RESUMEN – TRABAJO DE GRADO

AUTORES	JUNIOR ALEXANDER AREVALO PINEDA
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	ANDRÉS MAURICIO PUENTES VELASQUEZ
TÍTULO DE LA TESIS	ANÁLISIS DE RIESGOS ASOCIADO A LA IMPLEMENTACIÓN DE UNA POLÍTICA *"BRING YOUR OWN DEVICE"* EN LA EMPRESA INNOVA EN OCAÑA

RESUMEN
(70 PALABRAS APROXIMADAMENTE)

EL TRATAMIENTO DE LA INFORMACIÓN ABARCA ASPECTOS QUE VAN DESDE EL MANEJO DE DOCUMENTOS EN MEDIO FÍSICO COMO EL PROCESO DE ALMACENAJE Y RECUPERACIÓN CONOCIDO TAMBIÉN COMO PROCESO DE GESTIÓN DOCUMENTAL, HASTA LOS SISTEMAS DE INFORMACIÓN QUE TENGA LA ORGANIZACIÓN O SISTEMAS EXTERNOS A LOS QUE ESTÉ OBLIGADA A REPORTAR INFORMACIÓN, PASANDO POR ASPECTOS TAN IMPORTANTES COMO LA FORMA DE ALMACENAMIENTO DE LOS DATOS DIGITALES, MODELOS DE RESPALDO DE INFORMACIÓN.

CARACTERÍSTICAS

PÁGINAS: 67	PLANOS:0	ILUSTRACIONES:0	CD-ROM:1

ANÁLISIS DE RIESGOS ASOCIADO A LA IMPLEMENTACIÓN DE UNA POLÍTICA *"BRING YOUR OWN DEVICE"* EN LA EMPRESA INNOVA EN OCAÑA

AUTOR:

JUNIOR ALEXANDER AREVALO PINEDA

Trabajo de grado para Optar al título de Ingeniero de Sistemas, bajo la modalidad de monografia.

Director:

ANDRÉS MAURICIO PUENTES VELASQUEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERÍA DE SISTEMAS

PLAN DE ESTUDIOS INGENIERÍA DE SISTEMAS

Ocaña, Colombia Octubre de 2017

Agradecimientos

A mis padres por haberme proporcionado la mejor educación y lecciones de vida.

En especial a mi padre, por haberme enseñado que con esfuerzo, trabajo y consistencia todo se consigue.

A mi madre, por cada dia hacerme ver la vida de forma diferente y confiar en mis decisiones

De igual forma a mi tutor M.C. ANDRES MAURICIO PUENTES VELASQUEZ, que sin su ayuda y conocimientos no hubiese sido posible realizar este proyecto.

A mis compañeros de clase, con los que he compartido grandes momentos.

A mis familiares por su apoyo.

Índice

Lista de tablas

Lista de figuras

Resumen

Desde hace algunos años se está viviendo un fenómeno poco habitual en el entorno tecnológico. La tecnología más avanzada ya no está en las empresas, sino que es propiedad de los empleados. En casa tenemos el último ordenador, el último móvil, la conexión de mayor ancho de banda, más gigas de almacenamiento, correo ilimitado, videoconferencia, etc. Pero en el trabajo, en muchos casos, tenemos la sensación de que volvemos al pasado en lo que a tecnología se refiere. Este fenómeno es lo que se ha llamado "consumerización" de las TIC. Según Gartner, la consumerización de la TI será la tendencia más significativa que afectará a las TIC durante los próximos diez años.

El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas (Perafán Ruiz, 2014).

La más importantes, el BYOD (“Bring Your Own Device”) o “use su propio dispositivo”, hace referencia al uso de dispositivos personales (smartphones, tabletas, portátiles, discos USB) en el trabajo. Por lo que dicho fenómeno ha obligado a las empresas de Ocaña se vean en la necesidad de analizar los riesgos que se pueden presentar al implementar una a

políticas sobre BRING YOUR OWN DEVICE y así teniendo las cosas claras se tomen los correctivos necesarios para su prevención.

Introducción

Actualmente el mercado tecnológico se encuentra en una fase de globalización, modernización y alta competitividad en productos y servicios, lo que ha traído consigo una avalancha de equipos tecnológicos cada vez más potentes y con mayores capacidades de almacenamiento, como los computadores personales, teléfonos inteligentes, tablet, entre otros. Mediante de la investigación que se desea ejecutar se determinará el estado actual de la infraestructura, se analizaran los resultados para posteriormente realizar unas políticas que ayuden a mitigar o prevenir cualquier tipo de inconveniente que se pueda presentar en la incursión de esta nueva tendencia BYOD dentro de la empresa INNOVA OCAÑA.

La información es un activo valioso que puede impulsar o destruir su empresa. Si se gestiona de forma adecuada, le permite trabajar con confianza. La gestión de la Seguridad de la Información le ofrece la libertad para crecer, innovar y ampliar su base de clientes sabiendo que toda su información confidencial seguirá siéndolo. De igual forma los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio. (BSI, 2016)

El motivo principal de la investigación en el análisis de riesgos de la seguridad de los dispositivos personales(laptops)en la empresa INNOVA ocaña, ya que estas empresas no cuentan con unas políticas de seguridad de la información ni planes de contingencia ni protocolos de seguridad que les permitan brindar una seguridad óptima y oportuna de la

información, la ubicación y el análisis de riesgos y vulnerabilidades en determinados sectores donde se crea que más deficiente los casos de funcionamiento interno de las empresas INNOVA OCAÑA .

De otra parte en la monografia se encuentra el primer capitulo donde se expone el planteamiento del problema, justificación, objetivos a lograr dentro de la investigación y delimitaciones que se tienen, posteriormente en el capitulo dos, se encuentra las referencias historicas, teoricas, conceptuales, contextuales y legales.

Por ultimo en el capítulo tres se evidencia el diseño metodologico, con el tipo de investigacion, poblacion, muestra, e intrumento de recoelccion de información, en el capítulo cuatro se desarrollaron cada uno de los objetivos especificos, exouestos en el primer capitulo, dando estos como resultados el capitulo cinco con conclusiones de cada uno de los objetivos y el seis donde se hacen las respectivas recoemndaciones de la monografia.

Capítulo 1. Análisis de riesgos asociado a la implementación de una política “bring your own device” en la empresa Innova en Ocaña.

1.1 Problema de Investigación.

En la actualidad diferentes entidades pertenecientes al sector público como la empresa INNOVA ocaña, han incursionado en la tendencia (BYOD), permitiendo el uso de dispositivos personales de almacenamiento masivo a sus trabajadores.

Mediante el estudio que se desea realizar sobre el uso BYOD, para medir el impacto que está generando esta nueva tendencia tecnológica en nuestro entorno específicamente en la empresa INNOVA Ocaña, por esto se hace relevante hacer primero un estudio previo para saber si esta tecnología tiene un impacto positivo o negativo dentro de esta institución, ya que esta nueva tecnología se presta para que las personas generen mejores ambientes de trabajo, pero por otro lado, se presume que existen riesgos de seguridad de la información asociados a esa tendencia BYOD que no han sido evaluados adecuadamente.

1.2 Formulación de la Pregunta de Investigación.

¿ Con el análisis de riesgos asociado a la implementación una política “bring your own device”en la empresa innova ocaña Se mejorará la seguridad de la información?

1.3 Objetivo

1.3.1 General. Analizar los riesgos asociados a la implementación de una política "BRING YOUR OWN DEVICE" en la empresa INNOVA ocaña, para recomendar unos controles que permitan mitigar el riesgo al máximo y mejorar la efectividad y seguridad de la empresa.

1.3.2 Específicos. Analizar los problemas de seguridad asociados al uso de dispositivos externos en las empresas dedicadas a innovaciòn.

Diagnosticar las condiciones de uso de dispositivos electrónicos en la empresa INNOVA

Documentar un conjunto de buenas prácticas para la adopción segura de la política BYOD

1.4 Justificación.

Las empresas que pertenecen al sector público y las personas que laboran en ellas hoy en día cuentan con una infraestructura tecnológica en crecimiento, ya que ahora es más fácil encontrar a personas que trabajan en entidades públicas con equipos electrónicos y dispositivos móviles de alta gama, es por ello que algunos empleados se sienten más cómodos trabajando en los equipos de su propiedad llámese Smartphone, Tablet o computadora portátil (laptop).

La tendencia BYOD se introdujo en las empresas, gracias a la facilidad que se tiene para adquirir dispositivos electrónicos con especificaciones técnicas muy potentes, llámese a estos dispositivos Smartphone, Tablet, o laptops. Esto a su vez llevó a las personas a utilizar sus propios dispositivos como herramientas de trabajo, en casos donde los dispositivos propios superan las características de la infraestructura tecnológica que ofrece la empresa, dada esta tendencia es indispensable crear una política que la regule y mitigue los riesgos que la misma puede generar de forma negativa en las empresas.

La empresa INNOVA Ocaña, es una empresa que sirve de referente de estudio, pues pertenece al sector público y es notable la utilización de equipos de cómputo personales para el desarrollo de labores y tareas propias de la empresa y de estudio, es decir que en la empresa INNOVA Ocaña, se hace evidente la tendencia (BYOD), esto permitirá usar dicha entidad como referente para plantear políticas respecto al tema de seguridad que se está tratando.

Por esto mismo es que requiere descentralizar los procesos de información, y crear políticas y establecer estándares de seguridad, ya que estos se encuentran sujetos a todas las tecnologías y administración que funcionan en las empresas.

La información en gran parte se encuentra en los equipos de cómputo de fácil acceso que son vulnerabilidades en las dependencias, las cuales no cuentan con protocolos de seguridad ni planes de contingencia mínimos para el cuidado protección y conservación de la información en caso de cualquier eventualidad como (malware), o robo de información por parte de los mismos integrantes del equipo de trabajo o de personas ajenas o de circunstancias

ambientales o externas, no hay planes de contingencia que puedan mitigar o resolver los inconvenientes que se puedan presentar ante cualquier circunstancia.

Garantizar la seguridad de la información en las empresas, es un tema muy serio y relevante y se debe tomar correctivos si se hace evidente que dicho activo se está poniendo en riesgo, es por ello que se hace necesario definir políticas frente a la tendencia (BYOD). Las políticas de seguridad en las empresas, facilitan la toma de decisiones y fortalecen las organizaciones, dado que dichas políticas establecen lineamientos, en pro del mejoramiento de un proceso, en este caso se busca mejorar la seguridad de la información, cuando dicha información está siendo utilizada en equipos de cómputo de carácter personal y cuyo manejo debe ser regulado por las empresas.

Capítulo 2. Marco Referencial

La estandarización Internacional comenzó en el campo electrotécnico: la Comisión Electrotécnica Internacional (IEC) fue establecida en 1906. Iniciando el trabajo en otros campos fue realizado por la Federación Internacional de la Organización Estandarizadora Nacional (ISA), que fue instalada en 1926. El énfasis dentro de ISA fue puesto pesadamente en la ingeniería industrial. Las actividades de ISA acabaron en 1942. En 1946, delegados de 25 países se reunieron en Londres y decidieron crear una nueva organización internacional, de la cual el objeto sería "facilitar la coordinación y la unificación internacional de estándares industriales". La nueva organización, ISO, comenzó oficialmente operaciones el 23 de febrero de 1947. (Castro Toro, 2010)

De otra parte por eso mismo, el Ministerio TIC está profundizando en elementos que permitan entender la realidad frente al proceso de implementación de SGSI en el Estado. Se debe forjar una línea base sobre cuáles son los motivadores, inhibidores, actores, resultados, entre otros aspectos, que cada entidad afronta en el camino hacia la seguridad de la información. Para tal fin, se ha contratado un estudio para "conocer cuál es el estado actual de adopción y apropiación de los SGSI en las entidades del Estado, del orden nacional y territorial". (Ministerio de las TICs, 2016)

La implantación de un programa de BYOD involucra que los empleados utilicen sus propios equipos de cómputo, para llevar a cabo trabajos encomendados por las personas a cargo de las diferentes empresas del sector público, a través de acceso local o remoto a la intranet de

la organización. Uno de los objetivos de un programa de BYOD es permitir al empleado ser más productivo y eficiente mediante la selección del equipo que mejor se adapte a sus preferencias y necesidades de trabajo, mientras que al mismo tiempo se garantiza la integridad de datos y la protección de fugas de información. El uso de un equipo portátil (laptop) de propiedad de los empleados en el lugar de trabajo se diferencia del uso de un equipo (laptop) corporativo, de dos maneras (Occ mundial.com, 2017).

La primera es la propiedad: mientras que un equipo corporativo es propiedad de la organización que lo emite, un dispositivo BYOD, es propiedad del empleado. Esta diferencia en la propiedad resulta en una diferencia en usos entre los dos tipos de dispositivos. Debido a que un equipo (laptop) corporativo es propiedad de la organización, no necesariamente existiría una política que prohíbe o restringe los usos no relacionados con el trabajo. Por otro lado, debido a que un BYOD es propiedad del empleado y no de la organización en la que él trabaja, se puede suponer, si no se indica explícitamente en la política, que el empleado va a utilizar el equipo (laptop) para uso personal, además de trabajo.

La segunda manera gira en torno a que esta situación de BYOD donde se utiliza un dispositivo para fines personales y de trabajo, significa que dos tipos de información fluirán a través del equipo (laptop), las cuales requerirán una protección adecuada por parte de la organización que emplea a la persona que utiliza un BYOD. Por un lado, el dispositivo probablemente tendrá acceso a la información personal de los clientes de la organización, es decir, aquellas personas con las que la organización ha interactuado y en el que ha recogido de manera legítima y se usa la información personal. Por otro lado, el dispositivo también podrá

contener información personal sobre el empleado a quién pertenece el dispositivo, así como tal vez allegados al empleado, por ejemplo, otras personas importantes, miembros de la familia, amigos, etc.

2.1 Antecedentes.

El objetivo de las siguientes observaciones es dar una pequeña orientación al lector, puesto que resulta imposible en la extensión acotada de este artículo evaluar y emitir un juicio objetivo y exhaustive sobre cada una de las tecnologías implicadas en este entorno del mundo BYOD. En todo caso se recomienda al lector que repase el nº 96 de la revista SIC –páginas 68 a 74– del artículo titulado "La gestión segura de la movilidad". El citado texto explica muy bien algunas de las cosas que se tendrían que pedir a un fabricante.

Si bien es cierto que el cuadrante de MDM ha cambiado e incluso hay jugadores con destacadas referencias que han desaparecido del cuadrante de Gartner, se han producido compras como, por ejemplo, la adquisición de Zenprise por parte de Citrix (este último incorpora toda su experiencia en el mundo de la virtualización de escritorios y aplicaciones y un excelente Security Container –a la altura de otros jugadores– con la provisión de tecnologías como WorkWeb (navegación segura) Workmail (correo-e, calendario y contactos), ShareFile (Follow-me Data), GotoMeeting (herramientas de colaboración), Podio (red social corporativa). Good sigue siendo un gran referente para aquellos clientes que quieren adoptar una tecnología rápida y eficiente de SandBox "pura", sobre todo porque ha solventado sus problemas de compatibilidad con los aplicativos en la nube, como Office 365, Google Apps, SalesForce y otros "excepto por

el precio desproporcionado" de la licencia perpetua y su correspondiente mantenimiento, que no ayuda a los proveedores de servicios e con Android. Los jugadores que vienen del mundo MDP tienen la ventaja de aportar una consola centralizada y un único agente para muchas de sus disciplinas (Saro Luna & Fernández Martín, 2013).

Una mención a Sophos, que ha acertado de lleno con su política de implementar una licencia única de punto final, y que licencia por usuario y no por dispositivo (independientemente del número de estos), logrando una solución interesante; y aunque no incorpora de forma estricta un Sandbox, se puede determinar si podemos trabajar con su visión de repositorios corporativos / incorporar otra solución complementaria del mercado (por ejemplo, Fixmo, que sería válido para este y otros jugadores).

También merece la pena comentar que parece una solución muy equilibrada. Otros jugadores están realizando esfuerzos destacables, y entre ellos se encuentra Trend Micro, con una magnífica suite con una interesante relación calidad precio (precisamente BlackBerry les ha elegido como solución anti-malware y la gestión de los problemas de la privacidad con aplicaciones de terceros). También es recomendable revisar la visión de Kaspersky, que ha ampliado su portafolio de solvents productos.

Respecto a los líderes del cuadrante de Gartner de MDM (Mobile Device Management), destaca MobileIron como número uno indiscutible en la teoría y en la práctica, con respecto al número de referencias nacionales e internacionales con su excepcional tecnología; pero el número dos, Airwatch, es el que está haciendo más ruido en el mercado y

provocando una verdadera guerra de precios a la baja (Saro Luna & Fernández Martín, 2013).

De otra parte para el año 2016 se afianzará el BYOD en las empresas un estudio de la consultora en tecnología Gartner estimó que para el año 2016 el 38% de las empresas dejará de proporcionar dispositivos móviles a sus empleados, afianzando la tendencia del "Bring your own device" (BYOD). Algunos empresarios todavía se muestran reticientes a implementar el BYOD. Algunos empresarios todavía se muestran reticientes a implementar el BYOD. Considerando que hoy en día un 81% de las personas laboralmente activas en el mundo utilizan algún tipo de dispositivo personal en el trabajo, las empresas se muestran cada vez más reticentes a proporcionar equipamiento tecnológico a sus empleados. De hecho, un estudio realizado por la consultora Gartner estimó que para el año 2016, un 38% de las compañías se sumará a la tendencia del BYOD (“Bring your own device”, por sus siglas en inglés) que exhorta a los trabajadores a utilizar sus propios smartphones o tabletas en sus oficinas (Universidad Colombia, 2013).

Según publica el portal Silicon News, los expertos de Gartner llegaron a esta conclusión a través de una encuesta aplicada entre directores de información (CIO) de organizaciones de todo el mundo. El estudio destaca, además, que en 2017 la mitad de los profesionales utilizará sus recursos personales para trabajar. Si bien la tendencia BYOD se está extendiendo en las grandes multinacionales del mundo, es más común entre las PYMES que encuentran mayor facilidad de control en su implementación.

Por otra parte, el análisis indica que aunque las empresas norteamericanas y europeas

tienen el doble de posibilidades de permitir la expansión del BYOD, son los empleados indios, chinos y brasileños los más propensos a utilizar un dispositivo propio en sus empleos. Además, los expertos estiman que la próxima irrupción en el mercado de los nuevos terminales móviles que buscan mayor comodidad en el usuario, Como es el caso del smartwatch, contribuirá aún más a impulsar la tendencia del uso de equipos propios en el ámbito profesional futuro (Universidad Colombia, 2013).

La creciente tendencia de "traiga su propio dispositivo" (BYOD) se ha documentado bien. Nuestra investigación anterior sobre BYOD, en la que entrevistamos a cerca de 4900 líderes de negocios y responsables de la toma de decisiones de TI en nueve países, reveló que un impresionante 89 por ciento de las empresas permite que sus empleados usen sus propios dispositivos, específicamente, dispositivos móviles como computadoras portátiles, Smartphone y tabletas, con fines laborales (Cisco IBSG Horizontes, 2013).

No obstante, recientemente, ha habido escepticismo con respecto a los beneficios que las empresas pueden esperar al adoptar BYOD. Las empresas enfrentan un dilema. Los ejecutivos y trabajadores con conocimiento desean usar los dispositivos, las aplicaciones y los servicios de nube que elijan y están demandando acceso a la red corporativa y soporte de TI. Las empresas los están complaciendo, pero no están seguras de sí BYOD vale los riesgos y costos (Cisco IBSG Horizontes, 2013).

El Grupo de soluciones empresariales para Internet (IBSG) de Cisco, la práctica de asesoramiento global de la empresa, realizó un análisis financiero detallado para entender la

totalidad de beneficios (y costos) de BYOD. Lo que concluimos fue extremadamente positivo, tanto para las empresas como para los empleados.

Información pública de Cisco:

Grupo de soluciones empresariales basadas en Internet

Este estudio es la tercera etapa de la investigación de Cisco IBSG Horizons sobre BYOD. En junio de 2012, encuestamos a 600 responsables de la toma de decisiones de TI en empresas estadounidenses para determinar cuán frecuente es BYOD y de qué manera los departamentos corporativos de TI están manejando estos nuevos dispositivos en cuanto al soporte, el acceso a la red y la seguridad.

Cuando vimos el impresionante grado en que las empresas estadounidenses habían adoptado BYOD, ampliamos el estudio original para incluir ocho países adicionales en tres regiones e incluimos empresas medianas. Publicamos esos resultados en septiembre de 2012.

Esta es la tercera etapa de nuestras investigaciones y análisis, diseñada para ayudar a las empresas a entender los costos y beneficios financieros de la implementación de BYOD. Comenzamos con datos de nuestra investigación anterior y luego realizamos investigaciones adicionales en seis países (Estados Unidos, Reino Unido, Alemania, Brasil, India y China) para informar nuestro análisis.

Figura 1. Etapas del studio IBSG

Fuente. Cisco IBSG © 2013 Cisco y/o sus filiales.

2.2 Marco conceptual.

La creciente tendencia de “traiga su propio dispositivo” (BYOD) se ha documentado bien. Nuestra investigación anterior sobre BYOD, en la que entrevistamos a cerca de 4900 líderes de negocios y responsables de la toma de decisiones de TI en nueve países, reveló que un impresionante 89 por ciento de las empresas permite que sus empleados usen sus propios dispositivos, específicamente, dispositivos móviles como

computadoras portátiles, Smartphone y tabletas, con fines laborales (Occ mundial.com, 2017).

No obstante, recientemente, ha habido escepticismo con respecto a los beneficios que las empresas pueden esperar al adoptar BYOD. Las empresas enfrentan un dilema. Los ejecutivos y trabajadores con conocimiento desean usar los dispositivos, las aplicaciones y los servicios de nube que elijan y están demandando acceso a la red corporativa y soporte de TI. Las empresas los están complaciendo, pero no están seguras de si BYOD vale los riesgos y costos (Occ mundial.com, 2017).

El Grupo de soluciones empresariales para Internet (IBSG) de Cisco, la práctica de asesoramiento global de la empresa, realizó un análisis financiero detallado para entender la totalidad de beneficios (y costos) de BYOD. Lo que concluimos fue extremadamente positivo, tanto para las empresas como para los empleados.

Este estudio es la tercera etapa de la investigación de Cisco IBSG Horizons sobre BYOD.

En junio de 2012, encuestamos a 600 responsables de la toma de decisiones de TI en empresas estadounidenses para determinar cuán frecuente es BYOD y de qué manera los departamentos corporativos de TI están manejando estos nuevos dispositivos en cuanto al soporte, el acceso a la red y la seguridad.

Cuando vimos el impresionante grado en que las empresas estadounidenses habían adoptado BYOD, ampliamos el estudio original para incluir ocho países adicionales en tres

regiones e incluimos empresas medianas. Publicamos esos resultados en septiembre de 2012.

Esta es la tercera etapa de nuestras investigaciones y análisis, diseñada para ayudar a las empresas a entender los costos y beneficios financieros de la implementación de BYOD.

Comenzamos con datos de nuestra investigación anterior y luego realizamos investigaciones adicionales en seis países (Estados Unidos, Reino Unido, Alemania, Brasil, India y China) para informar nuestro análisis.

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. (Sanso, 2011)

Sistema de Gestión de Seguridad de la Información (SGSI). SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la

forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (Vargas, 2016)

El riesgo es aquello que puede acontecer en un futuro, más o menos cercano, y que preocupa por sus consecuencias porque está siempre presente en cualquier actividad que se realice. Pero no sólo tiene una vertiente negativa, relacionada con pérdidas económicas o daños físicos, o morales; también puede entenderse desde su lado positivo cuando la exposición a determinados riesgos permite obtener ganancias (por ejemplo, al arriesgar en una apuesta para ganar dinero, o al invertir en un determinado negocio para conseguir unos beneficios futuros).

Vulnerabilidad. En este contexto, la vulnerabilidad puede definirse como la capacidad disminuida de una persona o un grupo de personas para anticiparse, hacer frente y resistir a los efectos de un peligro natural o causado por la actividad humana, y para recuperarse de los mismos. Es un concepto relativo y dinámico. La vulnerabilidad casi siempre se asocia con la pobreza, pero también son vulnerables las personas que viven en aislamiento, inseguridad e indefensión ante riesgos, traumas o presiones. (Federación Internacional de Sociedades de la Cruz Roja, 2010)

Amenazas. Una amenaza es un fenómeno o proceso natural o causado por el ser humano que puede poner en peligro a un grupo de personas, sus cosas y su ambiente, cuando no son precavidos. Existen diferentes tipos de amenazas. Algunas son naturales, otras son provocadas

por el ser humano, como las llamadas industriales o tecnológicas (explosiones, incendios y derrames de sustancias tóxicas). Las guerras y el terrorismo también son amenazas creadas por el ser humano. (Unisdr, 2004)

2.3 Bases teóricas.

La gestión de riesgos implica conocer algunas definiciones que amplíen los conocimientos sobre el tema. A continuación se definen de manera clara y sencilla los términos relacionados con la gestión del riesgo.

Bring Your Own Device (BYOD), cuya traducción sería “trae tu propio dispositivo”, hace referencia a una tendencia que se está generalizando cada vez más en el ámbito empresarial, en la cual los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos (ordenadores portátiles, Smartphone y tabletas) para acceder a los recursos de su compañía.

¿Y cómo se ha producido la generalización de este fenómeno? Hasta hace algunos años, lo más habitual era que las empresas estuviesen tecnológicamente mejor equipadas que los usuarios. Por ejemplo, muchas personas no tenían ordenador en casa, pero sí en la oficina, y lo más frecuente era que quien disponía de un portátil o un teléfono móvil tuviese estos dispositivos porque se los había proporcionado su compañía. Sin embargo, los avances en la tecnología de consumo han invertido esta tendencia y, hoy por hoy, es más habitual que los usuarios dispongan de tecnología más avanzada, productiva y eficaz que la que pone a su disposición la propia empresa.

BYOD tiene ventajas e inconvenientes que te contamos un poco más adelante. Implica, por un lado, la redefinición de gran parte de los procesos y métodos de trabajo y, por otro lado, la revisión y adaptación de los protocolos de seguridad en las redes empresariales.

Figura 2. Busqueda del equilibrio

Fuente. SACA 2013 - Bring Your Own Device

AS/NZS 4360:1999 – Administración de Riesgos. En el Estándar Australiano AS/NZS 4360:1999, La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.

ISO 27000. La norma ISO/IEC 27000 es un estándar que propone un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información, con un enfoque basado en procesos. La

norma define los controles que deben implementarse para la adopción de un sistema de seguridad pero no indica cómo; la ISO 27001:2013 es una norma certifiable (International Organization for Standardization, 2013) que tiene como principales objetivos:

Establecer un marco metodológico para un SGSI, la adopción de controles proporcionales a los riesgos percibidos, la documentación de políticas, procedimientos, controles y tratamiento de riegos, identificación y asignación de responsabilidades al nivel adecuado, formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica, generación y preservación de evidencias, tratamiento de los incidentes de seguridad, revisión y mejora continua del SGSI y gestión de Riesgos (Valencia Duque, 2017)

Tabla 1.

Ciclo Deming (PHVA) aplicado a la Norma ISO/IEC 27.001

CICLO PHVA	PROCESOS
Planificar (*Plan*)	Establecer el contexto. Alcance y Límites Definir Política del SGSI
	Definir Enfoque de Evaluación de Riesgos Identificación de riesgos
	Análisis y Evaluación de riesgos
	Evaluar alternativas para el Plan de tratamiento de riesgos
	Aceptación de riesgos
	Declaración de Aplicabilidad

Tabla 1. (Continuación)

	Implementar plan de tratamiento de riesgos
	Implementar los controles seleccionados
acer (*Do*)	Definir las métricas
	Implementar programas de formación y sensibilización
	Gestionar la operación del SGSI
	Gestionar recursos
	Implementar procedimientos y controles para la gestión de incidentes de seguridad
Verificar (*Check*)	Ejecutar procedimientos de seguimiento y revisión de controles.
	Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI.
	Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.
	Revisión periódica de la evaluación de riesgos.
	Realización de auditorías internas
	Revisión de alcance y líneas de mejoras del SGSI por la Dirección.
	Actualización de los planes de seguridad
	Registro de acciones que podrían impactar la eficacia y/o eficiencia del SGSI

Tabla 1. (Continuación)

Actuar (*Act*)	Implementación las mejoras identificadas para el SGSI
	Implementación de las acciones correctivas y preventivas pertinentes. Comunicación de acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

Fuente. Norma ISO/IEC 27001

Los lineamientos metodológicos y los requerimientos de la norma ISO/IEC 27001 son propuestos bajo el enfoque metodológico del Ciclo de Deming: Planificar, Hacer, Verificar, Actuar.

Esta Norma Internacional está diseñada para que las organizaciones la utilizan como referencia para la selección de los controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO / IEC 27001, o como un documento de orientación para las organizaciones que efectúan controles de seguridad de la información generalmente aceptados. Esta norma también se destina para su uso en la elaboración de directrices de gestión de seguridad de la industria y organización específica de información, teniendo en cuenta su entorno específico de riesgos de seguridad de la información. (International Standard, 2013). La versión 2013 del estándar describe los siguientes catorce dominios principales:

Dominio 5 Políticas de seguridad de la información

5.1 Dirección de gestión de seguridad de la información

Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.

Las políticas de seguridad de la información

Control un conjunto de políticas de seguridad de la información debe ser definido, aprobado por la administración, publicar y comunicar a los empleados y colaboradores externos.

rio, utilizando los procedimientos formales.

Dominio 9 Control de Acceso

9.1 Los requisitos de negocio de control de acceso

Objetivo: limitar el acceso a las instalaciones de procesamiento de la información y de la información.

Política de control de Acceso. Control

Una política de control de acceso debe ser establecida, documentado y revisado basado en los requisitos de seguridad de negocios y de información (Valencia Duque, 2017).

El acceso a las redes y servicios de red. Control

Los usuarios sólo deben contar con acceso a los servicios de red y de la red que han sido autorizados específicamente para su uso.

Gestión de acceso de Usuario. Objetivo: Garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas y servicios.

Registro de usuarios y de la matrícula. Control

Un proceso formal de registro de usuario y la cancelación del registro debe ser implementado

para permitir la asignación de derechos de acceso.

Responsabilidades del usuario

Objetivo: hacer que los usuarios responsables de salvaguardar su información de autenticación.

Uso de la información secreta de autenticación

Control

Los usuarios deben ser obligados a seguir las prácticas de la organización en el uso de la información autenticación secreta.

Sistema de control de acceso y aplicación

Objetivo: Para prevenir el acceso no autorizado a los sistemas y aplicaciones (Saro Luna & Fernández Martín, 2013).

Restricción de acceso de Información. Control

El acceso a las funciones de información y sistema de aplicación debe limitarse de acuerdo con la política de control de acceso.

Los procedimientos de registro-en seguros. Control

Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de conexión segura.

Sistema de gestión de contraseña. Control

Sistemas de gestión de contraseña deben ser interactivos y deben asegurarse de contraseñas de

calidad.

Dominio 10 Criptografía

Controles criptográficos

Objetivo: garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, privacidad y / o integridad de la información.

Política sobre el uso de controles criptográficos. Control

Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.

Gestión de claves. Control

Una política sobre el uso, la protección y la duración de las claves de cifrado debe ser desarrollada e implementada a través de todo su ciclo de vida (Valencia Duque, 2017).

Dominio 11 La seguridad física y ambiental.

Las áreas seguras

Objetivo : Para prevenir el acceso no autorizado física , daño e interferencia a la información y sus instalaciones de procesamiento de la organización.

Perímetro de seguridad física

Control

Perímetros de seguridad deben ser definidas y utilizan para proteger áreas que contienen información y procesamiento de la información, ya sea instalaciones sensibles o críticos.

Controles de entradas físicas

Control

Áreas seguras deben ser protegidas por los controles de entrada adecuados para garantizar que se permite el acceso sólo el personal autorizado.

Equipos

Objetivo: Para evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

Ubicación de Equipo y protección

Control

El equipo debe estar ubicado y protegido para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado (Saro Luna & Fernández Martín, 2013).

Utilidades de apoyo

Control

El equipo debe ser protegido de fallas de energía y otros trastornos causados por fallas en el apoyo a los servicios públicos.

Seguridad de Cableado

Control

Energía y telecomunicaciones cableado que transporta datos o apoyar los servicios de información debe ser protegida de intercepción, interferencia o daño.

Mantenimiento de equipo

Control

El equipo debe mantenerse correctamente para asegurar su disponibilidad e integridad continua.

Controles contra el malware

Control

Detección, prevención y recuperación de controles para proteger contra el malware debe ser implementado, en combinación con el conocimiento del usuario apropiado.

Copia de seguridad

Objetivo: Para evitar la pérdida de datos (Valencia Duque, 2017).

Información de copia de seguridad

Control

Las copias de seguridad de la información, software y sistemas de imágenes deben ser tomadas y analizadas regularmente de acuerdo con una política de copia de seguridad convenidas.

Registro y supervisión

Objetivo: registrar eventos y generar evidencia.

Control del software operativo

Objetivo: garantizar la integridad de los sistemas operativos.

Controles de red

Control

Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

Seguridad de los servicios de red

Control

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red, si estos servicios son prestados en la empresa o subcontratados (Saro Luna & Fernández Martín, 2013).

La segregación en las redes

Control

Grupos de servicios de información, los usuarios y los sistemas de información deben ser segregados en las redes.

Transferencia de Información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Políticas y procedimientos de transferencia de información

Control

Formales de transferencia de políticas, procedimientos y controles deben estar en su lugar para

proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación (Saro Luna & Fernández Martín, 2013).

Por ultimo se debe decir que el tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas (Perafán Ruiz, 2014).

La información es un activo valioso que puede impulsar o destruir su empresa. Si se gestiona de forma adecuada, le permite trabajar con confianza. La gestión de la Seguridad de la Información le ofrece la libertad para crecer, innovar y ampliar su base de clientes sabiendo que toda su información confidencial seguirá siéndolo. De igual forma los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio. (BSI, 2016)

2.4 Marco legal.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” (Congreso de Colombia, 2016).

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos (Congreso de Colombia, 2016).

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos” que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad

de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones". El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga 5el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor (Congreso de Colombia, 2016).

Artículo 269 C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269 D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2016).

Artículo 269 F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus

empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

Artículo 269 G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito (Congreso de Colombia, 2016).

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

Por servidor público en ejercicio de sus funciones

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

Revelando o dando a conocer el contenido de la información en perjuicio de otro.

Obteniendo provecho para si o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales (Congreso de Colombia, 2016).

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos, así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal. Por su parte, el capítulo segundo establece:

Artículo 269 I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

Artículo 269 J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2016).

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa .

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea (Congreso de Colombia, 2016).

Ley 1273 del 5 de enero de 2009. El Congreso de Colombia decretó: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." (Congreso de Colombia, http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf, 2015)

Ley 1581 del 17 de octubre de 2012. El Congreso de Colombia decretó que esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política de Colombia; así como el derecho a la información consagrado en el artículo 20 de la misma. (República de Colombia, Ley 1581 de 2012, 2012)

Guía GTC 137 Gestión de Riesgos – Vocabulario. Esta norma suministra las definiciones de términos genéricos relacionados con la gestión del riesgo. El objetivo es fomentar un entendimiento mutuo y consistente de la descripción de las actividades relacionadas con esta gestión, así como un enfoque coherente de ésta, así el uso de terminología de gestión de riesgo uniforme en los procesos y los marcos de referencia relacionados con la gestión del riesgo.

Esta guía está destinada para el uso por parte de:

Aquellos involucrados en la gestión de riesgos.

Aquellos involucrados en actividades de ISO, IEC, y

Aquellos a cargo de desarrollar normas, guías, procedimientos y códigos de práctica nacionales o específicos del sector relacionados con la gestión del riesgo (Instituto Colombiano de Normas Tecnicas y Certificación, 2011).

Capitulo 3. Metodología de la Investigación

Para comenzar el desarrollo de este proyecto BYOD, se empezó por describir y conocer las características esenciales tales como el sitio de trabajo y las personas que laboran y el tipo de dispositivo que utilizan y los servicios para determinar cuales serian las mejores estudios para evaluar en esta empresa , los artefactos, roles y particularidades de cada uno, a partir de esto se comparó cada uno de estos métodos para concluir que tienen en común y definir cuál de sus características sería la mejor al momento de crear un nuevo método, luego se definió el método y fue evaluado con la herramienta de análisis mediante el estudio de artículos científicos específicamente Gestión de la seguridad del dispositivo móvil y comparación para saber si cumple con los requisitos para ser un método ágil.

3.1 Tipo de Investigación.

En este proyecto se utilizó la investigación cuantitativa, ya que a través de esta metodología de investigación se podrá identificar las vulnerabilidades más evidentes de la empresa de la exacta artefactos y roles se podrán identificar las pautas a seguir para el desarrollo de una nueva metodología ágil, y de igual manera al definir la herramienta BYOD podremos validar la metodología creada.

3.2 Población.

La población que se tuvo en cuenta para la realización de este proyecto fue la empresa

innova ocaña, conformados por los empleados estudiantes y visitantes que pertenecen al sector públicos quienes son los que tienen acceso a esta nueva práctica, ya que estos son los principales actores en el uso de estos métodos, lo que permite conocer el grado de aceptación del método planteado.

3.3 Muestra.

Para el desarrollo de esta investigación se utilizó el muestreo cuantitativo, en el cual podemos evidenciar en el cual no se usa el azar, sino el criterio del investigador, quien define si la muestra es representativa o no; lo cual permitió escoger una muestra representativa para la investigación teniendo en cuenta la línea de profundización del encuestado. (Innovatec)

Para el caso de este proyecto el tamaño de la muestra fue el mismo que la población dado que las personas encuestadas están comprendidos en esta tabla.

3.4 Recolección de la Información.

La recolección de la información se hizo mediante encuestas.

3.5 Análisis de la información.

El cumplimiento de los objetivos propuestos, se realizó mediante una serie de actividades que se describen a continuación.

Tabla 2.

Actividades por objetivo

OBJETIVO ESPECÍFICO	ACTIVIDAD	INDICADOR
Diagnosticar la situación actual para la identificación de riesgos de la empresa innova ocaña.	Recopilar información utilizando como instrumentos de recolección la entrevista, análisis de material documental de la dependencia y observación. Analizar los factores de riesgo de la información suministrada en la recopilación de información.	Entrevista con funcionarios, estudiantes y visitantes.
Diagnosticar las condiciones de uso de dispositivos electrónicos en la empresa INNOVA ocaña	Estudiar la norma ISO 27002:2013 contemplando su estructura para la aplicación de la misma. Clasificar y evaluar los riesgos acorde a las actividades del proceso de gestión de riesgo de la seguridad de la información.	Análisis de resultados obtenidos en la aplicación de la norma. analizar los resultados conforme a estándares internacionales para una buena practica
Documentar un conjunto de buenas prácticas para la adopción segura de la política BYOD basado en la norma ISO 27002: 2013	Clasificar los controles correspondientes a cada riesgo tratado.	Tabla de controeles establecidos.

Fuente. Autor de la monografia

Capítulo 4. Presentacion de resultados

4.1 Análisis de los problemas de seguridad asociados al uso de dispositivos externos en las empresas dedicadas a innovaciòn.

Actividades para el cumplimiento del objetivo

Recopilar información utilizando como instrumentos de recolección la entrevista, análisis, observación.

Analizar los factores de riesgo de la información suministrada en la recopilación de información.

Realizando el reconocimiento en la empresa innova ocaña, se procede a realizar la recopilación de información por medio de encuestas, entrevistas lo que nos permite documentar la información y realizar el análisis para nuestra investigación.

A continuación se describe la información detallada de hallazgos encontrados.

Tabla 3.

Hallazgos encontrados

RESULTADO DEL ANÁLISIS DE LA INFORMACIÓN RECOPILADA		
ORGANIZACIÓN Y SEGURIDAD DE LA INFORMACIÓN		
Organización Interna		
Objetivo:	Gestionar la seguridad de la información y su organización dentro de la empresa INNOVA OCAÑA.	
	localización de la información dentro de la empresa	la empresa innova ocaña cuenta con un sistema de archivo de información inadecuada
GESTIÓN DE ACTIVOS		
Clasificación de la información		

Tabla 3. (Continuación)

Objetivo:	Asegurar que la información recibe el nivel de protección adecuado.	
	Manejo de la información	actualmente el manejo de la información se lleva de manera inadecuada
GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		
Reporte sobre los eventos y las debilidades de la seguridad de la información		
Objetivo:	Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.	
	Reporte sobre los eventos de seguridad de la información	Según la forma actual de manejo y búsqueda de información dentro de la empresa , se hace imposible garantizar los reportes de anomalías o pérdida de información.
SEGURIDAD FÍSICA Y DEL ENTORNO		
Áreas seguras		
Objetivo:	Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.	
	Controles de acceso físico a los equipos tecnológicos.	la empresa innova dentro de sus instalaciones no son seguras puesto que no están protegidas con controles de acceso apropiados.
CONTROL DE ACCESO		
Control de acceso a equipos		
Objetivo:	Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.	
	Gestión de usuarios contraseñas para usuarios.	La asignación de usuarios y contraseñas se debe realizar a través de un proceso formal de gestión ya que en la actualidad los equipos no cuentan en su totalidad con este tipo de restricción.

Fuente. Autor de la monografia

Mediante el estudio que se realizó en las empresas que trabajan con tecnología en el sector público se pudo evidenciar que estas no cuentan con ninguna clase de política ni de control por parte de la persona encargada de la administración de las redes ni mucho menos por el personal de seguridad. En estas empresas no se puede diferenciar una persona ajena a un empleado y si está utilizando equipos suministrados por las empresas o sus propios equipos

mucho menos que quienes están manipulando los estén haciendo de la manera correcta ya que en ninguno de los casos se restringe el acceso a ningún portal o sitio no deseado dando esto pie para el filtro o el robo de información la propagación de malware.

4.2 Diagnóstico de las condiciones de uso de dispositivos electrónicos en la empresa INNOVA.

Actividades para el cumplimiento del objetivo.

Estudiar el artículo de Gestión de la seguridad del dispositivo móvil

En Sectores de Infraestructura Crítica

Contemplando su estructura para la aplicación de la misma.

Clasificar y evaluar los riesgos acorde a las actividades del proceso de gestión de riesgo de la seguridad de la información.

Mediante el estudio y el análisis que se le realizó al artículo se pudo evidenciar muchos aspectos interesantes sobre el uso de los dispositivos, y a su vez también se pudo evidencian muchos controles por parte de las empresas para el buen uso de esta nueva tendencia dentro de las recomendaciones más relevantes podemos rescataar de este articulo.

Control de acceso: En este artículo nos recomiendan tener un doble control de acceso para en caso de cualquier eventualidad como pérdida o robo de información se pueda mediante la inicialización de una cuenta se pueda proceder a la función de cierre de la cesión en el equipo perdido o robado para mantener la integridad y protección de los datos. a esto también se le

puede añadir para mayor seguridad la utilización de actividades inusuales o en ubicaciones inusuales.

Firewall de la próxima generación: La instalación de detección de intrusiones IDS esto a nivel de políticas y protocolos para tener restricciones y aplicaciones en los puertos ataques amenazas desconocidas vulnerabilidades.

Mecanismos de control BYOD: Para tener un mejor control de los activos cuando los usuarios de BYOD se sugiere utilizar mecanismos implican esencialmente encriptación, desinfección de datos,Control de cumplimiento y control de configuración centralizado,esto hace referencia a que si un dispositivo BYOD se pierde o se lo roban este cifrado y su información esté protegida y forzar a quien tenga esta información a restablecer los valores de fábrica de los equipos.

Gestión y política de BYOD: Definir dentro de la organización cuáles son los factores de confidencialidad, integridad y disponibilidad esto con el fin de que no sean de acceso a todas las personas de la empresa

Tabla 4.

Identificación de riesgos

IDENTIFICACIÓN DEL RIESGO			
Identif. de activos		Identif. de amenazas	Identif. de Consecuencias
Procesos realizados	localización de la información dentro de la empresa	Pérdida de información	retraso en proyectos e investigaciones realizadas por la empresa
	deterioro de los equipos de la empresa	mal uso de los equipos	perdida de dinero y recursos de la empresa
	el personal que trabaja en las dependencias no cuenta con espacios ni equipos adecuados para su normal funcionamiento	hurto de equipos pérdida de información	Bajo rendimiento en atención a los usuario Pérdida de información Alteración de procesos realizados Daños informáticos posturas ergonómicas inadecuadas
hardware	Equipos de cómputo(pc,tablet,teléfonos inteligentes etc) Impresoras Teléfonos	Polvo, Corrosión o Congelamiento Hurto,pérdida,mal uso etc	bajo rendimiento en la operatividad de la empresa Pérdida de información Pérdida financiera
Software	software importantes para el buen funcionamiento de la empresa	Manipulación con software Copia fraudulenta del software Corrupción de datos	Incapacidad para prestar el servicio Perdida en la credibilidad de la empresa Alteración de la operación interna
Redes	Red de datos de navegación	Escucha subrepticia Falla del equipo de telecomunicaciones Espionaje remoto, pérdida de la integridad,confidencialidad de la información	Alteración en la propia organización Costo intero adicional Alteración de las terceras partes que tienen transacciones con la organización Peligro para el personal de la organización y los usuarios

Tabla 4. (Continuación)

Personal	empleados estudiantes visitantes	Incumplimiento en la disponibilidad del personal Destrucción de equipos o medios magnéticos Error de uso Hurto de activos, equipos o documentos propagación de malware	Costo financiero para pérdidas o reparaciones Despidos Daños materiales robo o pérdida de información propagación de malware
Planta física	Oficina	Uso inadecuado o descuidado del control de acceso físico a la empresa y los recintos Falta de protección física de las puertas y ventanas Ubicación en un área susceptible de inundación robo o pérdida de información o propagación de malware	

Fuente. Autor de la monografia

Así mismo se procede a realizar la evaluación de los riesgos encontrados

Tabla 5.

Evaluación del riesgo

IDENTIFICACIÓN DEL RIESGO		Evaluación del Riesgo			
Identif. de activos		Probabilidad	impacto	Valoración del Riesgo	Tipo de Riesgo
Procesos realizados	Localización de la información dentro de la empresa	4	4	16	**Riesgo Alto**
	Deterioro de los equipos de la empresa	2	2	4	Riesgo Medio

Tabla 5. (Continuación)

	El personal que trabaja en las dependencias no cuenta con espacios adecuados para su normal funcionamiento	4	3	12	Riesgo Muy Alto
hardware	Equipos de cómputo (pc, tablet, teléfonos inteligentes etc) Impresoras Teléfonos	3	1	3	Riesgo Medio
Software	Software importantes para el buen funcionamiento de la empresa (pago o gratuito)	3	1	3	Riesgo medio
Redes	Red de datos de navegación	3	2	6	Riesgo Alto
Personal	Empleados estudiantes visitantes	4	3	12	Riesgo Muy Alto
Planta física	Oficina	3	2	6	Riesgo Alto

Fuente. Autor de la monografia

	Vulnerabilidad Baja	Vulnerabilidad Media	Vulnerabilidad Alta	Vulnerabilidad Muy Alta
Peligro Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto	Riesgo Muy Alto
Peligro Alto	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Muy Alto
Peligro Medio	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Alto

Figura 3. Caracterización de riesgos

Fuente. Ministerio de Tecnologías de la Información y de las Comunicaciones (MINTIC

Figura 4. Ingreso de equipos personales al area de trabajo

Fuente. Autor de la monografia

Mediante el estudio que se realizó en la empresa innova se pudo evidenciar que el flujo de personal es bastante amplio ya que se cuenta con tres grandes grupos de poblaciones que hacen un uso frecuente estas tecnologías.

Dando como resultado de quienes más utilizan la tendencia (BYOD) son los invitados y los estudiantes siendo así este un problema para la seguridad e integridad de la información de los trabajadores y el personal que esta empresa se maneja.

De igual forma el personal que trabaja en las dependencias no cuenta con espacios adecuados para su normal funcionamiento, lo que en muchas ocasiones dificulta el desarrollo de las actividades en la misma y esto puede llegar a traer demoras en los procesos.

Por otro lado los empleados quienes son los más privilegiados con esta tendencia y tienen más fácil acceso a todos los recursos de la empresa y como está no está exenta de la pérdida de información ya que no cuenta con unas políticas claras en cuanto a la seguridad de la información y el uso compartido de la red y el fácil acceso de sus empleados a recursos importantes de la misma ellos pueden ser los primeros potenciales para la pérdida de información ya que pueden mediante un pendrive o memoria usb o su equipo personal tablet o su teléfono inteligente sustraer información de la cual a la hora de una pérdida o un robo pondría en riesgo la integridad y confidencialidad de la empresa.

4.3 Documento sobre el conjunto de buenas prácticas para la adopción Segura de la política BYOD.

Actividades para el cumplimiento del objetivo

- ✓ Clasificar los controles correspondientes a cada riesgo tratado.

Los datos contemplados en la siguiente tabla describes el ejercicio realizado.

Tabla 6.

Controles por riesgo

	Identif. de activos	**Identif. de Consecuencias**	**Identif. de Controles**
	Localización de la información dentro de la empresa	Retraso en proyectos e investigaciones realizadas por la empresa	Mantener controles de acceso a los dispositivos y personas dentro de la empresa para tener el control de los mismos y ubicarlos en sitios visibles para su constante vigilancia.
	Deterioro de los equipos de la empresa	Perdida de dinero y recursos de la empresa	

Tabla 6. (Continuación)

Procesos realizados	El personal que trabaja en las dependencias no cuenta con espacios adecuados para su normal funcionamiento	Bajo rendimiento en atención al usuario Pérdida de información Alteración de procesos realizados Daños informáticos posturas ergonómicas inadecuadas	
Hardware	Equipos de cómputo(pc,tablet,teléfonos inteligentes etc) Impresoras Teléfonos	Bajo rendimiento en la operatividad de la empresa Pérdida de información	
Software	Software importantes para el buen funcionamiento de la empresa (pago o gratuito)	Pérdida financiera Incapacidad para prestar el servicio Perdida en la credibilidad de la empresa	
Redes	Red de datos de navegación	Alteración de la operación interna	Implementar políticas de seguridad y firewall para mantener protegidos los activos de la empresa
Personal	Empleados Estudiantes visitantes	Alteración en la propia organización Costo intero adicional Alteración de las terceras partes que tienen transacciones con la organización Peligro para el personal de la organización y los usuarios	Dentro de los controles de acceso y acceso remoto se tiene que implementan mediante un sistema de seguridad una doble autenticación para a la hora de cualquier eventualidad tener la opción de salvaguardar la información o destruirla
Planta física	Oficina	Costo financiero para pérdidas o reparaciones Despidos Daños materiales robo o pérdida de información propagación de malware	Tener en cuenta el personal que está ingresando al área de trabajo y que equipo trae consigo. Dentro de las instalaciones tener control por parte de los equipos y de los puertos a los que estén conectados mantener en constante vigilancia a todo el personal como trabajadores,visitantes y estudiantes.

Fuente. Autor de la monografia

La empresa innova tienen mucho que ganar si toman ventaja de las tendencias y desarrollan sus actividades dentro de un ecosistema tecnológico en donde predomina una

diversidad generada por el mismo empleado. Por ende la empresa innova si comparte los siguientes consejos para mejorar sus prácticas y su estrategia BYOD:

1. - Contar una clara política de seguridad para los dispositivos de los empleados. Las políticas de seguridad y de acceso a la red de la empresa deben estar redactadas en un documento que se pueda compartir con todos los empleados. Así, el personal conocerá a detalle lo que se puede o no hacer en caso de querer usar su dispositivo para conectarse a la red empresarial y tener acceso a sus recursos (SG BUZZ, 2017).

2.- Tener de antemano un proceso de control de accesos a los sistemas críticos del negocio. La empresa debe establecer diferentes niveles y perfiles de acceso para los empleados, estudiantes y visitantes. Como el dispositivo se transforma en un visor de lo que hay dentro de la empresa, es importante conocer el perfil del usuario que está solicitando el acceso y la información desde su dispositivo (SG BUZZ, 2017).

3.- Tener claramente un proceso de perfiles de usuarios con la opción de conexión. La empresa debe conocer la información que es crítica, estratégica o confidencial y permitir el acceso a ésta sólo a los empleados que la compañía defina (SG BUZZ, 2017).

4.- Tener un proceso y conciencia de clasificar la información. La empresa debe organizar su información por niveles para que pueda estar disponible y actualizada para los empleados que la requieran y, al mismo tiempo, restringir o limitar el acceso a los datos confidenciales para las personas que tengan conexión de forma remota dentro de la misa

empresa (SeG BUZZ, 2017).

5.- Contar con una herramienta de BYOD que se adapte a la necesidad y diversidad de dispositivos de su negocio. Es importante que la solución que elija la empresa pueda dar servicio a los diferentes dispositivos, a las múltiples versiones de sistemas operativos y que todos los usuarios puedan ver en sus equipos exactamente la misma información (SG BUZZ, 2017).

6.- El brindar la opción a los usuarios de conectividad por medio de sus propios dispositivos no deberá ser para cualquier tipo de usuario y dependerá de la necesidad. Es muy importante que la empresa defina en sus políticas los niveles de acceso que ofrece a sus empleados. Como se ha mencionado, no toda la información de la empresa debe estar disponible para todos los usuarios. Además en la estrategia de la empresa debe estar perfectamente definido el beneficio de negocios al ofrecer el acceso de los datos corporativos a los empleados (SG BUZZ, 2017).

7.- Adquirir un MDM de una compañía de servicios de confianza. Esta tendencia de BYOD no debe ser un dolor de cabeza para los DBMS de sistemas, pues ya pueden encontrar soluciones efectivas disponibles en el mercado. La recomendación es acercarse a un proveedor de confianza que ofrezca una solución integral de Administración de Dispositivos Móviles (Mobile Device Management, MDM) y que brinde seguridad y soporte (SG BUZZ, 2017).

8.- Adquirir MAM (Filtrado y control de aplicaciones de dispositivos) bajo servicios

administrados para atender y mantener la seguridad. Otra solución que ya está disponible en el mercado es la de Administración de Aplicaciones Móviles (Mobile Application Management, MAM) a través de la cual la empresa pueda controlar la navegación web y aplicaciones de los dispositivos de los empleados de forma segura (SG BUZZ, 2017).

9.- Tener un brazo consultivo que le apoye definir, implantar y mejorar sus procesos de seguridad. Es muy importante que al elegir un proveedor de MDM o MAM, éste también pueda proporcionar la asesoría personalizada necesaria para que la estrategia de BYOD sea exitosa, segura y aporte un importante retorno de la inversión (SG BUZZ, 2017).

10.- BYOD no debe ser una moda, sino una ventaja competitiva. Si la empresa amerita movilidad, exponer sus aplicaciones y requiere de un control adecuado, implementar MDM o MAM no es más un "algo interesante que podríamos tener", sino que puede representar una verdadera estrategia competitiva para estar adelante de la competencia (SG BUZZ, 2017).

Capítulo 5. Conclusiones

La principal conclusión que se puede generar de este nuevo método de trabajo es que si se utilizan las recomendaciones anteriormente expuestas la empresa puede mejorar su productividad porque según los estudios realizados a nivel mundial por cisco indican que los trabajadores que realizan sus actividades con sus equipos personales pueden mejorar la productividad hasta en un 50 % por esto es de vital importancia que esta empresa al implementar políticas y recomendaciones de seguridad le brinde al trabajador todas las herramientas necesarias para que pueda trabajar de manera más segura y confiable.

Por esto es de vital importancia que esta empresa implemente todos los protocolos de seguridad e implemente políticas que permita estar a la vanguardia de las tecnologías pero de la manera más Segura confiable y eficaz

Capítulo 6. Recomendaciones

Teniendo en cuenta la importancia de las políticas y su respectivo análisis se le recomienda a la empresa Innova, realizar dichos análisis de forma eficiente y eficaz, con el objetivo de evitar inconvenientes en el futuro, y que este llegue a afectar el normal funcionamiento del ente económico.

Referencias

Aguilar. (2002). Globalización y Capitalismo. Mexico: Plaza & Janés.

Alvarez, & Duran. (2009). Manual de la Micro, Pequeña y Mediana Empresa. Una contribución a la mejora de los sistemas de información y el desarrollo de las políticas públicas. San salvador.

Asociación de jovenes empresarios. (5 de Febrero de 2016). http://www.ajeimpulsa.es/documentos/banco_recursos/recurso_13.pdf. Obtenido de Analisis de los factores que contribuyen al éxito de proyectos empresariales: http://www.ajeimpulsa.es/documentos/banco_recursos/recurso_13.pdf

Barnes, H. E. (2000). Historia de la econimia del mundo occidental. Mexico.

Bosca, J. E., & M.J, M. (2004). Efectos Macroeconómicos de las Inversiones en Infraestructuras Públicas. Valencia.

BSI. (10 de Septiembre de 2016). http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/. Obtenido de Norma ISO/IEC 27001 - Gestión de la Seguridad de la Información.

Castro Toro, J. P. (2010). Compilacion bibliografica. Manizales: Universidad de Caldas.

Chacartegui. (4 de Octubre de 2010). http://comunicandova.com/que-es-la-diferenciacion-y-por-que-la-necesitas/. Obtenido de Estrategias de posicionamiento: http://marketingyconsumo.com/estrategias-de-posicionamiento.html

Cisco IBSG Horizontes. (2013). El impacto financiero de BYOD.

Díaz, C. (2003). La Creación de Empresas en Extremadura. Un Análisis Institucional.

Dubois, A. (2002). Un concepto de desarrollo para el siglo XXI. España: Editorial Vasco.

Garay, L. J. (2016). Colombia: estructura industrial e internacionalización 1967-1996. Bogotá.

Hurtado. (2011). PYMES y corporaciones en contextos de globalización. Palmira: UNAD.

Jürgen. (2007). Innovacion en los negocios. Auflage. Vahlen, München.

Lagos, Galeas, Barrios, & Ruiz. (2014). Asociatividad de las MIPYMES en Honduras. Honduras.

López Camacho, R. A. (2014). Diseño de un marco referencial para regular el uso de Bydo en organizaciones bajo estandares ISO 27002. Santiago de Cali: Universidad Icesi.

Marquina, S. M. (2013). Gobernanza Global del Comercio en Internet. Mexico: Ed INAP, 1.ª Edición.

Ministerio de las TICs. (28 de Octubre de 2016). http://www.mintic.gov.co/gestionti/615/w3-article-5482.html. Obtenido de Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ministerio de tecnologia de la infromación y la comunicación. (12 de Julio de 2012). http://www.mintic.gov.co/portal/604/articles-5259_doc_pdf.pdf. Obtenido de Infrome de gestion.

Perafán Ruiz, J. J. (2014). Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Popayán: Universidad Nacional Abierta y a Distancia.

Plana, C., & Cerpa, N. (2006). Bases para la creación de una metodologia de adopción de comercio electronico para las mypimes chilenas. Talca: P Rev. Fac. Ing. - Univ. Tarapacá, vol. 14 Nº 1.

SG BUZZ. (2017). https://sg.com.mx/buzz/10-consejos-para-una-estrategia-byod#.WVz2e8g2vIU. Obtenido de 10 consejos para una estrategia BYOD.

Saro Luna, J., & Fernández Martín, J. (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD: ¿Bring Your Own Device Bring Your Own Disaster. SiC, 65.

Spiegel. (1987). El desarrollo del pensamiento económico. Barcelona: Ediciones Omega, S.A.

Universidad Colombia. (21 de Mayo de 2013). http://noticias.universia.net.co/en-portada/noticia/2013/05/21/1024756/ano-2016-afianzara-byod-empresas.pdf. Obtenido de Para el año 2016 se afianzará el BYOD en las empresas.

Valencia Duque, F. J. (26 de Junio de 2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en 73RISTI, N.º 22, 06/2017Revista lbérica de Sistemas e Tecnologias de InformaçãoRevista lbérica de Sistemas y Tecnologías de Información73 Recebido/Submis. Obtenido de https://www.researchgate.net/publication/317904811_Metodologia_para_la_implementacion_de_un_Sistema_de_Gestion_de_Seguridad_de_la_Informacion_basado_en_la_familia_de_normas_ISOIEC_27000.

Villalon Huertas, A. (29 de Octubre de 2016). http://www.shutdown.es/ISO17799.pdf. Obtenido de Sistema de gestion de seguridad de la información.