que atraviesa el mundo, con grandes avances en las tecnologías de la información y las comunicaciones, los países deben adaptarse a las nuevas tecnologías en todos los sectores porque si o si corren el riesgo de quedar obsoletos, especialmente los países en desarrollo, de profundizar la llamada brecha tecnológica que los separa del mundo industrializado. Desde el punto de vista económico, la tecnología es un proceso muy importante en la producción, la innovación y el desarrollo tecnológico como fuentes de crecimiento de la productividad y competitividad, a nivel empresarial y nacional. La innovación juega un papel central en los distintos procesos económicos. La innovación se refiere a la asimilación y explotación exitosa de una invención para la mejora de procesos o introducción de nuevos productos o servicios en el mercado. Por su parte, el desarrollo tecnológico se refiere a las actividades involucradas en conducir la invención a un uso práctico. Capacidades dinámicas son las habilidades de la organización para integrar, construir competencias en ambientes de rápido cambio y reflejan la habilidad de la organización para alcanzar nuevas e innovadoras formas de ventaja competitiva con el objetivo de mantenerse en el mercado competitivo

Asimismo, estos resultados coinciden con los que sostiene teóricamente Garcia Moran (2013), el mismo que sostiene que, Los ataques internos son una realidad y representan una gran parte de los ataques informáticos según el FBI. Para poder mejorar la seguridad interna, se deberán hacer políticas más estrictas sobre acceso a recursos de información por parte de los usuarios. No hay motivo alguno para que la secretaria del jefe tenga acceso a la base de datos de cliente desde su ordenador si es que ella no trabaja con estos. Los accesos a los recursos de información deben estar definidos en un procedimiento de gestión de accesos e identidades de los sistemas de información, sistemas informáticos y plataformas tecnológicas, en la que se definen claramente las responsabilidades de cada trabajador, usuario y cliente. Asimismo, los jefes deben ser concientizados en temas de seguridad de información para que sepan el riesgo que están asumiendo al momento de dar su contraseña a otras personas. Con la concientización se mitigan los ataques internos que cada día van en aumento.

En referencia a la cuarta hipótesis específica, los resultados indican que se tiene el área representado por los datos incidencia de tecnologías de información incide en la integridad del Banco de la Nación, el cual se muestra el reporte del mismo con 59.6% de área bajo la curva COR; la administración de tecnologías de información influye en la disponibilidad del Banco de la Nación, 2016. Un resultado similar fue el de Valenzuela (2015), la misma que afirmó que el modelo de gestión del conocimiento, diseñado en primera aproximación y propuesto al BN en este estudio, tiene la validez necesaria para ser eventual componente del diseño de una nueva estrategia Competitiva del BN, en un contexto de creciente competencia motivada en parte por el rápido crecimiento y modernización del Banco de la Nación desde el año 2006, y las perspectivas objetivas que se derivarían de la eventual implementación de este modelo por el BN, para el próximo quinquenio, bajo distintos escenarios posibles del clima de negocios del país y de la banca, serán significativamente mejores para el BN. Cualquier optimización de los servicios de las empresas da como resultado inversiones rentables siempre y cuando estas hayan tenido como base la gestión del conocimiento de cómo optimiza los servicios. Para que esto tenga resultados positivos y se cumplan en los costos y plazos establecidos es vital considerarlos

dentro del plan estratégico empresarial. Considerar como objetivo específicos entre otros ampliación de servicios y fortalecer el conocimiento del cliente. El objetivo para ampliar los servicios es incrementar en cantidad, calidad y cobertura a nivel nacional, desarrollar nuevas modalidades crediticias, desarrollar interfaces electrónicas para facilitar el intercambio de información y medios de pago para que los clientes utilicen Internet como medio seguro para sus transacciones, implementar una solución antifraude para clientes y usuarios. Para dar un buen servicio la empresa fortalecer el conocimiento del cliente y para eso se necesita estar preparados al interno de la organización desarrollando una plataforma data warehouse y customer relationship management. En importante siempre considerar estrategia competitiva en las organizaciones como ampliar los canales de atención al cliente modernos, considerar ando una expansión de canales de atención como el internet, implementar una mesa de ayuda, ampliar las oficinas dependiendo del consumidor y necesidades del cliente. Otra arista importante en toda organización para mantenerse en este mercado cambiante y competitivo donde el cliente es cada vez más exigente es comprometerse en la modernización de las organizaciones y para lograr este objetivo también se debe tener una estrategia para integrar las tecnologías de información a los procesos de la organización.

Otro resultado fue el de Colorado (2012), quien afirmó que identificar áreas de oportunidad de mejora en el proceso de adquisiciones y establecer una propuesta de mejora del proceso de adquisiciones. Un área clave de mejora operativa más importante para la empresa se encuentra en el área de compras, que genera resultados inmediatos en el negocio no solo en costos, sino también en la calidad del producto y en la capacidad de atender al cliente. Se definen cuatro grandes grupos de actividades en el proceso de compras, actividades de información en el estudio de mercado de los proveedores, negociación de las necesidades de la empresa y habilidades del comprador, pedidos con las formalidades del caso desde la detección de la necesidad hasta la recepción del pedido y esta parte del proceso no tiene necesariamente que estar bajo la responsabilidad de la función de compras y seguimiento asegurando la demanda con la satisfacción del cliente, esta parte del proceso normalmente está mejor ubicada bajo la responsabilidad del área funcional que tiene más interés por el

producto comprado. También puede ser soportado por sistemas de información, no solo para la automatización de tareas, sino también para la generación de avisos y la realización de nueva planificación en casos de retrasos y modificaciones. Un proyecto de mejora de compras debe dedicarse a cada uno de estos cuatro grandes bloques de trabajo, que pueden y es recomendable deben estar distribuidos en diferentes áreas de responsabilidad en la organización. Hay de todo en este conjunto de actividades, desde tareas que pueden ser mecanizadas, actividades que pueden ser eliminadas y habilidades que pueden ser desarrolladas. Para lograr esto es necesario dividir la tarea de mejora continua en dos partes. La primera es la mejora continua de procesos del departamento. No importa que tan capaces y buenos negociantes sean las personas si su trabajo diario se ve afectado por un cumulo de procesos lentos, complicados, burocráticos que simplemente merman el talento de cada uno y disminuyen el valor real de su contribución a la empresa y la segunda es un plan estratégico del negocio donde la una estrategia definida para la mejora continua de los procesos del área de compras

Asimismo, estos resultados coinciden con los que sostienen teóricamente Bauset y Rodenes (2013), los mismos que los servicios de tecnologías de la información son cada vez más complejos, se incrementan sus niveles regulatorios, se producen frecuentes desviaciones en tiempo o en costes en su ciclo de vida, continuos avances tecnológicos, etc., todo lo cual hace su gestión más necesaria para que sigan siendo eficientes, pero a la vez más compleja. Si la gestión eficaz se consigue que los cambios se adapten proactivamente a la estrategia del negocio. Actualmente desde el punto de vista de tecnologías de información la única constante es el cambio, esto quiere decir que las organizaciones para mantenerse en el mercado deben desarrollar estrategia para aceptar el cambio, tanto los cambios regulatorios como los de las necesidades de los clientes que cada día son más específicos y generalizados entonces los procesos son más complejos y es ahí donde las herramientas de tecnologías de información deben apoyar a la gestión de servicios para seguir siendo eficientes y satisfacer las necesidades del cliente y se debe tratar de superar las expectativas del cliente para considerarlo en la cartera de proyectos.

V. CONCLUSIONES

Primera

La administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016. Como se demuestra con el área representado por los datos incidencia de la administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, el cual se muestra el reporte del mismo con 83.0% de área bajo la curva COR. (p – valor = 0.00 < 0.05).

Segunda

La administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016. Como se demuestra con el área representado por los datos incidencia de tecnologías de información incide en la seguridad de la información del Banco de la Nación, el cual se muestra el reporte del mismo con 67.7% de área bajo la curva COR. (p – valor = 0.00 < 0.05).

Tercera

La administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016. Como se demuestra con el área representado por los datos incidencia de tecnologías de información incide en la confidencialidad del Banco de la Nación, el cual se muestra el reporte del mismo con 87.2% de área bajo la curva COR. (p – valor = 0.00 < 0.05).

Cuarta

La administración de tecnologías de información incide en la Integridad del Banco de la Nación, 2016. Como se demuestra con el área representado por los datos incidencia de tecnologías de información incide en la integridad del Banco de la Nación, el cual se muestra el reporte del mismo con 63.1% de área bajo la curva COR. (p – valor = 0.00 < 0.05).

Quinta

La administración de tecnologías de información incide en la disponibilidad del Banco de la Nación, 2016. Como se demuestra con el área representado por los datos incidencia de tecnologías de información incide en la disponibilidad del Banco de la Nación, el cual se muestra el reporte del mismo con 59.6% de área bajo la curva COR. (p – valor = 0.00 < 0.05).

VI. RECOMENDACIONES

Primera:

Se recomienda a la gerencia general del Banco, a través de la gerencia de recursos humanos y seguridad incluir en los planes de capacitación talleres con el propósito de fortalecer la importancia de elaborar y mantener actualizados los procedimientos de seguridad informática. Esto podría servir de sustento, para estar preparados en la constante rotación de personal, asimismo, sustentar en las visitas de los órganos supervisores, de regulación, de auditorías internas y externas. Es importante considerar los procedimientos de seguridad informática desde un enfoque por procesos apoyados en marcos de trabajo como el COBIT, ITIL y las buenas prácticas como las NIST y PCI.

Segunda:

Se recomienda a gerencia general del Banco, a través de la gerencia de riesgos implementar el sistema de gestión de seguridad de información con el propósito de que los usuarios y clientes del Banco conozcan las políticas que rigen la seguridad de la información. Este sistema de gestión asegurar el tratamiento de la información de los trabajadores y clientes del Banco, además del uso adecuado de las tecnologías de información, plataformas tecnológicas y sistemas de información.

Tercera:

Se recomienda a gerencia general del Banco de la Nación, a través de las gerencias de seguridad y planeamiento y desarrollo establecer normas que pongan énfasis en la confidencialidad de los datos e información de los usuarios y clientes. Esta norma podría contribuir a que los datos e información que se procesa, transportan y almacenan el Banco deben tener acceso sólo los usuarios y clientes que estén autorizados, de esta manera se reduce los riesgos de fraudes. Además, el Banco de la Nación debe contar con una solución de monitoreo de control avanzado de seguridad interna.

Cuarta:

Se recomienda a gerencia general del Banco, a través de la gerencia de informática y seguridad y prevención, aplicar estrategias institucionales para fortalecer la dimensión integridad con la finalidad de evaluar la posibilidad de encriptar la base de datos de los clientes, de los servidores y de las comunicaciones en donde se almacenan se procesan y transportan los datos e información sensible de los clientes del Banco. Esta estrategia podría servir como cumplimiento de la ley de protección de los datos personales. Asimismo, el Banco de la Nación debe considerar en sus proyectos implementar una gestión de incidentes de seguridad informática.

Quinta:

Se recomienda a gerencia general del Banco, a través de la gerencia de finanzas y contabilidad elaborar un presupuesto contemplando las necesidades y requerimientos de tecnología de información de la gerencia de informática y de seguridad y prevención para contar con la disponibilidad presupuestal. Asimismo la gerencia de logística debe contemplar en la elaboración del plan anual de adquisiciones y contrataciones del estado considerar de bienes y servicios de tecnologías de información, sistemas informáticos y plataformas tecnológicas. Una elaboración del presupuesto y del plan de adquisiciones y contrataciones adecuadas podría contribuir a cumplir con la misión y visión del Banco y mantener la disponibilidad de las operaciones todos los días del año. El Banco de la Nación debe considerar en sus proyectos la necesidad de un análisis de seguridad de los ambientes de los canales.

VII. REFERENCIAS BIBLIOGRÁFICAS

Aguayo, M. (2012). Como hacer una regresión logística con SPSS. Dot. Núm 0702012. Sevilla. Recuperado el 31 de octubre de 2016 desde http://www. fabis.org/html/archivos/docuweb/Regres_log_1r.pdf

Barrionuevo, V., y Ortiz, E. (2015). Desarrollo de un modelo para logros de cumplimiento de las normativas del sector financiero público en la "Gestión de Servicios de TI". (Tesis para obtener el título de Máster en Gestión de las Comunicaciones y Tecnologías de la Información. Escuela Politécnica Nacional de Quito. Quito). Recuperado el 18 de febrero de 2016 desde http://bibdigital.epn.edu.ec/handle/15000/11529

Bauset, M., y Rodenes, M. (2013). Gestión de los servicios de tecnologías de la Información: modelo de aporte de valor basado en ITIL e ISO/IEC 20000".Valencia. España. Recuperado el 20 de abril del 2016 desde https://core.ac.uk/download/files/418/11890576.pdf

Beyon, P. (2014). Fundamentos epistemológicos de la investigación y la metodología de la investigación: cualitativa cuantitativa. Medellín, Colombia: Fondo Editorial Universidad EAFIT

Bon, J., Jong,A.,Kolthof, A.,Pieper,M.,Jassing,R.,Veen,A y Verheijen,T. (2008). Estrategia del servicio basada en ITIL V3- guía de gestión. Gobierno Británico, Gran Bretaña: Van Haren Publishing, Zaltbommel.

Burgueñoa, M., García, J., y Gonzales, J. (2012). Las curvas ROC en la evaluación de las pruebas diagnósticas. La Habana. Cuba. Recuperado el 31 de octubre de 2016 desde http://ferran.torres.name/download /shared/ roc/ROC%20M 104170 7.PDF

Bullón, L. (2010). Ventaja competitiva de las capacidades operacionales y dinámicas de la tecnología de la información: caso de Lima, Perú. (Tesis para optar el grado de doctor en administración estratégica de empresas.

Pontificia Universidad Católica. Perú). Recuperado el 06 de junio de 2016 desde http://tesis.pucp.edu.pe/repositorio/handle/123456789/1604

Carbajal, J. (2013). Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano. (Tesis para optar el grado de master en dirección estratégica en tecnologías de la información. Universidad de Piura. Perú). Recuperado el 18 de febrero de 2016 desde http://pirhua.udep.edu.pe/handel/123456789/2022

Colorado, M. (2012). Propuesta de Optimización y Normalización del Proceso Adquisitivo de Tecnologías de la Información y Telecomunicaciones del Instituto de Seguridad Social del Estado de México y Municipios. (Tesis para obtener el grado de maestro en ingeniería de calidad. Universidad Iberoamericana de México, D.F.). Recuperado el 18 de febrero de 2016 desde http://www.bib.uia.mx/tesis/pdf/015620/015620.pdf

Contraloría General de la República del Perú. (2006).Resolución N° 320 Normas de Control Interno. Publicado el 03 de noviembre de 2006. Recuperado el 20 de abril de 2016 desde http://controlinterno.concytec.gob. pe/images /stories/2012/normatividad/RCG_320_2006_CG.pdf

Consejo Nacional para la Enseñanza y la Investigación de las Ciencias de la Comunicación (2011). La comunicación que necesitamos el país que queremos. México, D.F: Editada por CONEICC. Recuperado el 18 de febrero del 2016 desde http://www.bib.uia.mx/tesis/pdf/015620/015620.pdf

Corletti, M. (2011). Estrategia de seguridad informática por capas, aplicando el concepto de operación militar por acción retardante. (Tesis para obtener el grado de doctor ingeniería de software y sistemas informáticos. Universidad nacional de educación a distancia de Madrid. España). Recuperado el 09 de junio de 2016 desde http://e-spacio. uned.es/ fez/eserv/tesisuned:IngInf-Accorletti/Documento.pdf

Costas, J. (2011). Seguridad Informática. Bogotá, Colombia: Editorial Ra-me

(España)

Cumbre Mundial de la Sociedad de la Información (2005). Sociedad de la Información Sociedad del conocimiento. Recuperado el 25 de octubre de 2016 desde http://www.google.com/url?sa=t&rct=j&q=esrc=s&source=web&cd=1&ved=0ahUKEwi109u-jPbPAhVGdD4KHfnGAAkQFggeMAA&url=http%3A%2F%2Fwww.ub.edu%2Fprometheus21%2Farticulos%2Fobsci berpro me%2Fsocinfsoccon.pdf&usg=AFQjCNE_5AVu2ORfw-gx-6ykE6PbbkC2dA

García-Moran, J., Fernandez, Y., Martínez, R., Ochoa, A., y Ramos, A. (2013). Haking y seguridad en internet (2da. Ed.). Bogotá, Colombia: Editorial Ra-ma (España)

Gallegos, F.P., y Murillo, M.F. (2015). Metodología de gestión de seguridad de la información enfocado a las industrias de telecomunicaciones en el ecuador. (Tesis para obtener el grado de Máster en Gestión de las Comunicaciones y Tecnologías de la Información. Escuela Politécnica Nacional de Quito. Quito). Recuperado el 18 de febrero de 2016 desde http://bibdigital.epn.edu.ec/handle/15000/10512

Gómez, A. (2007). Enciclopedia de la seguridad informática. Madrid, España: Alfaomega grupo editor.

Gómez, A. (2013). Seguridad en equipos informáticos. Bogotá, Colombia: Starbook editorial (España)

Heredia, J., Rodríguez, A., y Vilalta, J. (2012). Empleo de la regresión logística ordinal para la predicción del rendimiento académica. Revista investigación operacional. La Habana. Cuba. VOL. 33, NO. 3, 252-267, 2012. Recuperado el 31 de octubre de 2016 desde http://rev-inv-ope.univ-paris1.fr/files/33312/33312-06.pdf

Hernández, R., Fernández, C., y Baptista, M. (2014). Metodología de la investigación (6ta. Ed). Santa Fe, México D.F.: Editorial McGraw- Hill

Horna, L. (2016). Implementación de la ISO/IEC 12207:2008 para mejorar los procesos asociados al ciclo de vida de software en una micro empresa peruana cuyo objeto social es el desarrollo de sistemas de información. (Tesis para optar maestría en informática con mención en ingeniería de software. Pontificia Universidad Católica. Perú). Recuperado el 06 de junio de 2016 desde http://tesis.pucp.edu.pe/repositorio/handle/123456789/6298

Macau, R. (set – nov, 2004). Tecnologías de información y comunicaciones: ¿Para qué? Funciones de las tecnologías de la información y la comunicación en las organizaciones. Revista de universidad y sociedad del conocimiento. Barcelona, España, 1,1-12. Recuperado el 26 de setiembre 2016 desde http://www.redalyc.org/articulo.oa?id=78011256005

Marchand, W. (2013). Metodología de implantación del modelo balanced scorecard para la gestión estratégica de TIC. Caso: universidad nacional agraria de la selva. (Tesis para optar el grado de Master en dirección estratégica en tecnologías de la información. Universidad de Piura. Perú). Recuperado el 18 de febrero de 2016 desde http://pirhua.udep. edu.pe/ handle/123456789/1842

Norma internacional ISO/IEC 27001 (2013). Tecnología de la información técnica de Seguridad Sistema de gestión de seguridad de la información (SGSI). Madrid, España: Editada e impresa por AENOR

Superintendencia de Banca, Seguros y Administradores privada de fondo de pensiones. (2009).Circular N° G-140 Gestión de la Seguridad de la Información. Publicado el 02 de abril de 2009. Recuperado el 17 de febrero de 2016 desde https://intranet2.sbs.gob. pe/intranet/INT_ CN/DV_INT_ CN/249/v1.0/Adjuntos/g-140-2009.c.pdf

Schmarzo, B. (2014). Big data el poder de los datos. Madrid: Ediciones Anaya Multimedia

Toro, I., y Parra, R. (2010). Gestión de los servicios de tecnologías de la Información: modelo de aporte de valor basado en ITIL e ISO/IEC 20000".Valencia. España. Recuperado el 20 de abril del 2016 desde https://core.ac.uk/download/files/418/11890576.pdf

Valenzuela, Y. (2015). Sistema de gestión del conocimiento para la optimización de la relación entre los servicios y las inversiones del Banco de la Nación. (Tesis para optar el grado de maestro de ingeniería de computación y sistemas con mención en gestión de tecnologías de información. Universidad San Martín de Porres. Perú). Recuperado el 30 de mayo de 2016 desde http://www.repositorioacademico. usmp.edu. pe/handle/ usmp/ 1448

APENDICES

APENDICE 01

MATRIZ DE CONSISTENCIA

TÍTULO: ADMINISTRACION DE TECNOLOGIAS DE INFORMACIÓN EN LOS PROCEDIMIENTOS DE SEGURIDAD INFORMATICA DE

AUTOR: PEREZ CASTILLO, MARÍA ROSARIO

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARI
Problema general: **¿Cuál es la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016?** **Problemas específicos:** **¿Cuál es la incidencia de la administración de tecnologías de información en la seguridad de la información del Banco de la Nación, 2016?** **¿Cuál es la incidencia de la administración de tecnologías de información en la confidencialidad del Banco de la Nación, 2016?** **¿Cuál es la incidencia de la administración de tecnologías de información en la Integridad del Banco de la Nación, 2016?** **¿Cuál es la incidencia de la administración de tecnologías de información en la disponibilidad del Banco de la Nación, 2016?**	**Objetivo general:** **Determinar la incidencia de la administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016.** **Objetivos específicos:** **Determinar la incidencia de la administración de tecnologías de información en la seguridad de la información del Banco de la Nación, 2016.** **Determinar la incidencia de la administración de tecnologías de información en la confidencialidad del Banco de la Nación, 2016.** **Determinar la incidencia de la administración de tecnologías de información en la Integridad del Banco de la Nación, 2016.** **Determinar la incidencia de la administración de tecnologías de información en la disponibilidad del**	**Hipótesis general:** La **administración de tecnologías de información incide en los procedimientos de seguridad informática del Banco de la Nación, 2016.** **Hipótesis específicas:** La **administración de tecnologías de información incide en la seguridad de la información del Banco de la Nación, 2016.** **La administración de tecnologías de información incide en la confidencialidad del Banco de la Nación, 2016.** **La administración de tecnologías de información incide en la Integridad del Banco de la Nación, 2016.** **La aplicación del programa de administración de tecnologías de información influye en la disponibilidad del Banco de la Nación, 2016.**	**Variable: Administración de t** **Dimensiones** / **In** **Gestión de servicios de TI y procesos** / **Coherenc Estructura Calidad d de tecnol informaci** **Funcionalidad y garantía** / **Resultado Percepció Valor eco Riesgo** **Recursos y capacidades** / **Crear valo Habilidad organizac Experienc** **Activos de servicios** / **Acti org Actividad Actividad conocimi Acti inf Actividad aplicacion** **Cultura** / **Actitud de Valores d Adaptar a** **Variable : Procedimientos de** **Dimensiones** / **Indicador** **Seguridad de la información** / **Políticas la informa Procedim seguridad Estructura Herramien**

	Banco de la Nación, 2016.		**Confidencialidad**	**Gestión d** **Cuentas r** **Duplicida** **Cuentas r**
			Integridad	**Gestión d** **Gestión d** **vulnerabil**
			Disponibilidad	**Gestión d** **Usuarios** **durante el** **Requerim** **fuera del**

APENDICE 02

INSTRUMENTOS DE EVALUACION DE LA VARIABLE ADMINISTRACION DE TECNOLOGIAS DE INFORMACION

UNIVERSIDAD CESAR VALLEJO

ESCUELA DE POSTGRADO

CUESTIONARIO

Estimado (a) con el presente cuestionario se pretende obtener información respecto a la administración de tecnologías de información en el área donde Ud. trabaja, para lo cual le solicitamos su colaboración, respondiendo todas las preguntas. Los resultados permitirán proponer sugerencias para mejorar la administración de tecnologías de información. Marque con una (X) la alternativa que considera pertinente en cada caso

ESCALA VALORATIVA

CÓDIGO	CATEGORÍA	
S	Siempre	5
CS	Casi siempre	4
AV	A veces	3
CN	Casi nunca	2
N	Nunca	1

	VARIABLE : ADMINISTRACION DE LAS TECNOLOGIAS DE INFORMACION					
	DIMENSION GESTION DE SERVICIOS DE TECNOLOGIAS DE INFORMACION Y PROCESOS	**S**	**CS**	**AV**	**CN**	**N**
1	Las funciones de Tecnologías de información se encuentran en el manual de organización y funciones de la Gerencia de Informática					
2	Las responsabilidades de las áreas están de acuerdo a la estructura orgánica					
3	Los procesos están identificados adecuadamente					
4	Los responsables de los procesos están identificados					
5	En una reestructuración organizacional cambian los procesos					
6	Se utiliza una metodología para elaborar los procedimientos técnicos operativos					
	DIMENSION FUNCIONALIDAD Y GARANTIA	**S**	**CS**	**AV**	**CN**	**N**
7	Las metas propuestas en el plan de trabajo del					

	área de tecnologías de información, producen los resultados esperados anualmente					
8	Las actividades del área de seguridad informática apoyan los objetivos definidos en el Plan estratégico institucional					
9	La atención del personal de tecnologías de información es oportuna					
10	Los ambientes y oficinas para atender a los usuarios es adecuada					
11	Los empleados del área de tecnologías de información se encuentran dispuestos para ayudar a los usuarios					
12	La organización cuenta con una política de bancarización					
13	Se realizan planes de mitigación de los riegos identificados					
14	Los empleados del área de tecnologías de información transmiten confianza a sus usuarios					
	DIMENSION RECURSOS Y CAPACIDADES	**S**	**CS**	**AV**	**CN**	**N**
15	La organización formula planes estratégicos, operativos y de tecnologías de información					
16	Las tecnologías de información y servicios informáticos apalancan los objetivos definidos en el plan operativo anual					
17	La organización cuenta con un área de proyectos de tecnologías de información					
18	Se informa de manera oportuna y adecuada los resultados de la ejecución y cumplimiento de los proyectos de tecnologías de información					
19	El personal que labora en informática cuenta con conocimientos de procedimientos de seguridad informática					
20	La gerencia de tecnologías de información motiva al personal					
	DIMENSIÓN ACTIVOS DE SERVICIO	**S**	**CS**	**AV**	**CN**	**N**
21	El área de tecnologías de información, cuenta con el apoyo de la alta dirección					
22	La Gerencia de tecnologías de información ejerce un liderazgo adecuado					
23	Impactan los procesos de tecnologías de información en la institución					
24	La gestión de los procedimientos técnicos operativos es adecuada					
25	Se evalúa al personal respecto a la capacitación recibida					
26	El área de tecnología de información formula un plan de capacitación					

27	Se cuenta con una normativa para la clasificación de los activos de la información					
28	Son conocidos los activos de información y su clasificación					
29	Existen normativas y herramientas que apoyan a la gestión de las aplicaciones de tecnologías de información					
30	Los encargados del desarrollado, pruebas y pase a producción de las aplicaciones, tienen conocimiento del ciclo de vida de software					
	DIMENSION CULTURA	**S**	**CS**	**AV**	**CN**	**N**
31	El personal de informática se expresa favorablemente en cuanto al ambiente de trabajo					
32	El personal tiene una actitud positiva para identificar los procedimientos					
33	El reclutamiento de personal para el área de tecnologías de información es el adecuado					
34	La institución cuenta con un código de ética					
35	Se cuenta con una política clara y coherente a nivel de la alta dirección					
36	Se consideran proyectos para el cambio organizacional					

¡Muchas gracias!

APENDICE 03

INSTRUMENTOS DE EVALUACION DE LA VARIABLE PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA

UNIVERSIDAD CESAR VALLEJO

ESCUELA DE POSTGRADO

CUESTIONARIO

Estimado (a) con el presente cuestionario se pretende obtener información respecto a los procedimientos de seguridad informática en el área donde Ud. trabaja, para lo cual le solicitamos su colaboración, respondiendo todas las preguntas. Los resultados permitirán proponer sugerencias para mejorar los procedimientos de seguridad informática. Marque con una (X) la alternativa que considera pertinente en cada caso.

ESCALA VALORATIVA

CÓDIGO	CATEGORÍA	
S	Siempre	5
CS	Casi siempre	4
AV	A veces	3
CN	Casi nunca	2
N	Nunca	1

	VARIABLE : PROCEDIMIENTOS DE SEGURIDAD INFORMATICA					
	DIMENSION SEGURIDAD DE LA INFORMACION	**S**	**CS**	**AV**	**CN**	**N**
1	La organización cuenta con una política de la seguridad de la información					
2	las actividades de seguridad informática impactan en los objetivos de la seguridad de la información					
3	Los procedimientos de seguridad informática están actualizados					
4	La metodología que se utiliza para elaborar los procedimientos es la apropiada					
5	La organización cuenta con un área de seguridad de la información					
6	La organización cuenta con un área de seguridad informática					
7	Existen herramientas se utilizan para realizar el monitoreo del cumplimiento de la política de la					

	seguridad de la información					
8	La institución cuenta con una herramienta de para reportar eventos e incidentes de seguridad					
	DIMENSION CONFIDENCIALIDAD	**S**	**CS**	**AV**	**CN**	**N**
9	Existen directivas, circulares, procedimientos u otro documento que norme la gestión de accesos					
10	El acceso que se otorgado está de acuerdo a la función autorizada					
11	Se actualizan los roles funcionales de las áreas					
12	El cambio de rotación de personal se refleja en las cuentas					
13	La duplicidad de roles es debido a que no se actualiza la matiz funcional					
14	Las medidas correctivas para reducir la duplicidad de roles dan resultado					
15	La operatividad del servicio se ve afectada					
16	Los incidentes que los usuarios reportan son atendidos oportunamente					
	DIMENSION INTEGRIDAD	**S**	**CS**	**AV**	**CN**	**N**
17	Existen clientes que son afectados por ataques de phishing					
18	El monitoreo que se realiza es el adecuado					
19	Se realiza el seguimiento o monitoreo de las vulnerabilidades en los servicios informáticos					
20	Se realizan medidas correctivas a las vulnerabilidades encontradas					
	DIMENSION DISPONIBILIDAD	**S**	**CS**	**AV**	**CN**	**N**
21	Existe alguna metodología para realizar la gestión de roles de las áreas de la organización					
22	Los usuarios tienen roles de acuerdo a su perfil					
23	Los usuarios atendidos durante el plazo establecido dependen del requerimiento					
24	Las tecnologías de información apoyan a la atención usuario en el plazo establecido					
25	Los requerimientos enviados fuera del plazo tienen inconvenientes para ser atendidos					
26	Los requerimientos solicitados fuera del plazo afectan la operatividad					
27	Los usuarios son atendidos fuera del plazo por inconvenientes en las herramientas					
28	Las tecnologías de información apoyan a esta actividad					

¡Muchas gracias!

ANEXO 04

DOCUMENTOS PARA VALIDAR LOS INSTRUMENTOS DE MEDICION A TRAVES DE JUICIOS EXPERTOS

S

ANEXO 05

BASE DE DATOS DE LA PRUEBA PILOTO

Base datos Prueba piloto variable administración de tecnologías de información

	VARIABLE: ADMINISTRACION DE TECNOLOGIAS DE INFORMACION																																			
Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
1	5	5	4	5	3	3	4	5	4	4	5	4	4	4	4	4	5	4	5	5	5	5	5	5	4	4	5	4	4	4	5	4	4	5	4	4
2	4	4	4	4	4	3	3	4	3	3	4	3	3	3	4	4	3	4	3	3	4	3	4	3	3	4	3	3	4	3	3	3	3	3	2	3
3	5	4	3	3	4	4	5	5	5	3	5	5	5	5	5	5	5	5	4	1	4	2	5	3	5	5	4	2	4	4	1	3	4	5	5	5
4	5	5	2	2	5	5	4	5	5	4	5	5	5	5	5	5	5	5	5	2	5	4	5	5	5	5	5	5	5	2	5	5	4	5	5	5
5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	5	5	5	5	5	5	5	5	5
6	4	4	3	2	3	4	4	4	4	4	3	5	1	3	3	4	5	3	4	2	3	2	4	4	5	4	4	5	1	1	3	3	3	5	4	4
7	5	4	4	4	5	3	4	5	4	4	5	5	4	5	5	5	4	5	4	5	3	3	5	4	4	4	4	4	4	5	5	5	5	5	5	5
8	5	4	5	5	3	4	4	5	4	4	5	5	5	5	4	5	5	4	4	3	4	4	5	5	5	3	5	5	5	5	4	4	5	5	5	5
9	4	4	4	5	3	5	4	4	4	4	5	5	4	4	5	5	5	5	5	4	4	5	5	5	4	3	4	4	5	5	5	5	5	5	4	4
10	5	4	4	3	4	5	4	5	4	4	4	5	5	4	4	4	5	3	4	3	4	4	5	3	5	4	5	5	5	5	4	4	5	5	5	4
11	3	3	5	5	5	5	3	5	3	4	2	5	4	2	3	4	5	3	2	1	2	3	5	3	3	2	4	3	5	5	3	3	1	1	2	3
12	5	4	5	5	2	4	4	5	4	1	4	5	5	5	4	4	5	4	5	3	5	4	5	4	4	5	5	5	5	5	3	4	5	5	5	5
13	3	5	4	5	2	4	4	4	4	1	4	5	5	5	4	4	5	3	5	3	5	4	5	3	5	5	5	5	5	5	3	5	5	5	5	5
14	4	3	3	3	4	3	3	3	3	2	3	4	4	3	4	4	4	4	2	2	4	3	4	3	2	3	5	5	4	5	2	3	3	5	5	4
15	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	4	4	4	4	4	4	4
16	3	4	5	5	4	4	5	4	4	4	4	4	4	4	4	5	4	4	3	4	5	4	4	4	4	4	5	4	4	4	4	4	3	5	5	5
17	4	3	3	4	3	3	3	4	3	3	4	4	4	3	4	4	3	3	4	3	4	3	4	4	2	2	3	2	2	3	2	2	2	2	3	3
18	3	4	4	4	4	4	3	4	4	3	4	4	4	4	4	4	4	4	4	3	3	3	4	3	3	3	4	4	4	4	4	4	3	4	4	4
19	3	3	2	2	5	2	3	3	3	3	2	4	3	2	4	3	3	3	3	2	2	1	5	2	2	3	3	1	2	2	2	2	1	3	2	1
20	4	3	3	2	4	3	2	3	2	3	2	3	2	3	3	4	2	3	3	2	1	2	4	3	3	2	2	2	3	3	2	2	2	2	4	2

Base datos Prueba piloto variable procedimientos de seguridad informática

	VARIABLE: PROCEDIMIENTOS DE SEGURIDAD INFORMATICA																											
Nro.	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54	P55	P56	P57	P58	P59	P60	P61	P62	P63	P64
1	5	5	4	3	5	5	4	3	5	5	5	5	4	5	3	4	3	3	4	3	4	5	5	5	3	4	5	4
2	4	4	3	3	4	3	2	3	4	3	3	3	4	4	4	3	4	3	3	3	4	4	4	3	5	4	3	4
3	3	3	4	4	4	3	4	3	2	3	4	4	3	3	3	4	3	4	4	4	3	3	3	4	4	5	4	3
4	5	5	4	5	1	5	4	5	5	5	5	5	5	2	4	5	2	4	2	4	5	5	5	5	4	5	4	5
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	4	3	4	5	5	5	5	5	5	5	4	4	5
6	5	5	4	5	1	5	4	5	5	5	4	5	4	1	3	4	4	2	2	2	5	5	4	4	4	5	3	2
7	5	5	3	4	4	5	5	5	5	5	4	3	5	3	5	3	5	5	5	5	4	5	4	4	4	5	4	5
8	5	4	5	5	5	5	5	5	5	4	5	4	4	4	3	5	3	5	5	5	4	4	5	5	3	2	2	5
9	5	4	5	5	5	5	5	5	5	5	4	5	3	4	3	5	3	5	5	5	5	5	4	4	3	3	2	5
10	5	5	3	5	5	5	5	5	5	3	4	3	5	3	3	4	3	4	3	5	4	5	5	5	4	4	3	5
11	5	5	4	4	5	5	1	4	5	5	3	4	4	3	3	4	3	4	4	3	5	4	4	4	3	3	3	5
12	5	3	5	3	5	5	5	5	5	5	5	5	3	3	1	4	3	4	5	4	5	5	5	5	3	3	2	5
13	5	3	5	3	5	5	5	5	5	5	5	5	3	5	1	4	3	5	2	2	5	5	5	5	3	3	2	4
14	5	5	4	3	4	4	4	4	5	5	4	3	3	3	4	3	4	3	4	4	4	3	3	3	4	5	4	4
15	5	5	4	4	4	5	4	4	5	5	4	4	4	4	3	4	3	4	4	4	3	4	4	4	4	4	4	4
16	5	4	4	4	5	5	4	4	5	5	4	4	4	4	2	4	2	4	4	4	4	4	4	4	2	3	3	4
17	3	2	2	3	3	4	2	2	3	2	2	2	3	2	3	3	2	2	2	2	2	2	2	3	3	3	3	3
18	5	5	4	4	5	5	4	5	5	4	4	4	4	4	4	4	3	3	4	4	5	5	5	5	2	4	2	4
19	3	5	1	1	3	3	3	3	3	3	2	2	2	2	4	3	3	2	2	2	3	2	2	3	4	5	5	5
20	4	3	2	2	3	2	2	3	4	4	3	3	2	2	3	4	4	3	2	1	2	3	3	2	3	4	4	4

APENDICE 06

BASE DE DATOS DE LA MUESTRA

VARIABLE ADMINISTRACION DE TECNOLOGIAS DE INFORMACIÓN

	VARIABLE INDEPENDIENTE: ADMINISTRACION DE TECNOLOGIAS DE INFORMACION																																		
Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
1	5	5	4	5	3	3	4	5	4	4	5	4	4	4	4	4	5	4	5	5	5	5	5	5	4	4	5	4	4	4	5	4	4	5	4	4
2	4	4	4	4	4	3	3	4	3	3	4	3	3	3	4	4	3	4	3	3	4	3	4	3	3	4	3	3	4	3	3	3	3	3	2	3
3	5	4	3	3	4	4	5	5	5	3	5	5	5	5	5	5	5	5	4	1	4	2	5	3	5	5	4	2	4	4	1	3	4	5	5	5
4	5	5	2	2	5	5	4	5	5	4	5	5	5	5	5	5	5	5	5	2	5	4	5	5	5	5	5	5	5	2	5	5	4	5	5	5
5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	5	5	5	5	5	5	5	5	5
6	4	4	3	2	3	4	4	4	4	4	3	5	1	3	3	4	5	3	4	2	3	2	4	4	5	4	4	5	1	1	3	3	3	5	4	4
7	5	4	4	4	5	3	4	5	4	4	5	5	4	5	5	5	4	5	4	5	3	3	5	4	4	4	4	4	4	5	5	5	5	5	5	5
8	5	4	5	5	3	4	4	5	4	4	5	5	5	5	4	5	5	4	4	3	4	4	5	5	5	3	5	5	5	5	4	4	5	5	5	5
9	4	4	4	5	3	5	4	4	4	4	5	5	4	4	5	5	5	5	5	4	4	5	5	5	4	3	4	4	5	5	5	5	5	5	4	4
10	5	4	4	3	4	5	4	5	4	4	4	5	5	4	4	4	5	3	4	3	4	4	5	3	5	4	5	5	5	5	4	4	5	5	5	4
11	3	3	5	5	5	5	3	5	3	4	2	5	4	2	3	4	5	3	2	1	2	3	5	3	3	2	4	3	5	5	3	3	1	1	2	3
12	5	4	5	5	2	4	4	5	4	1	4	5	5	5	4	4	5	4	5	3	5	4	5	4	4	5	5	5	5	5	3	4	5	5	5	5
13	3	5	4	5	2	4	4	4	4	1	4	5	5	5	4	4	5	3	5	3	5	4	5	3	5	5	5	5	5	5	3	5	5	5	5	5
14	4	3	3	3	4	3	3	3	3	2	3	4	4	3	4	4	4	4	2	2	4	3	4	3	2	3	5	5	4	5	2	3	3	5	5	4
15	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	4	4	4	4	4	4	4	4
16	3	4	5	5	4	4	5	4	4	4	4	4	4	4	4	5	4	4	3	4	5	4	4	4	4	4	5	4	4	4	4	4	3	5	5	5
17	4	3	3	4	3	3	3	4	3	3	4	4	4	3	4	4	3	3	4	3	4	3	4	4	2	2	3	2	2	3	2	2	2	2	3	3
18	3	4	4	4	4	4	3	4	4	3	4	4	4	4	4	4	4	4	4	3	3	3	4	3	3	3	4	4	4	4	4	4	3	4	4	4
19	3	3	2	2	5	2	3	3	3	3	2	4	3	2	4	3	3	3	3	2	2	1	5	2	2	3	3	1	2	2	2	2	1	3	2	1
20	4	3	3	2	4	3	2	3	2	3	2	3	2	3	3	4	2	3	3	2	1	2	4	3	3	2	2	2	3	3	2	2	2	2	4	2
21	5	5	5	3	3	3	3	4	4	2	4	4	4	5	4	3	4	2	4	2	3	2	3	4	1	1	3	4	3	1	2	3	4	5	3	2

VARIABLE ADMINISTRACION DE TECNOLOGIAS DE INFORMACIÓN

	VARIABLE INDEPENDIENTE: ADMINISTRACION DE TECNOLOGIAS DE INFORMACION																																	
Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
22	3	4	3	3	3	4	4	3	4	3	4	4	4	4	3	4	5	4	3	2	3	3	4	3	2	3	4	4	4	4	3	3	3	4	3	2
23	4	5	4	4	4	4	4	4	4	5	5	5	4	5	4	4	5	4	5	4	5	4	4	4	4	4	4	3	4	4	5	5	4	5	4	4
24	5	5	5	3	4	5	5	4	4	3	4	5	5	5	4	4	5	4	5	4	4	4	5	3	5	4	5	5	5	5	5	5	5	5	4	5
25	5	5	5	5	3	5	5	4	4	3	5	4	5	4	4	5	4	4	4	3	3	3	5	4	4	3	4	4	4	5	3	3	3	4	3	5
26	4	4	4	4	4	5	4	4	4	3	5	4	4	5	4	5	4	4	4	3	5	4	5	5	5	4	4	4	5	4	4	4	5	5	5	5
27	3	1	3	4	2	4	4	4	4	2	5	3	3	4	4	3	3	3	2	4	4	4	4	4	3	3	3	3	4	3	3	4	3	5	2	4
28	3	3	2	2	3	2	3	3	4	2	5	5	3	4	4	3	5	2	3	3	4	4	5	4	5	3	4	3	4	4	3	4	5	4	4	4
29	4	4	4	4	5	5	4	4	5	3	5	5	4	5	5	4	3	4	5	3	3	4	4	2	2	3	4	4	4	4	5	5	5	4	4	4
30	3	4	4	4	5	3	3	4	4	2	3	4	3	3	3	4	4	2	4	3	3	4	4	4	3	2	3	2	4	2	3	3	2	4	4	5
31	4	4	4	3	5	4	4	5	4	5	5	5	4	5	3	5	4	5	4	5	5	3	4	5	3	4	5	4	5	5	4	5	4	4	5	5
32	4	4	3	4		4	4	3	4	3	5	4	3	5	4	4	4	4	3	3	3	3	4	3	4	3	4	3	3	3	3	3	4	3	4	3
33	3	4	4	3	3	4	3	3	4	3	5	4	3	4	4	4	4	5	3	3	3	3	4	3	4	3	4	5	3	3	4	3	4	3	4	3
34	4	5	4	3	2	3	5	4	4	4	5	4	4	5	4	4	4	4	3	2	4	4	4	3	4	3	3	3	4	3	4	4	4	3	3	4
35	5	4	4	4	3	2	3	4	4	4	5	5	5	5	5	4	5	4	3	3	4	4	5	4	3	3	4	4	3	4	3	3	3	5	5	5
36	5	5	5	4	4	4	3	4	5	5	5	5	5	5	5	5	5	5	5	4	5	4	4	5	5	5	5	5	5	4	4	5	4	5	5	4
37	4	3	5	5	1	4	5	3	4	2	5	5	4	4	3	3	1	4	3	3	2	2	4	4	3	2	3	2	4	3	4	5	4	5	4	4
38	1	1	2	4	1	1	3	4	4	3	4	1	2	5	3	3	3	3	4	1	3	2	2	2	1	1	1	1	3	2	2	5	2	3	3	3
39	5	5	5	4	4	4	4	4	5	4	5	5	5	5	4	5	5	5	5	4	5	4	4	5	4	5	5	5	4	5	5	5	4	5	5	4
40	4	4	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4	3	3	4	3	4	4	4	3	3	3	4	4	3	3	3	4	4	4
41	3	2	3	3	2	2	3	3	4	3	5	4	4	5	3	3	3	3	4	3	4	4	4	3	4	4	4	4	4	3	4	4	3	3	3	3
42	4	4	3	5	4	4	3	4	3	3	4	4	3	4	4	4	4	3	4	3	4	3	4	4	4	4	4	4	4	4	4	4	2	4	4	4
43	4	4	2	2	3	3	4	4	4	3	4	4	4	4	5	4	5	3	3	3	4	4	3	3	2	3	3	3	3	3	4	4	2	5	4	4

VARIABLE ADMINISTRACION DE TECNOLOGIAS DE INFORMACIÓN

	VARIABLE INDEPENDIENTE: ADMINISTRACION DE TECNOLOGIAS DE INFORMACION																																		
Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
44	5	4	4	4	4	5	5	5	4	2	5	4	5	4	5	5	4	5	4	4	5	4	3	4	5	5	5	1	5	4	3	5	4	5	5	5
45	5	5	3	4	5	4	4	4	4	1	5	5	4	4	4	4	5	2	4	2	4	4	5	4	2	1	4	4	4	4	1	4	2	5	4	4
46	4	4	3	3	4	4	4	3	3	3	3	3	3	3	4	4	4	3	3	2	4	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3
47	3	3	3	2	4	4	4	3	4	3	4	4	4	4	4	4	4	3	4	2	2	3	4	3	2	2	4	3	4	4	2	3	2	5	4	3
48	4	5	5	4	5	5	5	5	4	4	5	5	4	5	5	4	5	4	4	5	5	4	4	5	5	5	4	5	5	5	4	5	4	5	5	5
49	5	4	4	4	5	5	4	4	4	4	4	4	4	5	4	4	3	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	3	5	4	4
50	5	5	5	4	5	5	5	5	5	5	4	5	4	5	4	5	4	5	4	5	5	4	5	5	5	4	5	4	5	5	5	4	5	5	4	5
51	5	5	3	5	5	4	5	5	4	3	5	4	4	5	4	4	4	4	4	5	4	5	5	5	4	4	5	4	4	5	4	4	4	5	4	4
52	5	5	5	5	3	5	5	5	5	4	5	5	5	5	5	5	5	4	4	5	5	5	5	5	5	4	4	4	4	4	5	5	4	5	5	5
53	3	3	3	3	3	3	4	4	4	3	4	3	4	4	4	3	4	3	4	4	3	4	4	4	3	3	3	3	3	4	3	4	3	5	4	4
54	3	3	3	3	4	2	2	3	3	4	4	3	5	5	2	2	3	3	5	2	4	3	2	2	2	3	3	3	2	4	4	4	3	5	4	3
55	5	4	5	5	4	5	4	4	3	4	4	5	4	4	5	5	5	5	3	3	5	4	5	5	4	3	4	3	4	4	3	4	4	5	5	4
56	5	5	4	4	3	4	4	5	4	5	4	4	4	5	5	5	5	5	5	4	5	4	3	4	4	4	4	4	4	5	5	5	5	5	5	4
57	5	2	3	3	1	3	4	3	4	1	4	4	4	4	5	5	4	4	3	2	4	4	5	3	3	5	5	4	4	4	2	3	1	5	4	3
58	4	4	5	5	4	4	4	3	4	3	4	3	2	5	4	4	5	4	3	5	3	5	4	4	3	5	3	5	4	5	4	5	3	4	5	4
59	4	4	4	5	4	4	3	5	4	4	5	4	5	4	5	4	5	3	4	3	4	4	5	4	3	3	4	3	4	5	3	4	4	5	4	4
60	4	4	4	4	3	4	4	4	4	4	4	4	5	4	5	5	5	4	4	3	4	5	3	4	3	4	4	3	4	4	3	4	3	5	4	5
61	3	3	3	3	3	3	4	3	4	2	4	4	4	5	3	4	4	3	4	1	2	1	4	3	3	3	3	3	4	5	3	5	3	5	3	2
62	4	3	2	2	4	2	4	4	3	2	3	1	4	3	3	3	5	3	3	1	3	2	3	4	1	2	2	2	3	2	2	3	1	2	3	2
63	5	4	3	3	3	3	4	4	5	4	5	4	4	5	5	4	5	4	4	4	4	3	4	4	4	5	4	4	4	4	5	5	3	5	4	3
64	4	3	3	2	3	1	2	2	3	3	3	4	3	3	3	2	1	2	2	2	2	1	2	3	1	3	3	1	3	3	2	2	1	4	2	3
65	5	5	5	5	3	5	4	3	5	5	5	5	4	5	4	3	5	4	3	3	4	5	4	5	4	5	5	5		3	5	5	4	5	4	3

VARIABLE ADMINISTRACION DE TECNOLOGIAS DE INFORMACIÓN

	VARIABLE INDEPENDIENTE: ADMINISTRACION DE TECNOLOGIAS DE INFORMACION																																	
Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
66	5	5	4	5	1	5	5	5	5	5	5	5	4	5	5	4	5	5	5	5	5	5	5	5	2	5	5	5	4	5	5	5	5	5	5	5
67	3	4	3	4	3	3	4	3	3	2	4	4	4	4	4	4	2	4	2	1	2	1	3	3	2	3	2	2	2	4	3	3	2	5	3	3
68	4	4	3	3	3	4	3	3	3	1	1	4	5	1	3	3	3	3	4	2	4	4	5	4	3	3	4	4	3	4	2	2	1	1	1	5
69	5	5	4	4	3	4	4	4	4	3	5	5	5	4	4	4	5	4	4	3	5	4	4	4	4	3	5	3	4	5	5	4	4	5	4	4
70	5	5	4	5	3	5	3	4	4	4	5	5	4	3	3	3	5	3	3	2	4	5	3	4	2	3	4	4	5	3	4	4	5	5	4	3
71	3	3	2	3	4	2	3	2	4	2	4	4	4	4	4	4	4	4	4	4	4	3	5	3	3	2	2	3	3	3	4	4	4	4	4	4
72	3	4	3	4	4	4	3	3	3	3	3	4	4	3	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	4	3	4	3	4	3	4
73	4	4	4	4	5	4	3	3	4	4	5	5	4	5	4	4	5	3	3	2	3	3	4	4	3	3	5	4	5	5	3	4	3	5	3	3
74	4	4	3	3	3	3	3	3	4	2	4	3	4	4	3	3	4	3	3	3	3	3	4	3	3	4	3	3	3	4	3	4	3	4	3	3
75	4	4	3	3	3	3	3	3	4	2	4	3	4	4	3	3	4	3	3	3	3	3	4	3	3	4	3	3	3	4	3	4	3	4	3	3
76	5	4	3	3	3	3	4	3	4	3	5	4	4	4	5	4	5	4	4	3	5	3	3	3	3	1	3	2	3	4	4	4	2	5	3	3
77	5	4	3	4	3	3	4	3	4	3	5	4	4	4	5	4	5	4	4	3	5	4	3	3	5	2	3	3	3	4	4	4	2	5	3	3
78	5	4	4	4	4	4	4	4	4	4	5	3	3	5	3	4	3	5	5	3	4	4	5	4	4	4	3	3	4	4	4	4	4	4	4	4
79	5	5	4	4	5	4	5	5	4	4	5	5	5	5	4	5	4	4	5	4	4	4	5	4	5	5	5	4	5	5	5	4	4	5	4	5
80	4	3	4	4	3	4	4	3	5	3	3	3	4	4	4	3	4	3	3	3	4	3	3	3	4	3	4	4	3	4	4	3	3	4	3	4
81	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	2	2	2	2	2	2	2	2	2	2	5	5	5	5	5	5
82	5	5	5	5	4	4	5	5	5	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
83	5	5	5	4	4	4	5	4	5	4	4	3	5	2	5	5	5	5	5	4	4	4	4	3	5	5	5	4	4	4	5	5	5	4	5	5
84	5	4	4	4	2	5	5	5	4	5	5	3	4	4	5	5	5	4	5	4	5	5	5	4	3	3	3	3	3	4	4	5	4	5	4	4
85	5	5	5	5	3	5	4	5	4	4	5	5	4	4	5	5	4	4	5	5	5	4	5	4	4	5	5	4	5	4	5	4	4	5	4	5
86	5	3	4	4	3	4	4	4	5	3	3	4	3	4	4	4	4	3	3	2	4	4	3	4	3	3	3	3	4	3	3	3	4	4	3	2
87	5	5	4	4	3	4	3	3	3	3	4	4	3	4	4	4	4	4	4	2	4	3	4	4	3	4	3	4	4	4	4	4	3	4	3	4

VARIABLE ADMINISTRACION DE TECNOLOGIAS DE INFORMACIÓN

Nro.	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36
88	4	3	4	3	3	4	4	3	3	3	4	2	3	4	3	4	3	4	3	1	2	1	5	4	2	3	2	2	4	3	3	4	4	4	2	2
89	5	4	4	4	2	4	5	5	5	4	5	5	5	5	5	5	5	4	3	3	4	4	5	4	4	4	5	4	4	5	5	4	4	5	5	5
90	4	4	4	4	5	3	3	4	4	3	4	4	3	3	5	3	5	3	3	3	3	3	4	3	3	3	4	3	3	4	3	4	3	5	4	4
91	5	5	5	4	3	5	4	5	4	3	4	5	4	4	5	5	5	4	5	4	5	5	5	4	3	4	5	5	5	4	4	4	5	5	5	5
92	5	5	5	5	4	4	4	4	3	4	3	4	3	4	3	3	4	3	4	3	3	4	4	4	3	4	5	4	4	5	4	5	4	5	3	4
93	5	5	5	5	5	5	5	5	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4
94	4	4	3	3	3	5	4	5	5	4	5	5	4	5	4	4	4	5	3	5	5	5	5	4	5	4	4	4	4	4	5	4	5	5	4	4
95	5	5	4	4	1	5	4	5	4	4	3	5	5	5	5	5	5	4	3	4	3	4	3	2	4	5	5	5	5	3	4	3	5	4	3	3
96	4	4	3	4	4	3	3	4	3	3	5	4	4	4	3	4	5	4	4	4	3	3	2	3	4	4	5	3	4	4	5	4	4	4	4	4
97	4	5	4	5	3	3	5	5	4	4	5	4	5	4	4	4	5	4	4	5	5	5	5	5	5	4	5	4	4	4	4	4	4	5	4	5
98	4	5	4	4	4	3	3	5	3	3	4	3	3	4	4	4	3	4	3	4	4	3	4	3	3	5	3	3	4	3	3	4	3	3	2	3
99	5	4	4	3	4	4	5	5	4	3	5	5	5	4	5	5	5	5	4	4	4	2	5	3	5	4	4	2	4	4	4	3	4	5	5	4
100	5	5	2	4	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	4	5	4	5	5	5	4	5	5	5	2	5	4	4	5	5	5
101	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	4	5	5	5	5	5	5	4	5	5	5	4	5	5	5	5	5	4	5
102	4	4	3	2	3	4	5	4	4	4	3	5	4	3	3	4	5	3	5	2	3	4	4	4	5	4	4	5	4	3	3	3	3	5	4	4
103	5	4	4	4	5	3	4	4	4	4	5	5	4	4	5	5	4	5	4	4	3	4	5	4	4	4	4	5	4	5	5	5	4	5	5	5
104	5	4	5	5	3	4	4	5	4	5	5	5	5	5	4	4	5	4	4	4	4	4	5	5	4	4	5	5	5	4	4	4	5	5	4	5
105	4	4	4	5	3	5	4	4	4	4	4	5	4	4	5	4	5	5	5	4	4	4	5	5	4	3	5	4	5	5	5	4	5	5	4	5
106	4	4	4	3	4	4	4	5	4	4	5	5	5	4	4	5	5	3	4	4	4	4	5	3	5	4	4	5	5	5	4	4	4	5	5	4
107	3	4	5	5	5	5	4	5	3	4	4	5	4	3	3	4	5	3	4	3	3	4	5	3	3	4	4	3	5	5	3	3	4	3	3	3
108	5	4	5	4	3	4	4	5	4	3	4	5	5	4	4	4	5	3	5	3	5	4	4	4	4	5	4	5	5	5	4	4	5	5	4	5
109	3	5	4	5	4	4	4	5	4	4	4	5	5	4	4	4	5	3	4	3	5	4	5	4	5	5	5	4	5	5	3	4	5	5	5	4
110	4	4	3	3	5	3	4	3	3	4	3	4	4	3	4	4	4	4	3	2	4	3	4	3	3	3	5	5	4	5	4	3	3	5	5	5

VARIABLE PROCEDIMIENTOS DE SEGURIDAD INFORMATICA

	VARIABLE DEPENDIENTE: PROCEDIMIENTOS DE SEGURIDAD INFORMATICA																											
Nro.	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54	P55	P56	P57	P58	P59	P60	P61	P62	P63	P64
1	5	5	4	3	5	5	4	3	5	5	5	5	4	5	3	4	3	3	4	3	4	5	5	5	3	4	5	4
2	4	4	3	3	4	3	2	3	4	3	3	3	4	4	4	3	4	3	3	3	4	4	4	3	5	4	3	4
3	3	3	4	4	4	3	4	3	2	3	4	4	3	3	3	4	3	4	4	4	3	3	3	4	4	5	4	3
4	5	5	4	5	1	5	4	5	5	5	5	5	5	2	4	5	2	4	2	4	5	5	5	5	4	5	4	5
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	4	3	4	5	5	5	5	5	5	5	4	4	5
6	5	5	4	5	1	5	4	5	5	5	4	5	4	1	3	4	4	2	2	2	5	5	4	4	4	5	3	2
7	5	5	3	4	4	5	5	5	5	5	4	3	5	3	5	3	5	5	5	5	4	5	4	4	4	5	4	5
8	5	4	5	5	5	5	5	5	5	4	5	4	4	4	3	5	3	5	5	5	4	4	5	5	3	2	2	5
9	5	4	5	5	5	5	5	5	5	5	4	5	3	4	3	5	3	5	5	5	5	5	4	4	3	3	2	5
10	5	5	3	5	5	5	5	5	5	3	4	3	5	3	3	4	3	4	3	5	4	5	5	5	4	4	3	5
11	5	5	4	4	5	5	1	4	5	5	3	4	4	3	3	4	3	4	4	3	5	4	4	4	3	3	3	5
12	5	3	5	3	5	5	5	5	5	5	5	5	3	3	1	4	3	4	5	4	5	5	5	5	3	3	2	5
13	5	3	5	3	5	5	5	5	5	5	5	5	3	5	1	4	3	5	2	2	5	5	5	5	3	3	2	4
14	5	5	4	3	4	4	4	4	5	5	4	3	3	3	4	3	4	3	4	4	4	3	3	3	4	5	4	4
15	5	5	4	4	4	5	4	4	5	5	4	4	4	4	3	4	3	4	4	4	3	4	4	4	4	4	4	4
16	5	4	4	4	5	5	4	4	5	5	4	4	4	4	2	4	2	4	4	4	4	4	4	4	2	3	3	4
17	3	2	2	3	3	4	2	2	3	2	2	2	3	2	3	3	2	2	2	2	2	2	2	3	3	3	3	3
18	5	5	4	4	5	5	4	5	5	4	4	4	4	4	4	4	3	3	4	4	5	5	5	5	2	4	2	4
19	3	5	1	1	3	3	3	3	3	3	2	2	2	2	4	3	3	2	2	2	3	2	2	3	4	5	5	5
20	4	3	2	2	3	2	2	3	4	4	3	3	2	2	3	4	4	3	2	1	2	3	3	2	3	4	4	4
21	4	5	3	3	5	5	4	5	5	5	4	3	3	3	5	4	2	3	3	3	3	4	4	4	3	5	5	5

VARIABLE PROCEDIMIENTOS DE SEGURIDAD INFORMATICA

	VARIABLE DEPENDIENTE: PROCEDIMIENTOS DE SEGURIDAD INFORMATICA																											
Nro.	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54	P55	P56	P57	P58	P59	P60	P61	P62	P63	P64
22	3	3	3	3	3	5	4	4	3	4	3	3	3	3	3	3	2	3	3	3	2	3	3	3	4	4	4	4
23	4	4	4	4	5	5	5	5	5	4	4	4	4	4	4	5	4	5	5	5	4	4	5	4	3	5	4	5
24	5	5	5	4	5	5	5	5	5	4	5	4	4	3	3	5	3	4	4	5	5	5	5	5	3	3	3	5
25	5	5	4	3	5	5	4	5	5	5	5	5	5	3	3	4	1	4	5	5	5	5	5	5	4	4	5	4
26	3	5	4	3	3	3	4	5	3	3	4	4	2	2	3	4	3	2	3	3	3	4	2	4	4	5	5	5
27	3	4	3	3	2	4	3	3	2	2	3	3	3	3	4	4	3	4	3	3	3	4	4	4	4	5	3	4
28	4	5	3	4	5	5	4	4	5	5	5	4	4	3	4	4	4	4	3	4	4	4	4	3	4	3	5	5
29	5	4	4	4	5	5	5	5	4	4	5	4	4	4	4	5	3	5	5	5	4	4	4	5	4	4	5	4
30	4	3	2	3	4	3	4	4	4	4	4	4	4	3	3	2	3	3	3	4	4	3	3	3	4	4	3	3
31	5	4	3	5	4	4	5	4	5	4	4	5	4	5	5	3	5	5	5	5	4	5	5	5	4	3	5	5
32	4	3	4	4	3	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3	3	4
33	4	3	3	3	3	3	3	4	4	4	4	3	3	3	3	4	4	3	2	3	2	3	3	3	3	4	4	4
34	4	5	5	4	5	5	5	5	4	4	5	5	4	5	4	5	4	5	4	4	4	4	5	4	4	4	5	5
35	5	4	3	3	4	5	4	4	5	5	4	5	5	4	2	4	3	4	4	4	4	4	4	4	2	3	3	5
36	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	4	4	5	5	5	2	5	2	5
37	5	5	4	3	3	5	4	4	4	4	4	4	4	3	3	4	3	4	4	3	3	4	4	3	3	3	4	4
38	4	3	4	3	5	1	4	4	4	4	3	4	3	3	4	5	3	4	3	3	4	3	4	3	3	4	3	3
39	5	4	3	4	5	4	5	5	5	4	5	5	5	5	5	5	3	4	4	4	5	5	4	5	5	4	4	5
40	4	4	4	3	4	4	4	4	4	4	4	4	4	4	3	5	4	5	4	4	4	5	4	5	3	3	3	5
41	4	4	4	3	4	4	4	5	4	4	5	4	3	4	3	4	3	4	4	4	4	4	4	5	4	4	3	4
42	4	4	5	4	5	5	3	5	4	4	4	4	3	4	4	3	4	3	3	4	4	3	4	3	3	3	3	5
43	4	4	3	3	5	5	4	4	5	4	3	4	4	3	3	3	4	4	4	3	3	3	4	4	3	3	2	4

VARIABLE PROCEDIMIENTOS DE SEGURIDAD INFORMATICA

	VARIABLE DEPENDIENTE: PROCEDIMIENTOS DE SEGURIDAD INFORMATICA																											
Nro.	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54	P55	P56	P57	P58	P59	P60	P61	P62	P63	P64
44	5	5	4	5	5	5	5	5	5	5	5	5	5	4	1	4	4	4	5	5	4	3	3	4	4	3	4	5
45	4	4	4	3	5	1	2	4	5	2	2	5	4	4	4	3	3	4	3	4	4	4	4	2	2	4	4	5
46	4	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
47	4	3	3	3	5	5	3	2	4	4	3	3	4	3	3	4	3	3	2	3	2	3	4	4	3	2	2	4
48	5	4	5	4	5	4	4	4	5	4	5	5	5	5	4	5	3	5	5	5	4	4	4	5	5	4	5	5
49	5	4	4	4	5	5	5	5	4	4	4	4	4	4	5	4	3	4	4	4	4	4	4	4	3	3	3	4
50	5	4	5	4	5	5	4	4	5	5	4	5	5	4	5	5	5	5	4	5	5	4	4	5	5	5	5	4
51	5	4	4	4	5	5	4	4	4	4	4	4	4	4	3	5	2	4	4	4	4	4	4	4	4	3	3	3
52	5	5	4	3	5	5	5	3	3	5	3	4	4	5	5	5	3	4	4	3	3	5	4	3	3	5	5	4
53	4	4	4	3	4	4	4	4	4	4	3	4	3	4	3	4	4	4	3	4	3	3	4	4	3	3	3	4
54	4	4	4	4	4	3	3	5	5	5	5	4	4	4	4	3	4	3	4	4	4	3	3	5	4	5	4	5
55	5	5	3	4	5	5	4	4	5	4	4	4	4	4	5	3	5	4	3	4	4	4	4	4	4	5	4	5
56	5	4	4	4	4	5	5	5	5	5	4	4	3	3	3	3	2	4	4	4	4	3	4	4	3	3	4	4
57	1	5	3	3	5	5	2	5	5	3	3	3	5	4	5	3	4	2	4	4	4	4	4	4	5	5	3	5
58	4	5	5	4	3	4	3	4	5	4	3	3	4	4	5	4	4	5	5	4	5	4	4	4	5	4	3	4
59	5	4	4	4	5	5	4	4	4	4	3	4	3	4	4	4	3	4	5	4	5	4	4	4	3	4	3	5
60	5	5	4	4	5	5	4	4	5	4	3	5	4	4	3	4	4	3	4	5	4	4	4	4	3	3	3	5
61	4	3	3	3	5	5	3	4	5	5	4	4	4	3	3	4	4	3	4	4	4	3	4	4	3	4	3	5
62	2	2	3	2	2	2	2	2	3	3	2	1	3	2	4	2	3	3	3	2	2	1	4	2	5	5	4	5
63	4	4	4	4	5	5	5	5	4	4	5	4	4	4	4	4	4	4	4	4	3	4	4	4	3	4	4	4
64	3	3	3	2	5	1	1	1	3	1	2	2	4	2	3	3	3	2	2	2	1	1	1	1	2	3	3	3
65	4	5	3	4	5	5	5	5	5	5	5	4	3	4	3	3	3	4	3	3	4	3	4	4	3	4	3	5

VARIABLE PROCEDIMIENTOS DE SEGURIDAD INFORMATICA

	VARIABLE DEPENDIENTE: PROCEDIMIENTOS DE SEGURIDAD INFORMATICA																											
Nro.	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54	P55	P56	P57	P58	P59	P60	P61	P62	P63	P64
66	5	5	4	4	5	5	4	5	5	3	4	4	5	4	4	4	2	3	4	4	5	4	4	4	5	5	4	5
67	3	3	3	2	5	5	1	1	3	2	2	2	5	4	4	3	2	3	2	4	4	2	3	3	2	3	2	3
68	5	4	3	4	4	5	4	5	5	3	4	4	5	4	4	4	3	3	4	4	5	3	4	4	5	4	4	5
69	5	4	4	4	5	5	4	3	4	4	4	4	5	3	2	4	3	3	4	3	4	3	4	5	3	3	2	5
70	5	3	4	4	5	5	5	5	5	3	3	2	3	3	2	3	4	5	5	3	5	3	4	3	3	3	2	4
71	4	3	3	3	3	3	3	2	4	4	4	4	4	4	4	4	4	3	4	4	3	3	3	3	3	3	3	3
72	4	4	4	4	4	4	4	4	4	3	4	4	3	4	3	3	4	4	4	4	4	4	3	3	4	4	4	4
73	5	4	3	3	5	5	3	3	5	5	3	3	4	3	2	4	3	3	3	3	3	3	4	3	4	2	4	3
74	4	4	3	3	4	4	3	3	4	4	3	3	3	3	3	4	2	3	4	4	3	3	3	4	3	3	3	4
75	4	4	3	3	4	4	3	3	4	4	3	3	3	3	3	4	2	3	4	4	3	3	3	4	3	3	3	4
76	5	4	4	4	5	5	3	3	5	4	4	4	3	3	3	4	3	3	4	3	3	4	3	3	4	4	4	3
77	5	4	4	4	5	5	3	2	5	4	3	3	3	4	3	4	2	3	4	4	3	4	3	3	4	5	4	4
78	4	4	4	4	5	5	4	4	4	5	3	3	3	3	4	4	4	4	4	4	4	4	4	5	4	3	3	4
79	5	5	4	4	5	5	5	5	5	5	5	5	4	4	2	5	3	5	5	5	5	5	5	5	3	2	3	5
80	4	3	2	3	2	4	4	4	4	4	4	3	4	5	2	4	4	3	4	3	3	2	3	4	4	3	2	4
81	5	5	4	4	4	4	4	5	4	4	4	4	4	4	4	4	2	4	5	5	4	4	4	4	5	5	5	5
82	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	2	5	5	5	5	5	5	5	3	3	2	5
83	5	5	4	5	4	5	5	5	5	4	4	5	5	5	2	5	5	5	5	5	5	5	5	5	5	5	4	4
84	5	5	4	4	5	5	5	4	4	5	5	4	4	4	3	5	4	5	3	5	3	4	4	5	3	4	2	5
85	5	4	4	4	5	5	4	4	5	5	5	5	4	4	4	4	3	4	4	4	4	4	5	5	4	4	5	5
86	4	3	4	3	5	5	4	4	5	4	4	3	4	3	3	4	3	3	4	4	4	4	4	4	3	2	3	4
87	4	4	4	3	4	5	3	3	4	4	3	4	3	4	3	4	3	4	3	4	3	4	4	3	4	3	3	4

VARIABLE PROCEDIMIENTOS DE SEGURIDAD INFORMATICA

Nro.	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54	P55	P56	P57	P58	P59	P60	P61	P62	P63	P64
88	4	5	3	3	5	1	4	3	3	3	3	1	2	3	4	4	4	3	3	5	3	3	3	4	3	3	3	4
89	5	5	4	5	5	5	4	5	5	4	4	3	4	4	3	4	4	5	5	4	4	5	4	5	3	2	2	5
90	5	4	4	3	5	5	4	4	5	5	5	4	3	4	3	4	2	3	4	5	4	4	3	4	3	3	2	4
91	4	4	5	4	4	4	5	4	4	5	5	3	4	5	3	4	3	3	5	3	4	4	4	4	3	3	2	4
92	5	5	1	5	3	5	5	3	3	3	4	4	4	3	4	3	4	3	3	3	3	4	4	4	3	3	4	5
93	5	5	5	5	5	5	5	5	5	5	5	5	1	5	1	4	2	5	5	5	5	5	4	5	2	1	2	5
94	4	3	4	3	5	5	5	5	5	5	4	4	4	3	3	5	4	4	3	3	4	3	4	4	3	3	4	4
95	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
96	4	4	3	4	5	4	5	4	5	5	4	4	5	5	5	4	5	4	5	5	5	4	5	4	3	5	3	4
97	4	5	4	3	5	5	5	3	5	5	5	5	5	5	3	4	4	3	4	3	4	4	5	5	3	4	4	4
98	4	4	4	3	4	4	2	3	4	4	3	3	4	4	4	4	4	3	4	3	4	4	4	4	5	4	4	4
99	3	4	4	4	4	4	4	3	4	3	4	4	3	4	3	4	3	4	4	4	4	3	3	4	4	5	4	4
100	5	5	4	5	4	5	4	5	5	4	5	5	5	4	4	5	4	4	2	4	5	4	5	5	4	4	4	5
101	5	5	5	5	4	5	5	4	5	5	5	4	5	5	3	4	4	4	5	5	4	5	5	5	5	4	4	5
102	5	5	4	5	3	5	4	5	4	5	4	5	4	3	3	4	4	3	4	2	5	5	4	4	4	5	3	4
103	4	5	3	4	4	5	4	5	5	5	4	3	5	4	5	3	5	5	5	5	4	5	4	4	4	5	4	3
104	5	3	5	5	5	4	5	5	5	4	5	4	4	4	5	5	3	5	4	5	4	4	5	5	3	3	4	5
105	4	4	4	5	5	5	4	5	5	5	4	4	3	4	3	5	3	5	4	5	5	4	4	4	3	3	2	4
106	4	5	3	5	5	4	5	5	5	3	4	4	5	3	3	4	3	4	3	5	4	4	5	5	4	4	3	5
107	5	4	4	4	5	5	3	4	5	5	3	4	3	3	3	4	3	4	5	3	5	4	4	5	3	3	3	5
108	5	4	3	3	4	5	5	5	5	5	5	4	3	3	2	4	3	4	5	4	4	5	5	5	3	3	3	4
109	3	3	5	3	5	5	4	5	5	5	5	4	3	5	3	4	3	5	2	3	5	5	5	5	3	3	3	4
110	5	5	4	4	4	4	3	4	5	5	4	3	4	3	4	3	4	3	4	5	4	3	3	4	4	5	4	5

APENDICE 07

ESQUEMA DEL ARTICULO CIENTIFICO

DECLARACIÓN JURADA

DECLARACIÓN JURADA DE AUTORÍA Y AUTORIZACIÓN

PARA LA PUBLICACIÓN DEL ARTÍCULO CIENTÍFICO

Yo, María Rosario Pérez Castillo, estudiante (x), egresado ( ), docente ( ), del Programa Maestría de Gestión Pública de la Escuela de Postgrado de la Universidad César Vallejo, identificado(a) con DNI 27727965, con el artículo titulado

"Administración de tecnologías de información en los procedimientos de seguridad informática"

Declaro bajo juramento que:

1) El artículo pertenece a mi autoría
2) El artículo no ha sido plagiada ni total ni parcialmente.
3) El artículo no ha sido autoplagiada; es decir, no ha sido publicada ni presentada anteriormente para alguna revista.
4) De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), autoplagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo.
5) Si, el artículo fuese aprobado para su publicación en la Revista u otro documento de difusión, cedo mis derechos patrimoniales y autorizo a la Escuela de Postgrado, de la Universidad César Vallejo, la publicación y divulgación del documento en las condiciones, procedimientos y medios que disponga la Universidad.

Lugar y fecha: Lima, 07 de octubre del 2016

Nombres y apellidos: María Rosario Pérez Castillo