Diseño de un Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002

PROYECTO DE GRADO

Robin Alexander López Camacho

Ramiro López Obando

Asesor
Juan Manuel Madrid Molina
Ms Seguridad de la Información

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2014

Diseño de un Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002

Robin Alexander Lopez Camacho

Ramiro Lopez Obando

Trabajo de grado para optar al título de
Máster en Gestión de Proyectos y Tecnología con Énfasis en Ingeniería de Software

Asesor
Juan Manuel Madrid Molina
Ms Seguridad de la Información

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2014

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, <Fecha>

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

Actualmente el mercado tecnológico se encuentra en una fase de globalización y modernización de alta competitividad en productos y servicios, lo que ha traído consigo una avalancha de dispositivos móviles cada vez más potentes y con mayores capacidades de almacenamiento, tanto en el mercado de los smartphones como de las tablets. En este momento, el personal de las organizaciones ha integrado el uso de estos dispositivos a sus actividades laborales, generando cambios y adaptaciones en las empresas a nivel de informática, procesos y talento humano. Una organización, desde su nivel de gobierno hasta las áreas operativas, debe adoptar medidas de seguridad para los dispositivos móviles.

BYOD (Bring your Own Device), en español "Traiga su propio dispositivo", consiste en la incorporación de dispositivos móviles personales al ambiente de trabajo para acceder a los sistemas de información corporativo tales como: bases de datos, información comercial, correos electrónicos, archivos y aplicaciones propias de la organización.

A nivel de seguridad de la información existe un vacío conceptual en lo referente a los dispositivos móviles, puesto que el estándar ISO 27002 no considera de manera explícita la regulación del uso de BYOD.

Por lo anterior, y tomando como base la familia de estándares ISO 27002, en el presente trabajo se plantea un marco de referencia para la regulación del uso de BYOD en las organizaciones. Posteriormente se define un modelo para determinar el nivel de madurez de la organización con respecto al modelo propuesto, permitiendo identificar debilidades, fortalezas, además de establecer los puntos

críticos para el mejoramiento continuo de los procesos de seguridad referentes al uso de BYOD en la organización.

GLOSARIO

BYOD: Traiga su propio dispositivo (BYOD) es una estrategia que permite a los empleados, socios comerciales y otros usuarios, utilizar un dispositivo cliente seleccionado y comprado personalmente, para acceso a aplicaciones y datos empresariales. Típicamente se extiende por teléfonos inteligentes y tabletas, pero la estrategia también se puede usar para PC.

Confidencialidad: Es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (International Organization for Standardization, 2005)

Disponibilidad: Es la propiedad de la información que se refiere a que ésta sea accesible y utilizable por solicitud de una entidad autorizada, cuando así lo requiera. (International Organization for Standardization, 2005)

Integridad: Se define como la propiedad de salvaguardar la exactitud y completitud de los activos de información. (International Standard, 2013)

ISO: International Organization for Standarization (Organización Internacional para la Estandarización)

ISO/IEC 27000:2013 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Información: La información es un activo que, como otros activos importantes del negocio u organización, es esencial para las actividades del mismo y, en consecuencia, necesita una protección adecuada. (International Organization for Standardization, 2005)

Modelo de Madurez es un conjunto estructurado de elementos (buenas prácticas, herramientas de medición, criterios de análisis, etc.) que permiten identificar las capacidades instaladas en dirección de proyectos en la organización, compararlas con estándares, identificar vacíos o debilidades y establecer procesos de mejora continua. (MAP.)

Seguridad de la Información: La seguridad de la información es la protección de la información contra una gran variedad de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio. Además, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, otras propiedades tales como autenticidad y responsabilidad; no-repudio y confiabilidad pueden estar involucradas.

Smartphone es el término en inglés que se utiliza para denominar a un teléfono inteligente, es un equipo celular con funciones más avanzadas que las de un teléfono corriente.

KPI "Key Performance Indicator", conocido como Indicador clave de desempeño, (o también Indicador clave de rendimiento) es una medida del nivel de desempeño de un proceso; el valor del indicador está directamente relacionado con un objetivo a lograr.

1. INTRODUCCIÓN

1.1 CONTEXTO DE TRABAJO

BYOD (Bring your Own Device), en español “Traiga su propio dispositivo”, es una tendencia que cada vez está tomando más fuerza en el ambiente laboral. Consiste en la incorporación de los dispositivos móviles personales al ambiente de trabajo, para acceder a los sistemas de información corporativos tales como: bases de datos, información comercial, correos electrónicos, archivos y aplicaciones propias de la organización.

La tendencia del uso de Dispositivos Móviles Inteligentes continúa en un vertiginoso ascenso. En la imagen No 1 se muestra el crecimiento de la penetración de Smartphones en algunos países de América (GOOGLE, 2014). Para el tema particular de Colombia, según cifras del Ministerio de Tecnologías de la Información y las Comunicaciones en el “***Boletín Trimestral de las TIC Cifras Cuarto Trimestre de 2013”,*** el servicio de internet móvil por suscripción alcanzó un crecimiento del 42.2% con relación al cuarto trimestre del 2012, para un total de 4.563.644 suscriptores al finalizar el cuarto trimestre del 2013. El servicio de internet móvil por demanda, para el mismo período presentó un decrecimiento de 6.4%, para un total de 14.676.422 abonados. En Colombia, al finalizar el cuarto trimestre de 2013, el número de abonados era de 50.295.114. En el país existen 106.7 abonados en servicio por cada 100 habitantes (Ministerio de tecnologias de la Informacion y las comunicaciones, 2014) lo que indica que un 38.25% de los abonados a telefonia móvil tienen acceso a internet, una cifra bastante considerable que permite el cambio de la forma de vivir y trabajar, generando así una oportunidad para la proliferación de BYOD en las organizaciones.

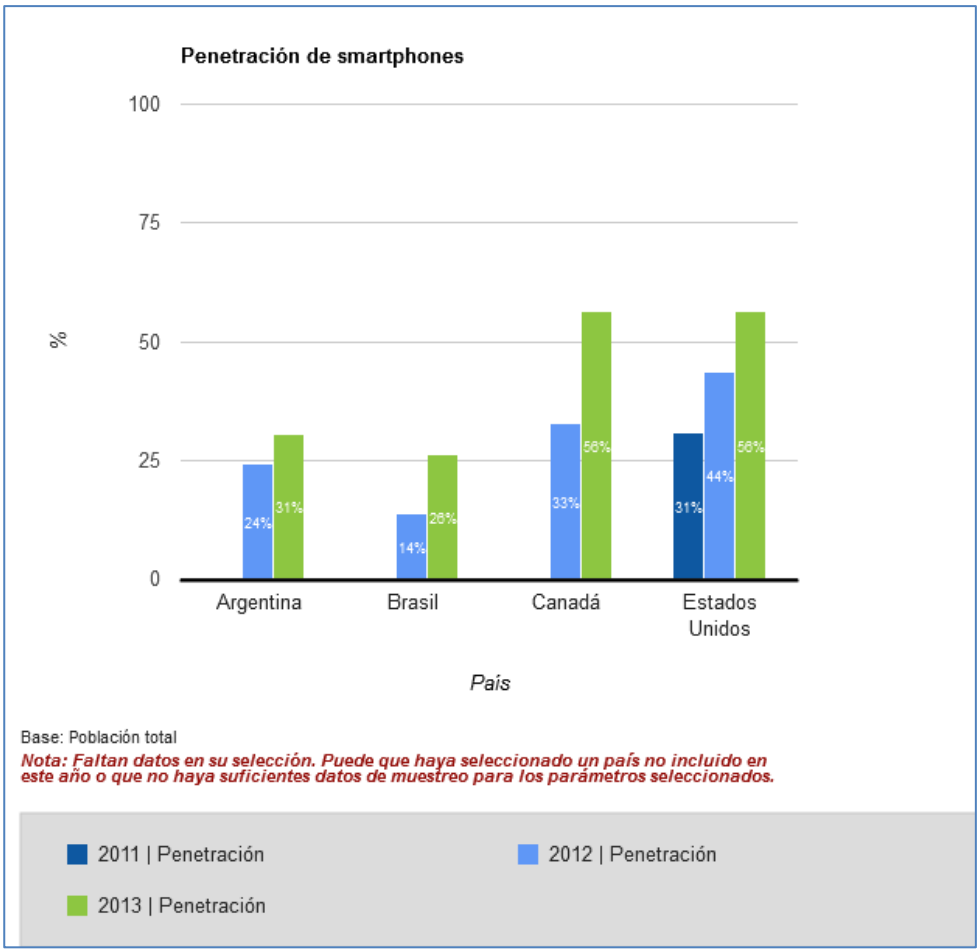

Imagen 1 Penetración de Smartphone's
Fuente: (GOOGLE, 2014)

Según cifras entregadas por Cisco, el 78% de los empleados administrativos en los Estados Unidos utilizan un dispositivo móvil para trabajar (Cisco IBSG Horizons, 2012). En el cuarto trimestre de 2012, un estudio global realizado por Forrester Research Inc. encontró que el 74% de los empleados utilizan los teléfonos inteligentes personales para tareas del negocio (Forrester Reseach, 2012).

Gartner pronostica que en el año 2020, el 45% de las empresas usarán completamente BYOD, mientras que sólo el 15% no incorporará BYOD en sus organizaciones (ver Imagen No 2).

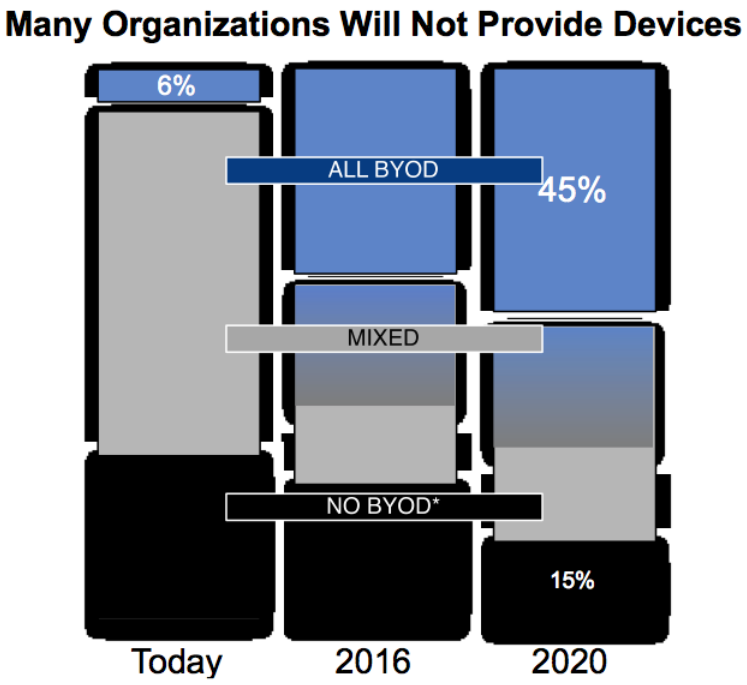

Imagen 2 Uso de BYOD
Fuente: (GARTNER, 2014)

Las organizaciones tienen la obligación de proteger la información propia y de sus clientes. Para una organización que no tenga controles de seguridad, o los tenga implementados inadecuadamente, BYOD se convierte en un riesgo con un gran impacto en la seguridad de la Información. Es necesario definir una política empresarial para afrontar adecuadamente este fenómeno, analizando y gestionando los riesgos para seleccionar los objetivos de control y los controles a implementar.

1.2 PLANTEAMIENTO DEL PROBLEMA

Las empresas no están afrontando adecuadamente la tendencia de BYOD. La adopción de esta tecnología se está realizando de manera progresiva y desorganizada, poniendo en riesgo la seguridad de la información. El estudio global realizado por Forrester Research Inc. en el cuarto trimestre de 2012, encontró que el 44% de los empleados utilizan los teléfonos inteligentes para el trabajo en cafeterías y otros lugares públicos, y el 47% los utilizan mientras viajan (Forrester Reseach, 2012). Lo que constituye un reto para la seguridad de la información, debido a que se está cambiando el modo de acceso y consumo de recursos tecnológicos dentro y fuera de la organización.

El rigor de la investigación académica alrededor del tema, permite precisar la diferenciación entre la naturaleza del problema de BYOD y el alcance del mismo. Dentro de los elementos de esta naturaleza, se precisa determinar el acceso a sistemas de información según los niveles de seguridad.

La implementación de políticas de BYOD depende netamente de las necesidades de cada sistema o sub sistemas de la organización, por tanto pasa por la implementación de subsistemas distribuidos de seguridad vs Productividad, que deben estar alineados con las mejores prácticas de seguridad de diferentes marcos de referencia, tales como ISO 27001:2013, ISO 27002:2013, PCI DSS versión 2.0 y otros.

1.3 OBJETIVOS

1.3.1 Objetivo General

Diseño e Implementación de un Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002.

1.3.2 Objetivos Específicos

1. Revisar y evaluar las mejores prácticas del marco de referencia ISO 27002:2013 para la seguridad de la información con respecto a BYOD.
2. Identificar y complementar los estándares de la ISO 27002:2013 de acuerdo con las buenas prácticas de BYOD y los numerales que apliquen.
3. Definir un modelo de madurez de BYOD basado en el modelo propuesto adoptado de ISO 27002:2013.
4. Evaluación de la madurez de una empresa bajo el modelo de madurez de BYOD propuesto.

1.4 RESUMEN DEL MODELO PROPUESTO

El Diseño del Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002, se estructuró en una serie de etapas, de acuerdo con dicho estándar. El Marco de Referencia propuesto para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002, permite identificar el estado del arte de la organización en cuanto al uso de dispositivos móviles personales en el ámbito empresarial. Toma para su validación referentes ampliamente reconocidos por los estándares ISO 27002.

La parte instrumental de este proyecto de investigación está constituida por una prueba piloto que se diseña y aplica para una empresa usuaria específica, con la cual se validan principios y parámetros del modelo.

1.4.1 Definición del problema.

En el primer paso, se describe el problema de la utilización de dispositivos personales por parte de los empleados en el ámbito empresarial.

1.4.2 Alcance de la propuesta del servicio.

El segundo paso consiste en la identificación de cada uno de los controles de la ISO 27002 que apliquen para el uso de BYOD.

1.4.3 Marco de Referencia para el uso de BYOD.

El tercer paso, es la creación del Marco de Referencia, para este objetivo se contó con el juicio de un experto para la selección de cada uno de los dominios y controles.

1.4.4 Modelo de Madurez.

En el cuarto paso, se crea un Modelo de Madurez para BYOD. En pos de este objetivo, se procede a efectuar una serie de preguntas seleccionadas de cada uno de los controles del nuevo Marco de referencia para el uso de BYOD a los interesados del departamento de T.I de la organización.

1.4.5 Implementación de la Propuesta.

En el quinto paso se selecciona una empresa para validar el Modelo de Madurez Propuesto de BYOD, se procede a identificar a los interesados, y posteriormente se efectúan las entrevistas creadas para conocer el estado de madurez en cuanto a BYOD en la organización; posteriormente se efectúa una valoración y se entregan unos escenarios donde se sugieren acciones para mejorar el nivel de madurez.

1.5 RESUMEN DE RESULTADOS OBTENIDOS

Los resultados de este proyecto son:

- Un Marco de Referencia para regular el uso de BYOD en organizaciones bajo el estándar ISO 27002
- Un Modelo de Madurez basado en el modelo propuesto de BYOD.

El Marco de Referencia propuesto, es una herramienta que consta de 14 dominios y 45 controles, los cuales permiten a la organización implementar buenas prácticas para el uso de BYOD.

1.6 ORGANIZACIÓN DEL DOCUMENTO

El documento consta de 6 capítulos descritos a continuación:

El capítulo 1 consiste en el planteamiento general del proyecto.

En el capítulo 2 se presenta el marco teórico de BYOD, su definición, ventajas y riesgos. Se abordan aspectos esenciales de Activos de Información y seguridad de la información.

En el capítulo 3 se presenta la metodología detallada que se empleó para obtener los controles del Marco de Referencia para regular el uso de BYOD en organizaciones, bajo el estándar ISO 27002.

En el capítulo 4 se muestra la metodología del Modelo de Madurez propuesto, describiendo las funciones de los roles establecidos del departamento de T.I.

En el capítulo 5 se efectúa la evaluación de una empresa bajo el modelo de

Madurez propuesto en el capítulo 4 y se describen en detalle los resultados obtenidos, así como 3 escenarios de mejora.

En el capítulo 6 se presentan las conclusiones del trabajo y recomendaciones futuras a desarrollar.

2. MARCO TEÓRICO

2.1 BYOD

La implantación de un programa de BYOD involucra que los empleados utilicen sus propios dispositivos de comunicación móviles, para llevar a cabo trabajo para su empleador, 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 dispositivo 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. (Ann Cavaukian, 2013)

El uso de un dispositivo móvil propiedad de los empleados en el lugar de trabajo se diferencia del uso de un dispositivo móvil corporativo, de dos maneras. La primera es la propiedad: mientras que un dispositivo móvil corporativo es propiedad de la organización que lo emite, un dispositivo BYOD (para abreviar, 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 dispositivo móvil 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 dispositivo 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 dispositivo, 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 quien pertenece el dispositivo, así como tal vez allegados al empleado, por ejemplo, otras personas importantes, miembros de la familia, amigos, etc. (Ann Cavaukian, 2013)

2.2 Activo de Información

En la era de la Informática y las Telecomunicaciones el insumo más importante es la información y por ende, el departamento de TI de las organizaciones debe estar a la vanguardia para salvaguardar este bien, proporcionando confidencialidad, disponibilidad e integridad de la información. Una de las definiciones que creemos más acertada para este trabajo en cuanto a los activos de información es *"Un recurso o bien económico propiedad de una empresa, con el cual se obtienen beneficios. Los activos de las empresas varían de acuerdo con la naturaleza de la actividad desarrollada."* (ISACA); estos pueden ser clasificados en diferentes tipos como se muestra en la imagen 3.

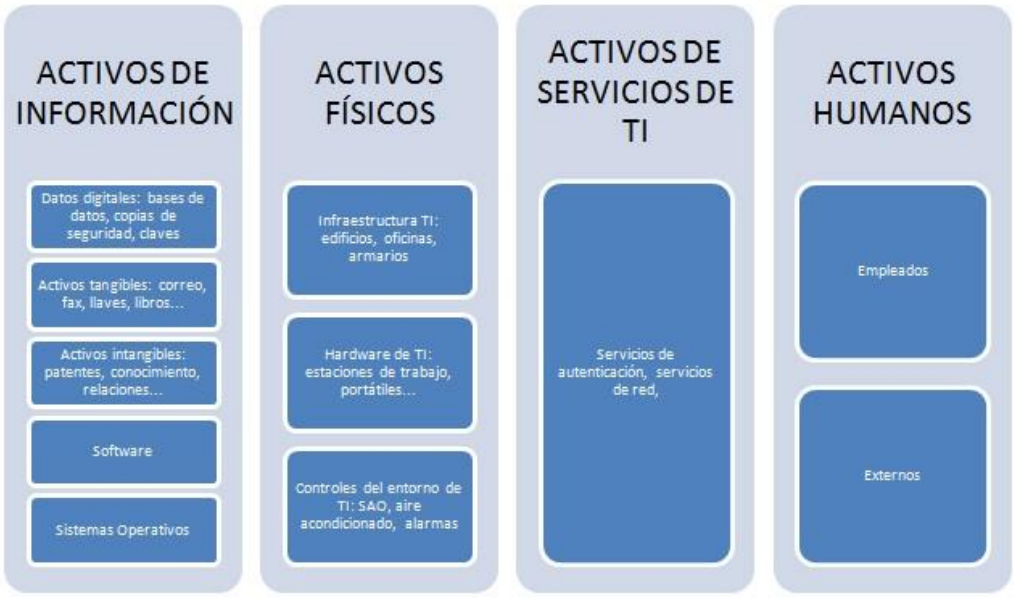

Imagen 3 Clasificación de Activos
Fuente: (Vera)

2.3 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 certificable (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.
- Gestión de Riesgos

En la Tabla 1, se especifican los principales procesos que indica la norma referida, mapeados con las etapas del ciclo PHVA.

Tabla 1 Ciclo Deming (PHVA) aplicado a la norma ISO/IEC 27.001

CICLO PHVA	PROCESOS
Planificar (***P****lan***)	Establecer el contexto. Alcance y Limites 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
Hacer (***D****o***)	Implementar plan de tratamiento de riesgos
	Implementar los controles seleccionados
	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 (***C****heck***)	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
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.

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.

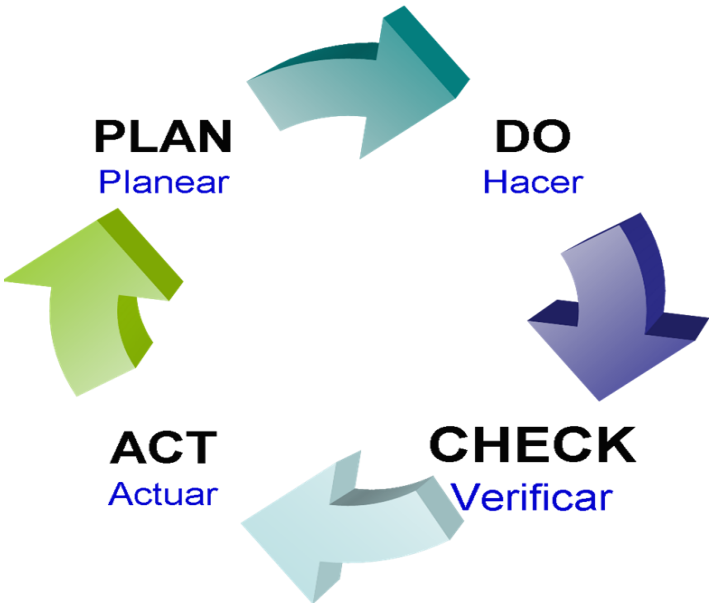

Imagen 4 Gestión de Seguridad de la Información
Fuente: (Vera)

2.3.1 ISO/IEC 27002

Esta Norma Internacional está diseñada para que las organizaciones la utilicen 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.

5.1.1 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.

5.1.2 Revisión de las políticas de seguridad de la información

Control

Las políticas de seguridad de la información deben ser revisados a intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.

Dominio 6 Organización de la seguridad de la información

6.1 Organización interna

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización .

6.1.1 roles y responsabilidades de seguridad de la información

Control

Todas las responsabilidades de seguridad de la información deben ser definidas y asignados.

6.1.2 Separación de funciones

Control

Las funciones en conflicto y áreas de responsabilidad deben estar separado para reducir las oportunidades para la modificación o mal uso de los activos de la organización no autorizado o involuntario.

6.1.3 Contacto con las autoridades

Control

Los contactos pertinentes con las autoridades pertinentes deben mantenerse.

6.1.4 El contacto con los grupos de interés especial

Control

Los contactos pertinentes con los grupos de interés u otros foros de seguridad especializada y las asociaciones profesionales deben mantenerse.

6.1.5 Seguridad de la información en la gestión de proyectos

Control

Seguridad de la información debería abordarse en la gestión de proyectos, independientemente del tipo de proyecto.

6.2 Los dispositivos móviles y el teletrabajo

Objetivo: garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 política de dispositivo móvil

Control

Una política y el apoyo a las medidas de seguridad deben adoptarse para gestionar los riesgos introducidos por el uso de dispositivos móviles.

6.2.2 El teletrabajo

Control

Una política y el apoyo a las medidas de seguridad se deben implementar para proteger la información visitada, procesada o almacenada en los sitios de trabajo a distancia.

Dominio 7 seguridad de los recursos humanos

7.1 Antes de empleo

Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

7.1.1 Proyección

Control

Controles de verificación de antecedentes de todos los candidatos a empleo deben llevarse a cabo de acuerdo con las leyes, regulaciones y ética y debe ser proporcional a los requerimientos del negocio, la clasificación de la información para acceder a ellos y los riesgos percibidos.

7.1.2 Términos y condiciones de empleo

Control

Los acuerdos contractuales con los empleados y contratistas deben indicar y responsabilidades de sus de la organización para la seguridad de la información.

7.2 Durante el empleo

Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.

7.2.1 Responsabilidades de la Administración

Control

La administración debe exigir a todos los empleados y contratistas para aplicar seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

7.2.2 Información de concienciación sobre la seguridad, la educación y la formación

Control

Todos los empleados de la organización y, en su caso, los contratistas deben recibir una educación adecuada en el conocimiento y la formación y actualizaciones periódicas en las políticas y procedimientos de la organización, como relevantes para su función de trabajo.

7.2.3 Proceso disciplinario

Control

Debe haber un proceso disciplinario formal y comunicado en lugar de tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.

7.3 Terminación y cambio de empleo

Objetivo: proteger los intereses de la organización, como parte del proceso de cambiar o terminar el empleo.

7.3.1 La terminación o el cambio de las responsabilidades laborales

Control

Las responsabilidades de seguridad de la Información y deberes que siguen vigentes después de la terminación o cambio de trabajo deberían ser definidos, comunicado al trabajador o contratista y forzada.

Dominio 8 Gestión de activos

8.1 La responsabilidad de los activos

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuados.

8.1.1 Inventario de activos

Control

Los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos activos debe elaborarse y mantenerse.

8.1.2 Propiedad de los bienes

Control

Los activos mantenidos en el inventario deben ser de propiedad.

8.1.3 El uso aceptable de los activos

Control

Normas para el uso aceptable de la información y de los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificadas, documentados e implementados.

8.1.4 Categorías de los activos

Control

Todos los empleados y los usuarios externos del partido deben devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.

8.2 Clasificación de la Información

Objetivo: Garantizar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

Control

La información debe ser clasificada en términos de requisitos legales, el valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada.

8.2.2 Etiquetado de la información

Control

Un conjunto apropiado de los procedimientos para el etiquetado información debe ser desarrollado e implementado de acuerdo con el esquema de clasificación de la información adoptado por la organización.

8.2.3 Manejo de los activos

Control

Procedimientos para la manipulación de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la organización.

8.3 Manejo de Medios

Objetivo: Para evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.

8.3.1 Gestión de soportes extraíbles

Control

Deberían aplicarse procedimientos para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización.

8.3.2 Eliminación de los medios de comunicación

Control

Los medios deben ser eliminados de forma segura cuando ya no es necesario, utilizando los procedimientos formales.

8.3.3 Transferencia de medios físicos

Control

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante el transporte.

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.

9.1.1 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

9.1.2 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.

9.2 Gestión de acceso de Usuario

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

9.2.1 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.

9.2.2 Acceso aprovisionamiento de Usuario

Control

Un proceso de provisión de acceso de usuarios formal debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.

9.2.3 Gestión de los derechos de acceso privilegiados

Control

La asignación y utilización de los derechos de acceso privilegiados deben ser restringidas y controladas.

9.2.4 Gestión de la información de autenticación de secreto de los usuarios

Control

La asignación de la información secreta de autenticación debe ser controlada a través de un proceso de gestión formal.

9.2.5 Revisión de los derechos de acceso de usuario

Control

Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

9.2.6 Retiro o el ajuste de los derechos de acceso

Control

Los derechos de acceso de todos los empleados y usuarios de partidos externos a las instalaciones de procesamiento de información y la información deben ser retirados a la terminación de su empleo, contrato o convenio, o ajustarse a cambio.

9.3 Responsabilidades del usuario

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

9.3.1 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.

9.4 Sistema de control de acceso y aplicación

Objetivo: Para prevenir el acceso no autorizado a los sistemas y aplicaciones.

9.4.1 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.

9.4.2 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.

9.4.3 sistema de gestión de contraseña

Control

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

9.4.4 El uso de los programas de servicios públicos privilegiados

Control

El uso de programas de utilidades que podrían ser capaces de anular sistemas y aplicaciones controles debe ser restringido y estrechamente controlado.

9.4.5 Control del acceso al código fuente del programa

Control

El acceso al código fuente del programa debe ser restringido.

Dominio 10 Criptografía

10.1 controles criptográficos

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

10.1.1 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.

10.1.2 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.

Dominio 11 La seguridad física y ambiental

11.1 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.

11.1.1 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.

11.1.2 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.

11.1.3 Protección de oficinas, salas e instalaciones

Control

La seguridad física para oficinas, salas e instalaciones deben ser diseñadas y aplicadas.

11.1.4 Protección contra amenazas externas y ambientales

Control

La protección física contra los desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.

11.1.5 Trabajar en zonas seguras

Control

Procedimientos para trabajar en zonas seguras deberían diseñarse y aplicarse.

11.1.6 Zonas de entrega y carga

Control

Los puntos de acceso como las zonas de entrega y de carga y otros puntos en los que personas no autorizadas puedan entrar en los locales deberán ser controlados y, si es posible, aislada de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

11.2 Equipos

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

11.2.1 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.

11.2.2 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.

11.2.3 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.

11.2.4 Mantenimiento de equipo

Control

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

11.2.5 Eliminación de los activos

Control

Equipos, información o software no deben tomarse fuera de las instalaciones sin autorización previa.

11.2.6 Seguridad de equipo y activos fuera de las instalaciones

Seguridad debe ser aplicado a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajo fuera de los locales de la organización

11.2.7 Eliminación segura o re-uso de equipos

Control

Todos los artículos de equipos que contengan soportes de almacenamiento deben ser verificados para asegurar que los datos sensibles y software con licencia han sido eliminados o sobrescrito de forma segura antes de su eliminación o reutilización.

11.2.8 equipo de usuario desatendida

Control

Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.

11.2.9 escritorio despejado y la política de pantalla transparente

Control

Una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política clara pantalla para las instalaciones de procesamiento de la información deben ser adoptada.

Dominio 12 Seguridad de Operaciones

12.1 procedimientos y responsabilidades operacionales

Objetivo: Garantizar las operaciones correctas y seguras de instalaciones de procesamiento de información.

12.1.1 procedimientos operativos documentados

Control

Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.

12.1.2 Gestión de cambios

Control

Cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados.

12.1.3 Capacidad de gestión

Control

El uso de los recursos debe ser monitoreado, se ajusta y proyecciones de las futuras necesidades de capacidad para garantizar el rendimiento del sistema requerido.

12.1.4 Separación de desarrollo, prueba y entornos operativos

Control

Entornos de desarrollo, prueba y operación deben ser separados para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional

12.2 Protección contra el malware

Objetivo: asegurar que las instalaciones de procesamiento de información y la información están protegidos contra el malware.

12.2.1 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.

12.3 Copia de seguridad

Objetivo: Para evitar la pérdida de datos.

12.3.1 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.

12.4 Registro y supervisión

Objetivo: registrar eventos y generar evidencia.

12.4.1 Log de Evento

Control

Los registros de eventos registran las actividades del usuario, excepciones, errores y eventos de seguridad de la información, se deben producir, mantener y revisados con regularidad

12.4.2 Protección de la información de registro

Control

Registro de instalaciones y registrar la información debe ser protegida contra la manipulación y acceso no autorizado.

12.4.3 registros de administrador y operador

Control

Sistema, el administrador y las actividades del operador del sistema deben ser registrados, y los troncos protegidos y regularmente revisados.

12.4.4 Sincronización de Reloj

Control

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente de tiempo de referencia.

12.5 Control del software operativo

Objetivo: garantizar la integridad de los sistemas operativos.

12.5.1 Instalación de software en sistemas operativos

Control

Deberían aplicarse procedimientos para controlar la instalación del software en los sistemas operativos.

12.6 de gestión de vulnerabilidades Técnica

Objetivo: prevenir la explotación de vulnerabilidades técnicas.

12.6.1 Gestión de las vulnerabilidades técnicas

Control

Información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilicen deben ser obtenidos de manera oportuna, la exposición de la organización a tales vulnerabilidades evaluado y tomado las medidas adecuadas para hacer frente a los riesgos asociados.

12.6.2 Restricciones a la instalación de software

Control

Las normas que rigen la instalación de software los usuarios deben establecerse e implementarse.

12.7 Sistemas de información Consideraciones de auditoría

Objetivo: minimizar el impacto de las actividades de auditoría en los sistemas operativos.

12.7.1 Sistemas de información controles de auditoría

Control

Requisitos y actividades de verificación de los sistemas operativos de auditoría deben ser cuidadosamente planificadas y acordadas para reducir al mínimo las interrupciones de los procesos de negocio.

Dominio 13 La seguridad de Comunicaciones

13.1 gestión de seguridad de red

Objetivo: garantizar la protección de la información en las redes y sus instalaciones de apoyo de información procesamiento.

13.1.1 controles de red

Control

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

13.1.2 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.

13.1.3 La segregación en las redes

Control

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

13.2 Transferencia de Información

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

13.2.1 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.

13.2.2 Los acuerdos sobre la transferencia de información

Control

Los acuerdos deben abordar la transferencia segura de información comercial entre la organización y las partes externas.

13.2.3 La mensajería electrónica

Control

Información involucrada en la mensajería electrónica debe ser protegido de manera apropiada.

13.2.4 Los acuerdos de confidencialidad o de no divulgación.

Control

Requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, revisados y documentados con regularidad.

Dominio 14 Sistema de adquisición, desarrollo y mantenimiento

14.1 Los requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

14.1.1 Información de análisis de requisitos de seguridad y las especificaciones

Control

Los requisitos relacionados con la seguridad de la información deben ser incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

14.1.2 servicios de aplicaciones de fijación de las redes públicas

Control

Información involucrada en los servicios de aplicaciones que pasan a través de redes públicas debe protegerse de la actividad fraudulenta, disputa contractual y la divulgación no autorizada y modificación.

14.1.3 Protección de las transacciones de servicios de aplicación

Control

Información involucrada en las transacciones de servicios de aplicación debe ser protegido para prevenir la transmisión incompleta, errónea enrutamiento, alteración mensaje no autorizado, revelación no autorizada, la duplicación de mensajes no autorizados o la repetición.

14.2 procesos de desarrollo y de apoyo

Objetivo: Garantizar que la seguridad de información se diseña e implementa dentro del ciclo de vida de desarrollo de sistemas de información.

14.2.1 política de desarrollo Segura

Control

Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a la evolución de la organización.

14.2.2 los procedimientos de control de cambio de sistema

Control

Los cambios en los sistemas dentro del ciclo de vida de desarrollo deben ser controlados por el uso de procedimientos formales de control de cambio.

14.2.3 Revisión técnica de solicitudes después de cambios en la plataforma de funcionamiento

Control

Cuando se cambian las plataformas que operan, aplicaciones críticas de negocio deben ser revisados y probados para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.

14.2.4 Restricciones en los cambios en los paquetes de software

Control

Las modificaciones a los paquetes de software deben ser desalentados, otros, las modificaciones necesarias y todos los cambios deben ser estrictamente controlados.

14.2.5 principios de ingeniería de sistemas seguros

Control

Principios para sistemas seguros de ingeniería deben establecerse, documentarse, mantenerse y aplicarse a cualquier esfuerzo de implementación de sistemas de información.

14.2.6 entorno de desarrollo seguro

Control

Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguras para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema.

14.2.7 Desarrollo tercerizado

Control

La organización debe supervisar y controlar la actividad de desarrollo del sistema tercerizado.

14.2.8 Pruebas de seguridad Sistema

Control

Pruebas de la funcionalidad de seguridad debe llevarse a cabo durante el desarrollo.

14.2.9 Pruebas de aceptación de Sistema

Control

Programas de pruebas de aceptación y criterios relacionados deben establecerse para los nuevos sistemas de información, actualizaciones y nuevas versiones.

14.3 Los datos de prueba

Objetivo: Garantizar la protección de los datos utilizados para la prueba.

14.3.1 Protección de datos de prueba

Control

Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados.

Dominio 15 Relaciones con los proveedores

15.1 Seguridad de la información en relación con los proveedores

Objetivo: garantizar la protección de los activos de la organización que sea accesible por los proveedores.

15.1.1 Política de seguridad de la información para relaciones con los proveedores

Control

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben arreglarse con el proveedor y documentados.

15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores

Control

Todos los requisitos de seguridad de la información pertinentes deben ser establecidos y acordados con cada proveedor que pueden acceder, procesar, almacenar, comunicar, o proporcionar TI componentes de la infraestructura de información de la organización.

15.1.3 Tecnología de la comunicación de Información y cadena de suministro

Control

Los acuerdos con los proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de información asociados a los servicios de información y tecnología de las comunicaciones y de la cadena de suministro de productos.

15.2 Gestión de la prestación de servicios de Proveedor

Objetivo: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los proveedores.

15.2.1 Seguimiento y revisión de los servicios de proveedores

Control

Las organizaciones deben controlar regularmente, revisar y auditar la prestación de servicios de los proveedores

15.2.2 Gestión de cambios en los servicios de proveedores

Control

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se deben manejar, teniendo en cuenta la criticidad de la información empresarial, los sistemas y los procesos involucrados y re-evaluación de los riesgos.

Dominio 16 Información de gestión de incidentes de seguridad

16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Para garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.

16.1.1 Responsabilidades y procedimientos

Control

Las Responsabilidades y procedimientos de gestión deben ser establecidos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

16.1.2 Informes eventos seguridad de la información

Control

Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuadas tan pronto como sea posible.

16.1.3 Informes debilidades de seguridad de información

Control

Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deberían estar obligados a observar y reportar cualquier debilidad de seguridad de información observados o sospechados en los sistemas o servicios.

16.1.4 Evaluación y decisión de los eventos de seguridad de información

Control

Los eventos de seguridad de la información deben ser evaluados y se debe decidir si han de ser clasificados como incidentes de seguridad de la información.

16.1.5 Respuesta a incidentes de seguridad de la información

Control

Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.

16.1.6 Aprendiendo de los incidentes de seguridad de la información

Control

Los conocimientos adquiridos desde el análisis y la resolución de los incidentes de seguridad de la información deben utilizarse para reducir la probabilidad o el impacto de futuros incidentes.

16.1.7 Reunión de pruebas

Control

La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como prueba.

Dominio 17 aspectos de seguridad de información de la gestión de la continuidad del negocio

17.1 Información continuidad seguridad

Objetivo: Información sobre la continuidad de seguridad, debe estar integrada en los sistemas de gestión de continuidad de negocio de la organización.

17.1.1 Planificación de la continuidad seguridad de la información

Control

La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

17.1.2 Implementación información continuidad seguridad

Control

La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles que garanticen el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

17.1.3 Verificar, revisar y evaluar la información de seguridad de continuidad

Control

La organización debe verificar la información de controles de continuidad de seguridad establecido y aplicado a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.

17.2 Redundancia

Objetivo: asegurar la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información

Control

Instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para satisfacer los requisitos de disponibilidad

Dominio 18 cumplimientos

18.1 Cumplimiento de los requisitos legales y contractuales

Objetivo: evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la información y la seguridad de todos los requisitos de seguridad.

18.1.1 Identificación de la legislación aplicable y requisito contractual.

Control

Todo legal legislativo pertinente, los requisitos reglamentarios, contractuales y el enfoque de la organización para cumplir con estos requisitos deben ser identificados de manera explícita, documentados y actualizados a la fecha de cada sistema de información y la organización

18.1.2 Derechos de propiedad intelectual

Control

Procedimientos apropiados deben ser implementadas para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software privativo.

18.1.3 Protección de registros

Control

Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y la liberación no autorizada, de conformidad con los requisitos legales, reglamentarios, contractuales y comerciales.

18.1.4 de privacidad y protección de datos personales

Control

Privacidad y protección de la información de identificación personal que se debe garantizar a lo dispuesto en la legislación y la regulación en su caso relevante

18.1.5 Regulación de controles criptográficos

Control

Controles criptográficos deben ser utilizados en el cumplimiento de todos los acuerdos pertinentes, la legislación y los reglamentos.

18.2 revisiones de seguridad de información

Objetivo: Garantizar que la seguridad informática es implementado y operado de acuerdo con las políticas y procedimientos de la organización.

18.2.1 Revisión independiente de seguridad de la información

Control

El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información) debe ser revisado de forma independiente a intervalos planificados o cuando se producen cambios significativos.

18.2.2 El cumplimiento de las políticas y estándares de seguridad

Control

Los gerentes deben comprobar periódicamente el cumplimiento de los procedimientos de procesamiento y la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.

18.2.3 revisión de cumplimiento técnico

control

Los sistemas de información deben ser revisados regularmente por el cumplimiento de las políticas y normas de seguridad de la información de la organización.

2.4 CMMI

Los modelos CMMI® (Capability Maturity Model® Integration) son colecciones de buenas prácticas que ayudan a las organizaciones a mejorar sus procesos. Estos modelos son desarrollados por equipos de producto con miembros procedentes de la industria, del gobierno y del Software Engineering Institute (SEI). (Software Engineering Institute, 2010)

Los niveles se utilizan en CMMI-DEV para describir un camino evolutivo recomendado para una organización que quiera mejorar los procesos que utiliza en el desarrollo de productos o servicios. Para dar soporte a aquellos que utilizan la representación por etapas, todos los modelos CMMI reflejan niveles de madurez en su diseño y contenido. Un nivel de madurez consta de prácticas específicas y genéricas relacionadas para un conjunto predefinido de áreas de proceso que mejoran el rendimiento global de la organización. (Software Engineering Institute, 2010)

El nivel de madurez de una organización proporciona una forma para caracterizar su rendimiento. La experiencia ha mostrado que las organizaciones toman una decisión acertada cuando centran sus esfuerzos de mejora de procesos en un número manejable de áreas de proceso a la vez y que dichas áreas requieren refinarse a medida que la organización mejora. Un nivel de madurez es una plataforma evolutiva definida para la mejora de procesos de la organización. Cada nivel de madurez desarrolla un subconjunto importante de procesos de la organización, preparándola para pasar al siguiente nivel de madurez. Los niveles

de madurez se miden mediante el logro de las metas específicas y genéricas, asociadas con cada conjunto predefinido de áreas de procesos. (Software Engineering Institute, 2010)

Los cinco niveles de madurez, cada uno de ellos una base para la mejoras de proceso en curso, son los siguientes:

1. Inicial.
2. Gestionado.
3. Definido.
4. Gestionado cuantitativamente.
5. En optimización.

2.4.1 Nivel de madurez 1: Inicial

En el nivel de madurez 1, los procesos son generalmente ad hoc y caóticos. La organización generalmente no proporciona un entorno estable para dar soporte a los procesos. El éxito en estas organizaciones depende de la competencia y la heroicidad del personal de la organización y no del uso de procesos probados. A pesar de este caos, las organizaciones de nivel de madurez 1 a menudo producen productos y servicios que funcionan, sin embargo, exceden con frecuencia el presupuesto y los plazos planificados. Las organizaciones de nivel de madurez 1 se caracterizan por una tendencia a comprometerse en exceso, a abandonar sus procesos en momentos de crisis y a no ser capaces de repetir sus éxitos. (Software Engineering Institute, 2010)

2.4.2 Nivel de madurez 2: Gestionado

En el nivel de madurez 2, se garantiza que en los proyectos los procesos se planifican y ejecutan de acuerdo con las políticas; los proyectos emplean personal

cualificado que dispone de recursos adecuados para producir resultados controlados. Se involucra a las partes interesadas relevantes; se monitorizan, controlan, revisan y se evalúan en cuanto a la adherencia a sus descripciones de proceso. La disciplina de proceso reflejada por el nivel de madurez 2 ayuda a asegurar que las prácticas existentes se mantienen durante periodos bajo presión. Cuando estas prácticas están desplegadas, los proyectos se realizan y gestionan de acuerdo a sus planes documentados. (Software Engineering Institute, 2010)

2.4.3 Nivel de madurez 3: Definido

En el nivel de madurez 3, los procesos están bien caracterizados y comprendidos; estos se describen en estándares, procedimientos, herramientas y métodos. El conjunto de procesos estándar de la organización, que es la base del nivel de madurez 3, se establece y se mejora a lo largo del tiempo. Estos procesos estándar se utilizan para establecer la integridad en toda la organización. (Software Engineering Institute, 2010)

2.4.4 Nivel de madurez 4: Gestionado cuantitativamente

En el nivel de madurez 4, la organización y los proyectos establecen objetivos cuantitativos para la calidad y el rendimiento del proceso, y los utilizan como criterios en la gestión de los proyectos. Los objetivos cuantitativos se basan en las necesidades del cliente, usuarios finales, organización e implementadores del proceso. La calidad y el rendimiento del proceso se interpretan en términos estadísticos y se gestionan durante la vida de los proyectos. (Software Engineering Institute, 2010)

2.4.5 Nivel de madurez 5: En optimización

En el nivel de madurez 5, una organización mejora continuamente sus procesos

basándose en una comprensión cuantitativa de sus objetivos de negocio y necesidades de rendimiento. La organización utiliza un enfoque cuantitativo para comprender la variación inherente en el proceso y las causas de los resultados del proceso. El nivel de madurez 5 se centra en optimizar continuamente el rendimiento de los procesos mediante mejoras incrementales e innovadoras de proceso y de tecnología. Los objetivos de calidad y de rendimiento del proceso de la organización se establecen y continuamente se modifican, para reflejar cambios en los objetivos del negocio y en el rendimiento de la organización; éstos se utilizan como criterios para gestionar la mejora de procesos. (Software Engineering Institute, 2010)

3. MODELO PROPUESTO

Permitir el uso de dispositivos personales para las funciones laborales (BYOD), sin una regulación adecuada, puede generar problemas de seguridad en los activos de información con consecuencias legales y económicas. Se evidencia entonces, la necesidad de tener un marco de referencia de seguridad de la información, buscando mitigar los riesgos que trae el uso de los dispositivos personales.

En este parte del documento se presentan los imperativos a ser resueltos, motivados en las particularidades del estándar ISO 27002:2013 para el uso de BYOD en una organización, sea que tengan o no implementado un SGSI.

Se tomó como base la norma ISO 27002 para determinar los controles aplicables a BYOD, y se definió una metodología que consta de cuatro pasos, el primero consiste en una revisión objetivo por objetivo y control por control, buscando obtener un profundo conocimiento del marco. El segundo, consiste en realizar un análisis de la norma frente al conocimiento adquirido de BYOD y determinar posibles controles de la misma; luego en el tercer paso, se validan estos análisis con un experto detalle en el anexo No 2, para que de esta forma se llegue al cuarto paso en el cual se definen los controles aplicables en la presente propuesta. El resumen de la misma se muestra en la Imagen No 5.

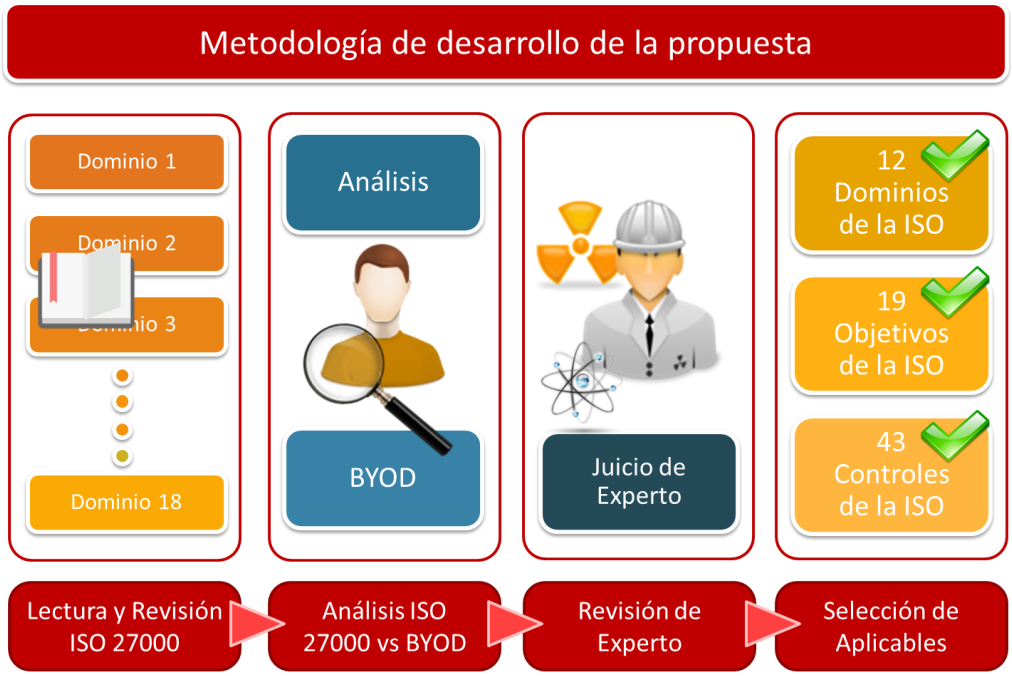

Imagen 5 Método de Selección del Modelo Propuesto
Fuente: Propia

El anexo No 1 ilustra la ejecución de los pasos 2 y 3 de la metodología. Como resultado se seleccionaron 12 dominios y 43 controles de la ISO 27002:2013, adicionalmente se aportaron 2 dominios y 2 controles que no son planteados por la ISO 27002:2013 complementando el marco propuesto de acuerdo con nuestra experiencia. Se especifican al detalle en el anexo No 1. El resumen se muestra en la imagen No 6.

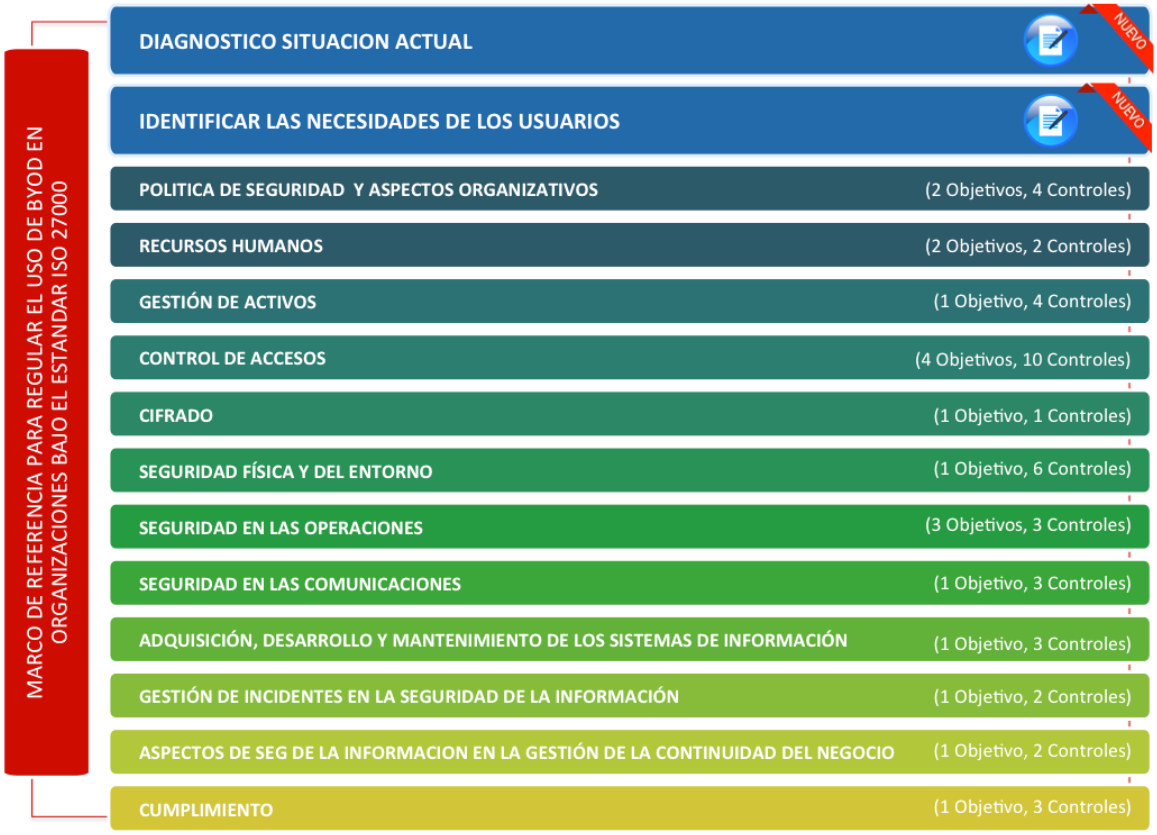

Imagen 6 Marco de Referencia BYOD
Fuente: Propia

A continuación se detallan los dominios propuestos.

3.1 Diagnóstico situación Actual

Se requiere realizar un diagnóstico actual de la organización con el fin de determinar:

- ¿Cuáles son los usuarios que utilizan sus dispositivos móviles?
- ¿Qué aplicaciones propias de la organización emplean?

- ¿Qué mecanismos o herramientas emplean para acceder a la red corporativa?
- ¿Qué tipo de dispositivos son utilizados para realizar sus labores?

Esto permitirá identificar rápidamente que activos de información están siendo accedidos y de qué forma se está realizando el acceso. El diagnóstico de la situación actual incluye la revisión y análisis de los procesos operativos y tecnológicos que conllevan el uso de BYOD en el ambiente empresarial, permitiendo la identificación de oportunidades de mejora en estos dos ítems.

3.2 Identificar las Necesidades de los Usuarios.

En las organización existen diferentes tipos de usuarios con diferentes necesidades para el uso de BYOD; se toma en consideración lo propuesto por Cisco: "*Una recomendación es realizar un análisis de segmentación de usuarios dentro de la empresa para ayudar a entender necesidades y el nivel probable de apoyo requerido"* (Cisco Systems, 2013) como se muestra en la Imagen 7.

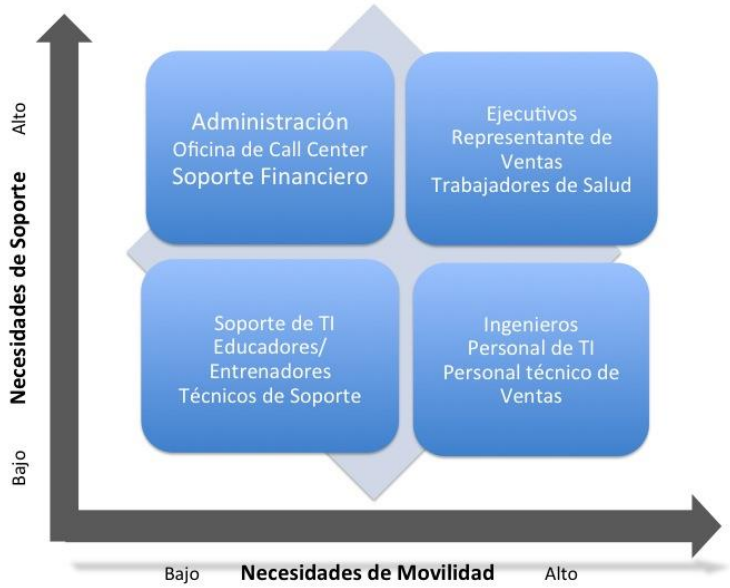

Imagen 7 Segmentación de Usuarios y Necesidades
Fuente: (Cisco Systems, 2013)

Con esta segmentación se realiza una caracterización de necesidades de acuerdo al segmento que pertenece, simplificando la identificando del alcance deseado.

3.3 Política de Seguridad

BYOD no es sinónimo de "ser libre para todo" (Mathias, 2014); es necesario delimitar el alcance para el uso de estos dispositivos mediante una política de seguridad para BYOD, la cual debe estar apoyada por la alta dirección. Esta política contiene las decisiones corporativas sobre los aspectos relacionados con el uso de dispositivos para acceder y utilizar los recursos de la organización. Teniendo en cuenta lo planeado anteriormente, la ISO 27002:2013 contiene el dominio "**5 Política de Seguridad**" con el ítem de control "**5.1 Dirección de Gestión para la Seguridad de la Información**" el cual tiene como *objetivo la orientación y apoyo a la seguridad de la información de acuerdo con los requerimientos del Negocio y a la reglamentación que rige a la organización"* (International Standard, 2013). Específicamente, para el manejo de dispositivos móviles, se tiene el dominio "**6 Organización de la seguridad de la información"** con el ítem de control **"6.2 Los dispositivos móviles y el teletrabajo"** cuyo objetivo *es garantizar la seguridad del teletrabajo y el uso de dispositivos móviles* (International Standard, 2013).

Es necesario garantizar el alcance de implementar esta Política y los escenarios que se verán impactados por el uso de BYOD, abarcando temas específicos de la organización como: ¿a qué activos de información podrán acceder?, ¿Qué tipo de dispositivos serán permitidos?, ¿ Qué Pasos se deben seguir al momento de presentarse la pérdida o robo del dispositivo?, entre otras.

Esta política debe ser revisada, evaluada, comunicada y ajustada periódicamente.

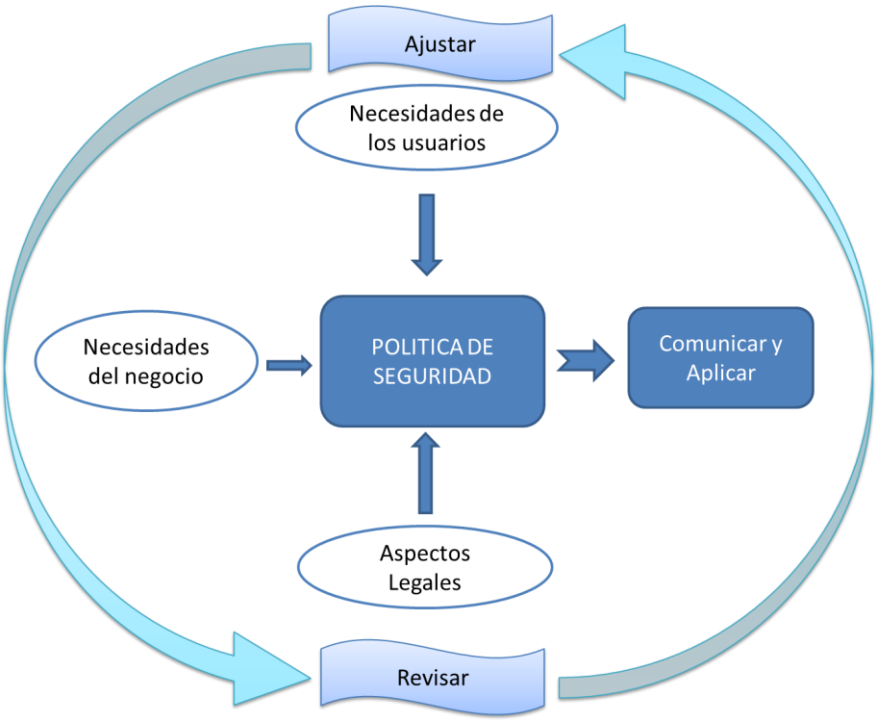

Imagen 8 Política de Seguridad
Fuente: Propia

3.4 Recursos Humanos

Los empleados y contratistas viven diferentes momentos en las organizaciones, durante el proceso de contratación, como empleados activos y cuando se termina el vínculo laboral. Para el caso de BYOD se establecerán los lineamientos para los momentos en que el empleado está activo, y en la terminación del vínculo laboral. Estos ítems son abarcados en la ISO 27002:2013 en el dominio "**7 Seguridad en los Recursos Humanos".**

Durante el vínculo laboral, la ISO 27002:2013 contiene el objetivo de control "**7.2 Durante el Empleo"** enfocando en *Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información* (International Standard, 2013). Para ello es necesario asegurar que los empleados y contratistas, sin importar su nivel jerárquico, sean conscientes de las amenazas

y vulnerabilidades de seguridad de la información que conlleva el uso de BYOD, ayudando así a reducir los riesgos. Buscando que esto se lleve a cabo, la organización deberá generar programas de concientización, educación y formación en seguridad de la información utilizando los BYOD.

Durante la terminación del vínculo laboral, la ISO 27002:2013 contiene el objetivo de control **"7.3 Terminación y cambio de empleo"** cuyo objetivo *es proteger los intereses de la organización como parte del proceso de cambiar o terminar empleo* (International Standard, 2013). Para ello se deberá establecer los procedimientos necesarios para garantizar la adecuada devolución de los activos de información a los que tenía acceso el empleado, así como también la anulación de los permisos de acceso.

El principal objetivo es proteger los activos de información que los empleados o contratistas accederán desde sus dispositivos, con el fin de garantizar su uso adecuado y su devolución en el momento oportuno.

3.5 Gestión de Activos

El objetivo principal de este punto es establecer los lineamientos necesarios para la adecuada gestión de los activos de información de la Organización que serán utilizados por los BYOD. Este ítem es abarcado en la ISO 27002:2013 en el domino **"8 Responsabilidad de los activos",** el cual permitirá identificar y controlar las amenazas y vulnerabilidades sobre los activos de información que sean fuente directa o indirecta para los BYOD. Adicionalmente se plantean los siguientes pasos para una adecuada gestión:

- **Identificación de Activos:** El punto de partida es la identificación de los activos de información que estarán disponibles para los BYOD; esto

permitirá la agrupación de los recursos que tengan características comunes y que se pueda aplicar la misma estrategia de seguridad simplificando el proceso.

- **Clasificación de Activos:** Es necesario analizar cada activo de información para determinar los niveles de criticidad, disponibilidad y confidencialidad, y ordenarlos de acuerdo con su importancia.

- **Análisis de riesgos de los activos de Información:** Para cada grupo de activos se realiza una evaluación de riesgos. Se toman como referencia los pasos planteados en la tesis "*Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización"* (Fernando C., 2012)*:*
    1. Identificación de los riesgos tecnológicos a los que se está expuesto.
    2. Identificación de Controles
    3. Valoración de riesgos (probabilidad e impacto)

- **Gestión:** Consiste en la elaboración, ejecución y seguimiento de las estrategias para la mitigación de los riesgos a los que se exponen los activos de información por el uso de BYOD, buscando una utilización adecuada de los activos de información.

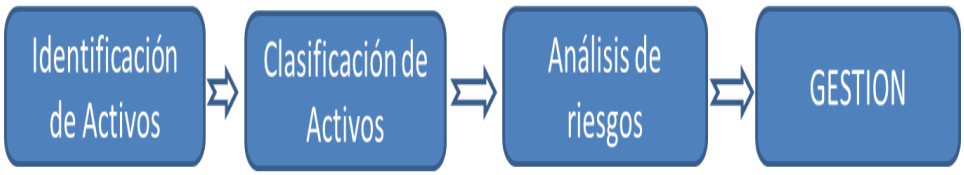

Imagen 9 Gestión de Activos
Fuente: Propia

3.6 Control de Acceso

El objetivo principal en este punto es el de controlar el acceso a la información desde los BYOD. Estos controles deberán ser definidos por los propietarios de los activos respaldados por la política de seguridad. Este ítem es abarcado en la ISO 27002:2013 en el dominio **"9 Control de Acceso***".* Para el caso de BYOD son aplicables los ítems de control **"9.1 Requerimientos de Negocio para el Control de Acceso", "9.2 Gestión de Accesos de Usuario"**, **"9.3 Responsabilidades del Usuario"** y **"9.4 Control de Acceso de Sistemas y Aplicaciones"**, tal como se muestra en el anexo **1.**

Además de lo anterior, la gestión de acceso a usuarios consiste en establecer los procedimientos para controlar la asignación, el mantenimiento y la eliminación de permisos de acceso a los activos de información.

Se aclara también que los usuarios deberán ser conscientes y responsables de los controles de acceso a los activos de información que tienen a su disposición. Para el control de acceso a sistemas y aplicaciones, se deberán utilizar dispositivos o métodos de seguridad con el objetivo de restringir o limitar la entrada a los sistemas, aplicaciones y su información; en pocas palabras, solo se debe permitir el acceso al personal autorizado.

3.7 Claves

El objetivo principal es establecer los lineamientos necesarios para un adecuado manejo de las claves de cifrado de acceso, tanto para el administrador del sistema como para el usuario que utilizará su dispositivo personal. Este ítem se abarca en la ISO 27002:2013 en el domino **"10 Criptografía".**

Comprende las reglas de la organización que establecen el modo de generación, almacenamiento, distribución, eliminación, actualización y recuperación de las claves de acceso a los activos de información desde los BYOD, estableciendo así los responsables y actividades para la ejecución de cada una de estas tareas.

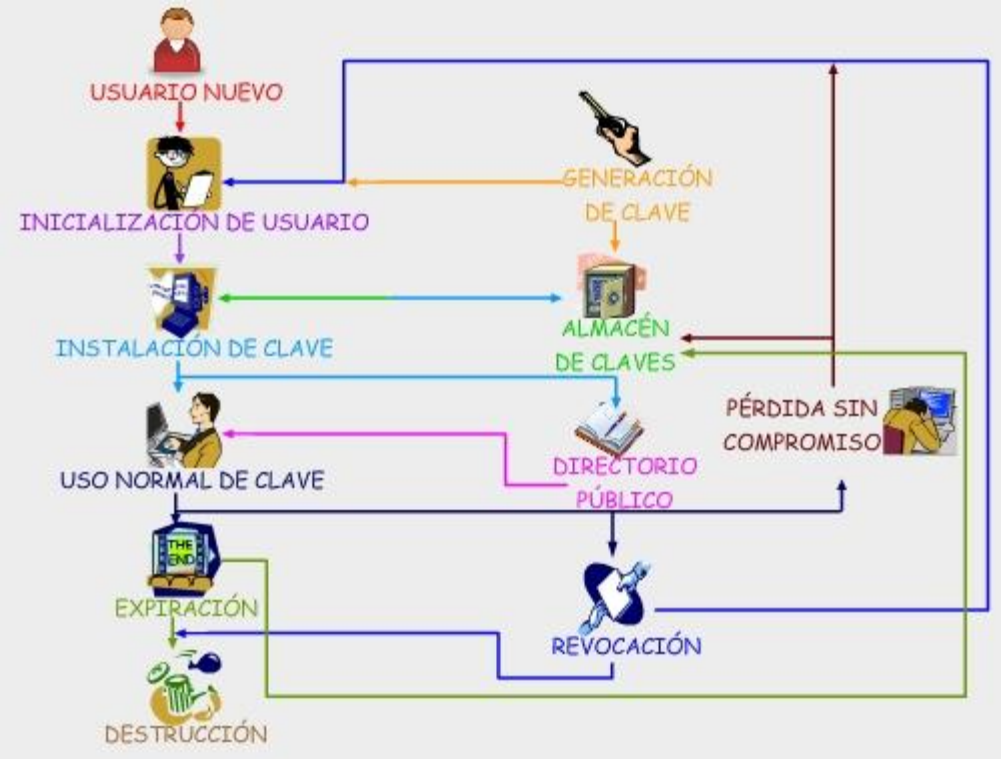

Imagen 10 Ciclo de vida de las contraseñas
Fuente: (Martínez, 2012)

3.8 Seguridad Física y del Entorno

Su objetivo principal es la implementación de barreras físicas y procedimientos de control para evitar la pérdida, daño, robo o puesta en peligro de los activos de información. Este ítem se abarca en la ISO 27002:2013 en el dominio ***"11 Seguridad Física y del Entorno".***

Se deberán implementar controles para mitigar el riesgo contra el acceso no autorizado a los activos de la organización accedidos desde los dispositivos personales y su protección contra la pérdida o robo.

3.9 Seguridad en las Operaciones

Consiste en asegurar la operación correcta y segura de los activos de información. Este ítem se abarca en la ISO 27002:2013 en el domino ***"12* Seguridad en las Operaciones*".*** Para el caso de BYOD son aplicables los ítem de control "**12.2 Protección contra Software Malicioso**", "**12.4 Registro y Monitoreo**" y "**12.6 Gestión de Vulnerabilidades Técnicas**" como se muestra en el anexo **1.**

Para la protección contra software malicioso, se debe tener cuidado en prevenir y detectar programas maliciosos en los dispositivos personales que son utilizados para acceder a activos de información de la organización. Los propietarios de los dispositivos deberán conocer los peligros que ocasiona este tipo de software y los departamentos de TI deberán introducir controles y medidas especiales para detectar y evitar este tipo de software.

El registro y monitoreo de los dispositivos BYOD deberá estar a cargo del departamento de TI y este a su vez tendrá registrar los eventos de seguridad. Esta información podrá ser utilizada para verificar la efectividad de los controles adoptados, así como también la identificación de nuevos riesgos. Lo anterior busca cumplir con los requerimientos legales en lo que respecta al monitoreo y registro debido a que los dispositivos BYOD no son de la organización.

Para la gestión de gestión de vulnerabilidades Técnicas, se deberá obtener de manera oportuna las posibles vulnerabilidades a las cuales los activos de

información se exponen al ser accedidos desde los BYOD, de tal forma que se tomen medidas para mitigar los riesgos.

3.10 Redes

Se debe garantizar la protección de la información en las redes de la organización a las cuales se conectarán los dispositivos BYOD. Este ítem se abarca en la ISO 27002:2013 en el domino ***"13 Seguridad en las Comunicaciones".***

La gestión de la seguridad en las redes desde el concepto BYOD no sólo abarca las redes internas de la organización; se debe considerar cómo estos dispositivos pueden acceder a recursos de la organización desde redes externas sin comprometer la seguridad.

3.11 Requerimientos de Seguridad de Sistemas de Información

Su objetivo es asegurar la seguridad de la información de los sistemas durante todo su ciclo de vida. Este ítem se abarca en la ISO 27002:2013 en el dominio **"14 Adquisición, Desarrollo y Mantenimiento de Sistemas"** bajo el control **"14.1 Requerimientos de Seguridad de Sistemas de Información".**

Se deberán identificar los requisitos de seguridad que impliquen el uso de BYOD antes, durante y después del desarrollo e implementación de sistemas de información.

3.12 Reporte de Eventos y Debilidades de Seguridad de la Información

Su objetivo es asegurar que los eventos y las debilidades de la seguridad de la información, asociados con los sistemas de información, se comuniquen de forma tal que permitan tomar las acciones correctivas oportunamente. Este ítem se

abarca en la ISO 27002:2013 en el domino "**16 Gestión de Incidentes de Seguridad de la Información**"

Es fundamental que todos los empleados, contratistas y clientes que hagan uso de BYOD reporten eventos y debilidades de seguridad observados lo más pronto posible, para mitigar así los riesgos que esto pueda conllevar.

3.13 Revisiones de Seguridad de la Información

Su objetivo garantiza que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos de la organización. Este ítem se abarca en la ISO 27002:2013 en el domino **"18 Cumplimiento".**

Para el cumplimiento de este punto es necesario establecer periodos de validación de la seguridad de la información, determinando así el cumplimiento de las políticas y procedimientos aplicables a BYOD.

4. MODELO DE MADUREZ PROPUESTO

Un modelo de madurez y de capacidad (Capability Maturity Model, CMM) se centra en mejorar los procesos de una organización. Contiene los elementos esenciales de los procesos eficaces de una o más disciplinas, y describe un camino evolutivo de mejora de procesos ad hoc e inmaduros, hacia procesos disciplinados y maduros con calidad y eficacia mejoradas. (Software Engineering Institute, 2010).

Teniendo en cuenta el Modelo Propuesto en el capítulo 3, se hace necesaria la elaboración de un instrumento para determinar el nivel de madurez de la organización con respecto al modelo propuesto. Esto permitirá identificar debilidades, fortalezas y establecer los puntos críticos para el mejoramiento continuo de los procesos de seguridad referentes al uso de BYOD en la organización. Para determinar el nivel de madurez se propone un modelo de madurez basado en entrevistas.

4.1 Descripción del Proceso

El Modelo de Madurez Propuesto (MMP) involucra a los responsables de procesos del área de tecnología, proponemos una agrupación de funciones como se ilustrada en la imagen No 11 con respecto a los dominios propuestos en el capítulo 3, que están caracterizadas de la siguiente manera:

- **Dimensión de Gobierno**: Está definida por el conjunto estructurado de actividades que realiza el área de TI en coordinación con la alta dirección, para orientar el área en función de los objetivos estratégicos del negocio y los requisitos legales.

- **Dimensión de Desarrollo y Arquitectura:** Está definida por el conjunto de actividades usados para estructurar, planificar y controlar el desarrollo o adquisición de software en la organización.
- **Dimensión de Seguridad:** Está definida por el conjunto de actividades para minimizar y mitigar los riesgos de los activos de información.
- **Dimensión de Infraestructura:** Está definida por el conjunto de actividades usadas para estructurar, planificar y controlar el hardware, comunicaciones, servidores, base de datos, entre otros.

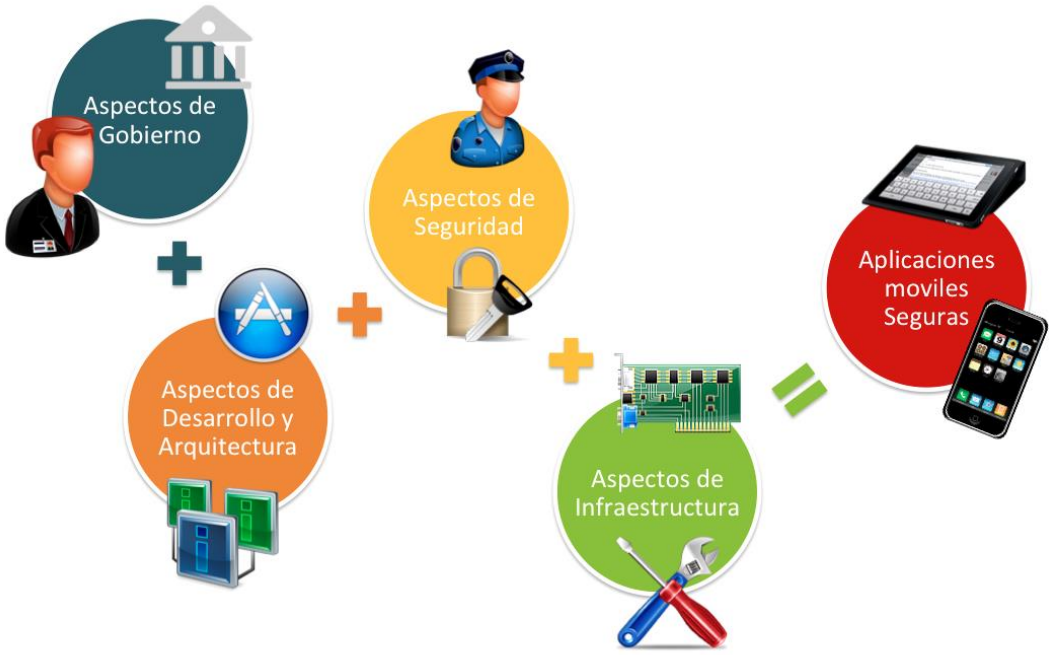

Imagen 11 Áreas de TI
Fuente: Propia

El enfoque multidimensional del modelo propuesto se centra en identificar a los interesados y efectuar encuestas, según el cargo o responsabilidad del entrevistado sobre los servicios de TI en la organización. En estas entrevistas se pretende conocer el estado de la seguridad de la Información en la

organización, y las expectativas en el alcance de la implementación de BYOD.

El MMP propone, inicialmente, identificar el personal de TI que corresponde a las dimensiones que se muestran en la imagen 11. Para cada dimensión se plantean las funciones respectivas en el numeral 4.2, proporcionando un panorama completo desde las funciones de las áreas de Tecnología e Informática en las organizaciones. Una vez identificado el personal, se efectúa una serie de preguntas claves que ayudan a identificar el nivel de madurez en cada uno de los dominios propuestos en el capítulo 3. Las preguntas de la encuestas se seleccionaron efectuando un mapeo entre los roles y los controles que aplican para regular el uso de BYOD, tal como se muestra en la tabla 2. Con base en las respuestas dadas, se realiza un análisis para identificar el nivel de madurez de cada uno de los dominios, teniendo una perspectiva del estado actual de la organización en el uso de BYOD. Este proceso se muestra en la imagen No 12.

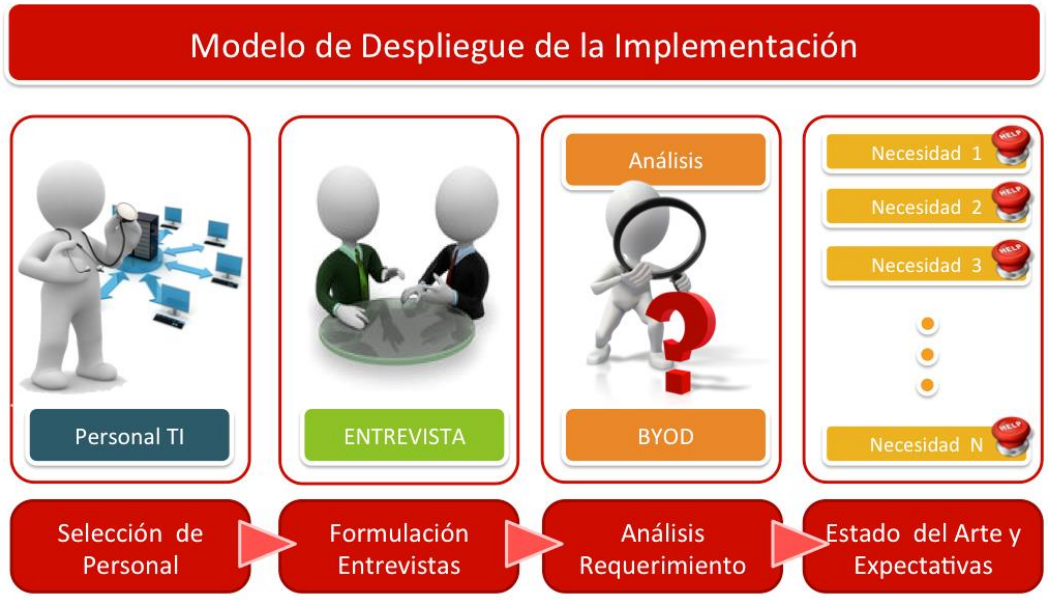

Imagen 12 Modelo de Despliegue de la Implementación
Fuente: Propia

Tabla 2 Roles con respecto a Dominios

DOMINIOS	Área de Gobierno	Area de Desarrollo Y Arquitectura	Área de Seguridad	Área de Infraestructura
DIGANOSTICO SITUACION ACTUAL	1			
IDENTIFICAR LAS NECESIDADES DE LOS USUARIOS	1			
POLÍTICAS DE SEGURIDAD.	2	0	0	0
ASPECTOS ORGANIZATIVOS DE LA S.I.	2	0	2	0
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	0	0	2	0
GESTIÓN DE ACTIVOS.	0	4	0	0
CONTROL DE ACCESOS.	1	5	7	0
CIFRADO.	0	0	1	0
SEGURIDAD FÍSICA Y AMBIENTAL.	1	0	6	0
SEGURIDAD EN LA OPERATIVA.	0	1	3	0
SEGURIDAD EN LAS TELECOMUNICACIONES.	0	0	1	3
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS S.I.	0	0	3	1
GESTIÓN DE INCIDENTES EN LA S.I.	0	0	3	0
ASPECTOS DE SIG EN LA CONTINUIDAD DEL NEGOCIO	0	0	1	1
CUMPLIMIENTO.	4	0	0	0

Nota: Fuente Propia

Se propone un conjunto de criterios que permiten identificar el nivel de madurez de cada uno de los dominios. Estos niveles están diseñados para la descripción de los posibles estados actuales y futuros, y "son un medio para mejorar de forma incremental los procesos que corresponden a un área de proceso dada" (Software Engineering Institute, 2010). Se establecieron cinco (5) niveles, de acuerdo con la tabla 3:

Tabla 3 Niveles de Madurez

Nivel	Nivel de Madurez
Nivel 1	Inexistente
Nivel 2	Informalidad, no comunicado y desorganizado
Nivel 3	Procesos documentados y comunicados
Nivel 4	Procesos monitoreados y medidos
Nivel 5	Buenas prácticas implementadas y repetibles

Nota: Fuente Propia

Se alcanza un nivel de madurez para un dominio específico cuando se satisfacen todas las metas hasta ese nivel. A continuación se presenta una breve descripción de cada uno de los niveles de madurez propuestos, basados en los niveles de madurez de CMMI. (Chrissis, 2011) .

Nivel de Madurez 1: Inexistente

Un nivel de madurez inexistente o 1, indica un proceso que no se realiza, o se realiza parcialmente. Al menos una de las metas del dominio no se cumple. La organización no da prioridad a estas necesidades.

Nivel de Madurez 2: Informalidad, no comunicado y Desorganizado

Un nivel de madurez 2 se caracteriza por la informalidad, la no comunicación y la desorganización. Los procesos son generalmente ad-hoc y caóticos; no se genera un entorno estable para dar soporte a los procesos que corresponden a los dominios. Nacen por la iniciativa de personal de T.I que quiere mejorar en algunas áreas puntuales, no son comunicados a la organización y los efectúan en forma desordenada.

Nivel de Madurez 3: Procesos documentados y comunicados

En el nivel de madurez 3, se garantiza que los procesos están documentados y son conocidos por toda la organización. Los procesos se planifican y se ejecutan de acuerdo con lo documentado para producir resultados controlados. Estos procesos están bien caracterizados y comprendidos y se describen en estándares, procedimientos, herramientas y métodos.

Nivel de Madurez 4: Procesos monitoreados y medidos

En el nivel de madurez 4, se establecen objetivos cuantitativos para la calidad y cumplimiento de los procesos. La calidad y el cumplimiento se interpretan en términos estadísticos y cuantitativos.

Nivel de Madurez 5: Buenas prácticas implementadas y repetibles

En el nivel de madurez 5, la organización efectúa mejora continua de los procesos basados en una comprensión cuantitativa. El análisis de los datos ayudan a identificar deficiencias en el cumplimiento de los objetivos; estas deficiencias se utilizan para el mejoramiento de los procesos.

Las organizaciones pueden lograr mejoras progresivas en su madurez consiguiendo primero el control a nivel de proyecto y continuando hasta el nivel más avanzado (gestión de rendimiento y mejora continua de procesos en toda la organización) utilizando datos tanto cualitativos como cuantitativos para la toma de decisiones. (Software Engineering Institute, 2010).

4.2 Descripción de los perfiles

El departamento de TI de una organización cuenta con un conjunto de actividades que están directamente asociadas con el comportamiento que se espera de los individuos que ocupan determinados posiciones dentro de la organización . Estas funciones pueden ser conocidas por el individuo debido a la información que tiene del proceso técnico y de las tareas, o se le dan a conocer mediante manuales que la organización elabora con tal fin. Para nuestro propósito se establecieron cuatro (4) perfiles específicos que agrupan el conjunto de todas las tareas que se realizan en el Departamento de T.I: Gobierno, Desarrollo y arquitectura, Seguridad e Infraestructura. A continuación se describen las funciones de cada uno de los perfiles.

4.2.1 Perfil de Gobierno

El perfil de gobierno comprende el personal encargado del conjunto de actividades que realiza el área de TI en coordinación con la alta dirección, para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.

Entre sus responsabilidades están:

- Participación en las decisiones estratégicas de la compañía que involucren sistemas de información.
- Alinear los recursos tecnológicos con los objetivos de la organización.
- Gestionar adecuadamente las necesidades y solicitudes de los clientes internos y externos.
- Definir y ejecutar adecuadamente el presupuesto, de acuerdo con los lineamientos de la organización.
- Mantener las relaciones con proveedores.

- Gestionar los recursos humanos del departamento de tecnología.

Las preguntas asociadas con este perfil para la identificación del estado de madurez es:

Tabla 4 Preguntas del Perfil Gobierno

MODELO DE MADUREZ								
Formato de Madurez Dimensión de Gobierno								
Empresa								
Realizado Por:		**FECHA**						
Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no esta comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.								
ID	**PREGUNTAS**	**CONTROLES DE LA ISO 27002**	**NIVEL DE MADUREZ**					
			1	**2**	**3**	**4**	**5**	
PG-1	Plan para verificar si los empleados o contratistas hacen uso de sus dispositivos personales para acceder a sistemas de información.	N/A						
PG-2	Plan para determinar las necesidades de utilización de BYOD de los empleados o contratistas.	N/A						
PG-3	Políticas de seguridad de la información que apliquen a dispositivos BYOD.	5.1.1 y 6.2.1						
PG-4	Esquema de Teletrabajo para BYOD	6.2.2						
PG-5	Auditoria de Seguridad Externa	18.1.1						
PG-6	Verificaciones de cumplimientos de las políticas de seguridad	18.1.2						
PG-7	Auditorías internas de seguridad	18.1.3						

Nota: Fuente Propia

4.2.2 Perfil de Desarrollo y Arquitectura

El perfil de desarrollo y arquitectura comprende el personal encargado de la adquisición o desarrollo de software para los sistemas de información.

Entre sus responsabilidades están:

- Analizar las necesidades de información de las diferentes áreas de la organización.
- Planear, desarrollar o adquirir nuevas aplicaciones de acuerdo a las necesidades de la organización.
- Definir y verificar las normas de calidad de software en todas las etapas del desarrollo e implantación.
- Asegurar que los sistemas sean operados en forma adecuada por los usuarios de los diferentes procesos.
- Apoyar a los usuarios en el uso y explotación de la información

Las preguntas asociadas a este perfil para la identificación del estado de madurez son:

Tabla 5 Preguntas Perfil de Desarrollo y Arquitectura

MODELO DE MADUREZ			
Formato de Madurez Dimensión de Desarrollo y Arquitectura			
Empresa			
Realizado Por:		**FECHA**	
Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no está comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.			
ID	**PREGUNTAS**	**CONTROLES DE LA ISO 27002**	**NIVEL DE MADUREZ**
			1 **2** **3** **4** **5**

PDA-1	Levantamiento de requerimientos de seguridad para los sistemas de información que serán accedidos desde los BYOD antes de la adquisición, desarrollo o mejora de los sistemas.	14.1.1					
PDA-2	servicios de conexión segura VPN para la conexión de equipos BYOD desde el exterior a aplicaciones o servicios de la organización.	14.1.2					
PDA-3	Certificados o firmas electrónicas para la encriptación de las comunicaciones entre las aplicaciones y los BYOD.	14.1.3					

Nota: Fuente Propia

4.2.3 Perfil de Seguridad

El perfil de seguridad comprende el personal encargado de minimizar y mitigar los riesgos de los activos de información.

Entre sus responsabilidades están:

- Gestionar adecuadamente los riesgos según el impacto de los activos de información.
- Garantizar el cumplimiento de las políticas y controles de la seguridad de la información.
- Definir las especificaciones de seguridad de los sistemas de información.
- Garantizar el cumplimiento de las regulaciones legales que rigen la organización con referente a la seguridad de la información.
- Mitigar y controlar los riesgos de seguridad de la información.

Las preguntas asociadas a este perfil para la identificación del estado de madurez son:

Tabla 6 Preguntas Perfil de Seguridad

MODELO DE MADUREZ			
Formato de Madurez Dimensión de Seguridad			
Empresa			
Realizado Por:		**FECHA**	

Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no está comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.

ID	PREGUNTAS	CONTROLES DE LA ISO 27002	NIVEL DE MADUREZ				
			1	2	3	4	5
PS-1	Capacitado a los colaboradores concientización del uso de sus dispositivos personales para desempeñar tareas de su trabajo.	7.2.2					
PS-2	Métodos, esquemas, para proteger los activos de información del uso de dispositivos personales, cuando se presenta un despido o un cambio de puesto.	7.3.1					
PS-3	Asignación de acceso y políticas de privilegios por cargos para dispositivos BYOD	9.2.2					
PS-4	asignación de la información secreta "Contraseñas", mediante algoritmos de encriptación para dispositivos BYOD	9.2.4					
PS-5	Revisión de los permisos asignados a los dispositivos BYOD	9.2.5					
PS-6	Herramientas o sistemas de información para adicionar o retirar permisos o privilegios al personal que utilice dispositivos BYOD.	9.2.6					
PS-7	Conocen los usuarios la exigencia sobre las prácticas de autenticación existentes que rigen para dispositivos BYOD	9.3.1					
PS-8	Métodos y procedimientos de control de acceso para dispositivos BYOD, de acuerdo a la política de control de acceso.	9.4.1					
PS-9	Procedimientos para el inicio de sesión a aplicativos o sistemas de la compañía desde BYOD.	9.4.2					
PS-10	Los sistemas de gestión de contraseñas también gestionan conexiones de dispositivos BYOD.	9.4.3					
PS-11	Política y métodos para la gestión de claves específicas para los dispositivos BYOD.	10.1.2					
PS-12	Políticas y metodologías que especifiquen las medidas de seguridad generales (robo, incendios, perdidas) para dispositivos BYOD relacionados a la organización.	11.2.1					

PS-13	Políticas, métodos o sistemas de información para proteger los activos usados fuera de las instalaciones de la compañía por dispositivos BYOD.	11.2.5					
PS-14	Políticas, métodos o sistemas de información para proteger los dispositivos BYOD usados en tareas de la compañía y fuera de la misma.	11.2.6					
PS-15	Métodos o sistema de información para la eliminación de datos sensibles o software de la compañía en los dispositivos BYOD.	11.2.7					
PS-16	Métodos o sistemas para asegurar que los dispositivos personales de los usuarios desatendidos cuentan con la protección adecuada.	11.2.8					
PS-17	Métodos o sistemas de información para puesto de trabajo despejado y bloque de pantalla enfocado en los dispositivos BYOD.	11.2.9					
PS-18	Se exige o se entrega software Antivirus en los dispositivos BYOD.	12.2.1					
PS-19	Se registran los eventos de seguridad y se toman medidas para contrarrestar en el ámbito BYOD.	12.4.1					
PS-20	Medidas para mitigar las vulnerabilidades en los sistemas de información detectadas en el ámbito BYOD.	12.6.1					
PS-21	Métodos de reporte de eventos o debilidades de seguridad.	16.1.2					
PS-22	Métodos de reporte de debilidades de seguridad	16.1.3					

Nota: Fuente Propia

4.2.4 Perfil de Infraestructura

El perfil de infraestructura comprende el personal encargado de las actividades usadas para estructurar, planificar y controlar el hardware, comunicaciones, servidores, base de datos, entre otros.

Entre sus responsabilidades están:

- Planificar y coordinar la implementación y funcionamiento efectivo de los servicios de base de datos, sistemas operativos, backups, y aplicaciones.

- Gestionar los servicios de TI suministrados a través de la infraestructura tecnológica.
- Diseñar planes de contingencia y continuidad de los sistemas de información.
- Monitorear y verificar los sistemas de información para garantizar el correcto funcionamiento.
- Gestionar, diseñar, mantener e implementar redes LAN / WAN.
- Gestionar, diseñar, mantener e implementar el Data Center.

Las preguntas asociadas a este perfil para la identificación del estado de madurez son:

Tabla 7 Preguntas Perfil de Infraestructura

MODELO DE MADUREZ								
Formato de Madurez Dimensión de Infraestructura								
Empresa								
Realizado Por:		**FECHA**						
Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no esta comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.								
ID	**PREGUNTAS**	**CONTROLES DE LA ISO 27002**	**NIVEL DE MADUREZ**					
			1	**2**	**3**	**4**	**5**	
PI-1	Registro de todos los activos de la organización y están relacionados a u su posible uso desde BYOD.	8.1.1						
PI-2	Identificación de responsables para los activos de información que sean utilizados por los BYOD.	8.1.2						
PI-3	Comunicado y capacitado a los responsables de la información para un uso aceptable desde los BYOD.	8.1.3						
PI-4	Herramientas o sistemas de información para asegurar los activos de información en los dispositivos BYOD cuando se presente un cese laboral.	8.1.4						

PI-5	Política de control de Acceso está incluido el acceso de los BYOD.	9.1.1					
PI-6	Control de acceso a redes internas y aplicativos de la compañía para dispositivos BYOD.	9.1.2					
PI-7	Controles de RED para los BYOD.	13.1.1					
PI-8	Controles para la conexión a la RED para los dispositivos BYOD (Firewall, Autenticación).	13.1.2					
PI-9	Segregación de red (VLAN) de acuerdo a la necesidad de servicios que desean acceder los BYOD.	13.1.3					

Nota: Fuente propia.

5. EVALUACIÓN DE UNA EMPRESA EN BASE AL MODELO DE MADUREZ PROPUESTO

5.1 Selección de la Empresa

Una vez realizado el Modelo de Madurez Propuesto (MMP) se realizó una prueba del modelo a una empresa del sector Solidario de la ciudad de cali, con una trayectoria de 40 años brindando servicios que propenden por el mejoramiento de la calidad de vida y el bienestar integral a sus asociados. Hoy es una organización que presenta un crecimiento sostenido y gran solidez patrimonial, producto de un proceso de planificación desarrollado a través de cada uno de los imperativos que componen el Direccionamiento Estratégico. Ellos son: Crecimiento, Posicionamiento, Desarrollo y Fortalecimiento Institucional, Desarrollo Económico-Social del médico y Responsabilidad Social. Se ha consolidado como la entidad solidaria más importante, con mayor liderazgo y proyección a nivel nacional.

Se seleccionó esta empresa por tener un gran acercamiento con el departamento de tecnología e Informática, adicionalmente la empresa se encuentran en un proceso de aseguramiento de la información por lo cual este análisis le contribuirá en dicho proceso.

5.2 Diagnóstico de las dimensiones

5.2.1 Diagnóstico de madurez en la dimensión de Gobierno

Para evaluar el nivel de madurez en la dimensión de Gobierno en empresa se realizaron las siguientes actividades:

1. Se identificó la persona que ejecuta las funciones descritas en el punto 4.2.1 para determinar el responsable de Gobierno.
2. Se tomó como referencia la encuesta de la tabla 3 para analizar y determinar la evolución del nivel de madurez real de la organización, obteniendo como resultado la encuesta de la dimensión de Gobierno.

Tabla 8 Resultado Encuesta Dimensión Gobierno

MODELO DE MADUREZ			
Formato de Madurez Dimensión de Gobierno			
Empresa			
Realizado Por:		**FECHA**	

Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no esta comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.

ID	PREGUNTAS	CONTROLES DE LA ISO 27002	NIVEL DE MADUREZ				
			1	2	3	4	5
PG-1	Plan para verificar si los empleados o contratistas hacen uso de sus dispositivos personales para acceder a sistemas de información.	N/A	X				
PG-2	Plan para determinar las necesidades de utilización de BYOD de los empleados o contratistas.	N/A	X				
PG-3	Políticas de seguridad de la información que apliquen a dispositivos BYOD.	5.1.1 y 6.2.1	X				
PG-4	Esquema de Teletrabajo para BYOD	6.2.2	X				
PG-5	Auditoria de Seguridad Externa	18.1.1		X			
PG-6	Verificaciones de cumplimientos de las políticas de seguridad	18.1.2		X			
PG-7	Auditorías internas de seguridad	18.1.3	X				

Nota: Fuente Propia.

5.2.2 Diagnóstico de madurez en la dimensión de Desarrollo y Arquitectura

Para evaluar el nivel de madurez en la dimensión de Desarrollo y arquitectura en la empresa se realizaron las siguientes actividades:

1. Se identificó la persona que ejecuta las funciones descritas en el punto 4.2.3 para determinar el responsable de desarrollo y arquitectura.
2. Tomado como referencia la encuesta de la tabla 5 para analizar y determinar la evolución del nivel de madurez real de la organización. Obteniendo como resultado la encuesta de la dimensión de Desarrollo y Arquitectura.

Tabla 9 Resultado Encuesta Desarrollo y Arquitectura

MODELO DE MADUREZ								
Formato de Madurez Dimensión de Desarrollo y Arquitectura								
Empresa								
Realizado Por:		**FECHA**						
Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no esta comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.								
ID	**PREGUNTAS**	**CONTROLES DE LA ISO 27002**	**NIVEL DE MADUREZ**					
			1	**2**	**3**	**4**	**5**	
PDA-1	Levantamiento de requerimientos de seguridad para los sistemas de información que serán accedidos desde los BYOD antes de la adquisición, desarrollo o mejora de los sistemas.	14.1.1			**X**			
PDA-2	servicios de conexión segura VPN para la conexión de equipos BYOD desde el exterior a aplicaciones o servicios de la organización.	14.1.2			**X**			
PDA-3	Certificados o firmas electrónicas para la encriptación de las comunicaciones entre las aplicaciones y los BYOD.	14.1.3			**X**			

Nota: Fuente Propia

5.2.3 Diagnóstico de madurez en la dimensión de Seguridad

Para evaluar el nivel de madurez en la dimensión de Seguridad en la empresa se realizaron las siguientes actividades:

1. Se identificó la persona que ejecuta las funciones descritas en el punto 4.2.4 para determinar el responsable de Seguridad.
2. Tomado como referencia la encuesta de la tabla 6 para analizar y determinar la evolución del nivel de madurez real de la organización. Obteniendo como resultado la encuesta de la dimensión de Seguridad.

Tabla 10 Resultado Encuesta Dimensión Seguridad

MODELO DE MADUREZ								
Formato de Madurez Dimensión de Seguridad								
Empresa								
Realizado Por:		**FECHA**						
Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no esta comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.								
ID	**PREGUNTAS**	**CONTROLES DE LA ISO 27002**	**NIVEL DE MADUREZ**					
			1	**2**	**3**	**4**	**5**
PS-1	Capacitado a los colaboradores concientización del uso de sus dispositivos personales para desempeñar tareas de su trabajo.	7.2.2	**X**				
PS-2	Métodos, esquemas, para proteger los activos de información del uso de dispositivos personales, cuando se presenta un despido o un cambio de puesto.	7.3.1	**X**				
PS-3	Asignación de acceso y políticas de privilegios por cargos para dispositivos BYOD	9.2.2	**X**				
PS-4	asignación de la información secreta "Contraseñas", mediante algoritmos de encriptación para dispositivos BYOD	9.2.4	**X**				
PS-5	Revisión de los premisos asignados a los dispositivos BYOD	9.2.5	**X**				
PS-6	Herramientas o sistemas de información para adicionar o retirar permisos o privilegios al personal que utilice dispositivos BYOD.	9.2.6	**X**				

PS-7	Conocen los usuarios la exigencia sobre las prácticas de autenticación existentes que rigen para dispositivos BYOD	9.3.1	X				
PS-8	Métodos y procedimientos de control de acceso para dispositivos BYOD, de acuerdo a la política de control de acceso.	9.4.1	X				
PS-9	Procedimientos para el inicio de sesión a aplicativos o sistemas de la compañía desde BYOD.	9.4.2	X				
PS-10	Los sistemas de gestión de contraseñas también gestionan conexiones de dispositivos BYOD.	9.4.3	X				
PS-11	Política y métodos para la gestión de claves específicas para los dispositivos BYOD.	10.1.2	X				
PS-12	Políticas y metodologías que especifiquen las medidas de seguridad generales (robo, incendios, perdidas) para dispositivos BYOD relacionados a la organización.	11.2.1	X				
PS-13	Políticas, métodos o sistemas de información para proteger los activos usados fuera de las instalaciones de la compañía por dispositivos BYOD.	11.2.5	X				
PS-14	Políticas, métodos o sistemas de información para proteger los dispositivos BYOD usados en tareas de la compañía y fuera de la misma.	11.2.6	X				
PS-15	Métodos o sistema de información para la eliminación de datos sensibles o software de la compañía en los dispositivos BYOD.	11.2.7	X				
PS-16	Métodos o sistemas para asegurar que los dispositivos personales de los usuarios desatendidos cuentan con la protección adecuada.	11.2.8	X				
PS-17	Métodos o sistemas de información para puesto de trabajo despejado y bloque de pantalla enfocado en los dispositivos BYOD.	11.2.9	X				
PS-18	Se exige o se entrega software Antivirus en los dispositivos BYOD.	12.2.1	X				
PS-19	Se registran los eventos de seguridad y se toman medidas para contrarrestar en el ámbito BYOD.	12.4.1	X				
PS-20	Medidas para mitigar las vulnerabilidades en los sistemas de información detectadas en el ámbito BYOD.	12.6.1	X				
PS-21	Métodos de reporte de eventos o debilidades de seguridad.	16.1.2		X			
PS-22	Métodos de reporte de debilidades de seguridad	16.1.3		X			

Nota: Fuente Propia

5.2.4 Diagnóstico de madurez en la dimensión de Infraestructura

Para evaluar el nivel de madurez en la dimensión de Infraestructura en la empresa se realizaron las siguientes actividades:

3. Se identificó la persona que ejecuta las funciones descritas en el punto 4.2.5 para determinar el responsable de infraestructura.
4. Tomado como referencia la encuesta de la tabla 7 para analizar y determinar la evolución del nivel de madurez real de la organización. Obteniendo como resultado la encuesta de la dimensión de Infraestructura.

Tabla 11 Resultado Encuesta Dimensión Infraestructura

MODELO DE MADUREZ								
Formato de Madurez Dimensión de Infraestructura								
Empresa								
Realizado Por:		**FECHA**						
Instrucciones: Asigne una calificación a cada uno de los siguientes ítems de acuerdo a la escala de valores: Nivel 1: Inexistente, Nivel 2: Existe pero Informal, no esta comunicado y es desorganizado, Nivel 3: El Proceso esta documentados y comunicados, Nivel 4: El proceso esta monitoreado y medido, Nivel 5: Las mediciones se utilizan para la mejora u optimización de los proceso.								
ID	**PREGUNTAS**	**CONTROLES DE LA ISO 27002**	**NIVEL DE MADUREZ**					
			1	**2**	**3**	**4**	**5**
PI-1	Registro de todos los activos de la organización y están relacionados a u su posible uso desde BYOD.	8.1.1	**X**				
PI-2	Identificacion de responsables para los activos de información que sean utilizados por los BYOD.	8.1.2	**X**				
PI-3	Comunicado y capacitado a los responsables de la información para un uso aceptable desde los BYOD.	8.1.3	**X**				
PI-4	Herramientas o sistemas de información para asegurar los activos de información en los dispositivos BYOD cuando se presente un cese laboral.	8.1.4	**X**				
PI-5	Política de control de Acceso está incluido el acceso de los BYOD.	9.1.1	**X**				

PI-6	Control de acceso a redes internas y aplicativos de la compañía para dispositivos BYOD.	9.1.2	X				
PI-7	Controles de RED para los BYOD.	13.1.1	X				
PI-8	Controles para la conexión a la RED para los dispositivos BYOD (Firewall, Autenticación).	13.1.2	X				
PI-9	Segregación de red (VLAN) de acuerdo a la necesidad de servicios que desean acceder los BYOD.	13.1.3	X				

Nota: Fuente Propia

5.3 ANÁLISIS DE LOS RESULTADOS OBTENIDOS

Los resultados obtenidos en la realización de las entrevistas en la empresa desde la dimensión de Dominios se visualizan en la Imagen 13 y con respecto a la dimensión de perfiles se muestra en la imagen 14.

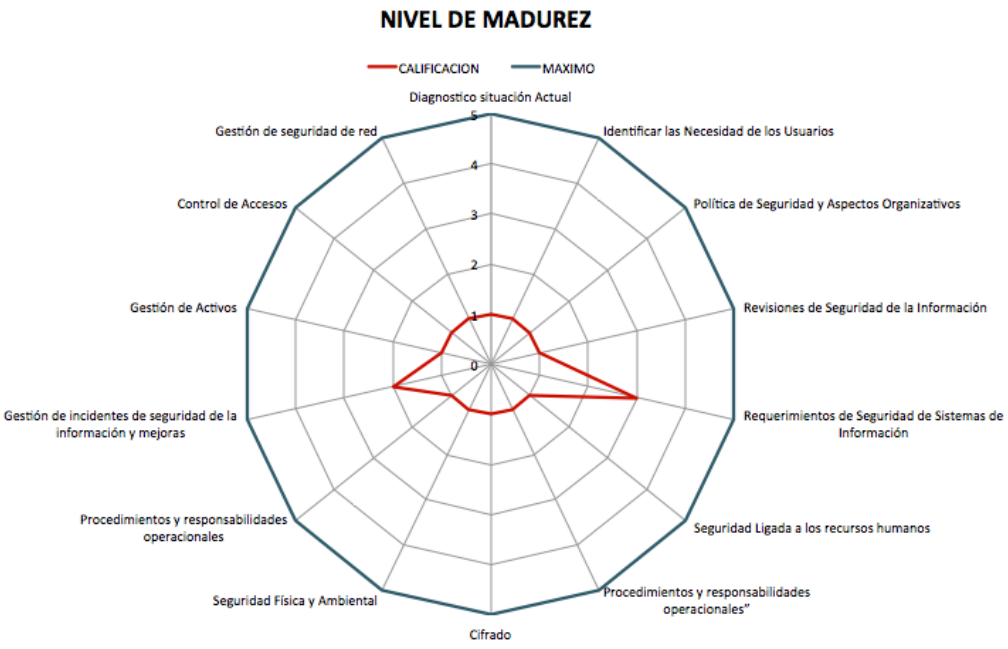

Imagen 13 Resultados Obtenidos de la Evaluación dimensión de Dominios
Fuente: Propia

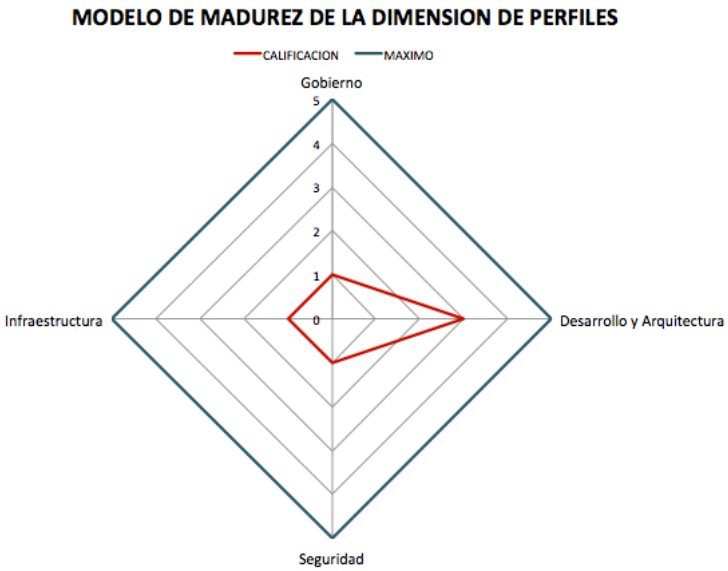

Imagen 14 Resultados Obtenidos de la Evaluación dimensión de Perfiles

Fuente: Propia

A continuación se realiza un análisis desde las dimensiones de Perfiles.

5.3.1 Dimensión de Gobierno

Después de realizar las encuestas para la calificación del MMP en la dimensión de Gobierno, se determinó las actividades que se ejecutan con respecto a los Dominios de "Diagnóstico situación Actual", "Identificar las Necesidad de los Usuarios", "Política de Seguridad y Aspectos Organizativos" y el dominio de "Revisiones de Seguridad de la Información" que corresponden a esta dimensión (Tabla 12).

Para el Dominio "Diagnóstico situación Actual" no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Identificar las Necesidad de los Usuarios” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Política de Seguridad y Aspectos Organizativos” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Revisiones de Seguridad de la Información” se cumplen algunas actividades correspondientes al nivel de madurez 2, pero no se cumplen todas las actividades correspondientes a este nivel por lo tanto su calificación de nivel de madurez es 1.

La interpretación de los resultados para esta dimensión se muestra en la tabla 13, en el formato “***RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE GOBIERNO”***

Tabla 12: Actividades de Gobierno

MODELO DE MADUREZ		
CUMPLIMIENTO DE ACTIVIDADES DE GOBIERNO		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**ACTIVIDADES**	**CUMPLE**
Diagnostico situación Actual	La organización tiene un plan para verificar si los empleados o contratistas hacen uso de sus dispositivos personales para acceder a sistemas de información.	NO
	La organización tiene la documentación de los procedimientos para la identificación de la utilización de dispositivos personales para acceder a sistemas de información de la organización.	NO

	La organización cuentan con KPI's para medir la utilización de dispositivos personales para acceder a sistemas de información de la organización.	NO
	La organización utiliza los KPI's para determinar acciones de seguridad.	NO
Identificar las Necesidad de los Usuarios	La organización cuenta con un plan para determinar las necesidades de utilización de BYOD de los empleados o contratistas.	NO
	La organización Tiene documentado el plan para determinar las necesidades de utilización de BYOD.	NO
	La organización cuenta con KPI's para determinar el grado de necesidad de la utilización de BYOD en la organización.	NO
	La organización utiliza los KPI's para determinar acciones y políticas de seguridad.	NO
Políticas de Seguridad y Aspectos Organizativos	La organización cuenta con políticas de seguridad de la información que apliquen a dispositivos BYOD	NO
	La organización tiene un plan para la revisión de la políticas de seguridad de la información para BYOD	NO
	La organización cuenta con la documentación de las políticas para dispositivos BYOD y su plan de revisión.	NO
	La organización cuenta con KPI's para medir el impacto de las políticas para dispositivos BYOD.	NO
	La organización utiliza estos KPI's para medir mejorar las políticas de BYOD y lo aplican al plan de revisión.	NO
	La organización cuenta con el esquema de teletrabajo.	NO
	La organización tiene Documentado el esquema de teletrabajo, para las áreas, cargos y aplicativos que estén inmersos en el mismo.	NO
	La organización cuenta con KPI's para medir como se está trabajando con el teletrabajo	NO
	La organización utilizan estos KPI's para la mejora u optimización del teletrabajo.	NO
Revisiones de Seguridad de la Información	La organización realiza auditoría de seguridad externa.	SI
	La organización realiza verificaciones de cumplimientos de las políticas de seguridad.	SI
	La organización realiza auditorías internas de seguridad.	NO

	La organización tiene documentados los procesos para las revisiones de seguridad.	NO
	La organización tienen un KPI para las Revisiones y auditorías.	NO
	La organización utiliza los resultados de los KPI's para mejorar y monitorear la revisión de seguridad de la información.	NO

Nota: Fuente Propia

Tabla 13: Resultados de la Evaluación de Madurez de la dimensión de Gobierno

MODELO DE MADUREZ		
RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE GOBIERNO		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**DESCRIPCION DE RESULTADOS**	
	ASPECTOS SATISFACTORIOS	**ASPECTOS POR MEJORAR**
Diagnostico situación Actual		Definir un plan para verificar si los empleados o contratistas hacen uso de sus dispositivos personales para acceder a sistemas de información.
		Documentar los procedimientos para la identificación de la utilización de dispositivos personales para acceder a sistemas de información de la organización.
		Definir indicadores de medición para medir la utilización de dispositivos personales para acceder a sistemas de información de la organización.
		Utilizar los indicadores para determinar acciones de seguridad.
Identificar las Necesidad de los Usuarios		Definir un plan para determinar las necesidades de utilización de BYOD de los empleados o contratistas.
		Documentar el plan para determinar las necesidades de utilización de BYOD.

		Definir indicadores de medición para determinar el grado de necesidad de la utilización de BYOD en la organización.
		Utilizar los indicadores para determinar acciones y políticas de seguridad.
Políticas de Seguridad y Aspectos Organizativos	La Organización cuenta con una política de seguridad pero no abarca el uso de BYOD.	Definir una política para el uso de BYOD
		Definir un plan para la revisión de la política de seguridad
		Documentar la política dispositivos BYOD y definir un plan de revisión.
		Definir indicadores de medición para el impacto de las políticas para dispositivos BYOD.
		Utilizar los indicadores de medición para la mejora de las Políticas de Seguridad.
		Determinar la viabilidad del esquema de teletrabajo.
		Si es viable el teletrabajo, realizar la documentación.
		Si es viable el teletrabajo, definir indicadores de medición para el teletrabajo.
		Utilizar los indicadores de teletrabajo para la mejora del esquema de seguridad.
Revisiones de Seguridad de la Información	La organización realiza auditoría de seguridad externa. La organización realiza verificaciones de cumplimientos de las políticas de seguridad.	Realizar auditorías internas de seguridad de manera periódica.
		Documentar los procesos para las revisiones de seguridad.
		Definir indicadores de medición para las Revisiones yauditorías.
		Utilizar los indicadores para mejorar y monitorear la revisión de seguridad de la información.

Nota: Fuente Propia

5.3.2 Dimensión de Desarrollo y Arquitectura

Después de realizar las encuestas para la calificación del MMP en la dimensión de Desarrollo y Arquitectura, se determinó las actividades que se ejecutan con respecto al Dominio de "Requerimientos de Seguridad de Sistemas de Información" que corresponden a esta dimensión (Tabla 14).

Para el Dominio “Requerimientos de Seguridad de Sistemas de Información” se determinó que se encuentra en un nivel de madurez 3 puesto que cumple con las actividades hasta este nivel.

La interpretación de los resultados para esta dimensión se muestra en la tabla 15, en el formato “***RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE DESARROLLO Y ARQUITECTURA”***

Tabla 14: Actividades de Desarrollo y Arquitectura

MODELO DE MADUREZ		
CUMPLIMIENTO DE ACTIVIDADES DE DESARROLLO Y ARQUITECTURA		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**ACTIVIDADES**	**SE EJECUTA**
Requerimientos de Seguridad de Sistemas de Información	La organización realiza el levantamiento de requerimientos de seguridad para los sistemas de información que serán accedidos desde los BYOD antes de la adquisición, desarrollo o mejora de los sistemas.	SI
	La organización cuenta con servicios de conexión segura VPN para la conexión de equipos BYOD desde el exterior a aplicaciones y/o servicios de la organización	SI
	La organización cuenta con certificados o firmas electrónicas para la encriptación de las comunicaciones entre las aplicaciones y los BYOD	SI
	La organización cuenta con la documentación para la conexión de los BYOD desde las redes públicas.	SI
	La organización cuenta con un KPI para los requerimientos y controles de seguridad de acceso desde redes publica en el ámbito BYOD.	NO
	La organización utiliza los resultados de los KPI's para mejorar y monitorear los requerimientos de seguridad en el ámbito BYOD.	NO

Nota: Fuente Propia

Tabla 15: Resultados de la Evaluación de Madurez de la dimensión

MODELO DE MADUREZ		
RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE GOBIERNO		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**DESCRIPCION DE RESULTADOS**	
	ASPECTOS SATISFACTORIOS	**ASPECTOS POR MEJORAR**
Requerimientos de Seguridad de Sistemas de Información	La organización realiza el levantamiento de requerimientos de seguridad para los sistemas de información que serán accedidos desde los BYOD antes de la adquisición, desarrollo o mejora de los sistemas. La organización cuenta con servicios de conexión segura VPN para la conexión de equipos BYOD desde el exterior a aplicaciones o servicios de la organización. La organización cuenta con certificados o firmas electrónicas para la encriptación de las comunicaciones entre las aplicaciones y los BYOD. La organización cuenta con la documentación para la conexión de los BYOD desde las redes públicas.	Definir indicadores de medición para los requerimientos y controles de seguridad de acceso desde redes publica en el ámbito BYOD. Utilizar los KPI para mejorar y monitorear los requerimientos de seguridad en el ámbito BYOD.

Nota: Fuente Propia

5.3.3 Dimensión de Seguridad

Después de realizar las encuestas para la calificación del MMP en la dimensión de Seguridad, se determinó las actividades que se ejecutan con respecto a los Dominios de “Seguridad Ligada a los recursos humanos”, “Procedimientos y responsabilidades operacionales”, “Cifrado”, “Seguridad Física y Ambiental”, “Procedimientos y responsabilidades operacionales” y “Gestión de incidentes de seguridad de la información y mejoras”, que corresponden a esta dimensión (Tabla 16).

Para el Dominio “Seguridad Ligada a los recursos humanos” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Procedimientos y responsabilidades operacionales” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Cifrado” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Seguridad Física y Ambiental” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Procedimientos y responsabilidades operacionales” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el dominio “Gestión de incidentes de seguridad de la información y mejoras” se determinó que se encuentra en un nivel de madurez 2 puesto que cumple con las actividades hasta este nivel.

La interpretación de los resultados para esta dimensión se muestra en la tabla 17, en el formato “***RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE SEGURIDAD”***

Tabla 16: Actividades de Seguridad

MODELO DE MADUREZ		
CUMPLIMIENTO DE ACTIVIDADES DE SEGURIDAD		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**PREGUNTAS**	**SE EJECUTA**
Seguridad Ligada a los recursos humanos	La organización capacita a los colaboradores y son estos conscientes del uso de sus dispositivos personales para desempeñar tareas de su trabajo	NO
	La organización tiene implementada métodos, esquemas, para proteger los activos de información del uso de dispositivos personales, cuando se presenta un despido o un cambio de puesto.	NO
	La organización tiene documentadas las evidencias de capacitaciones a colaboradores y los métodos para el cambio de puesto o despido de personal en el ámbito BYOD.	NO
	La organización cuenta con KPI's para medir la efectividad de capacitaciones.	NO
	La organización cuenta con KPI's para medir la efectividad de los métodos y esquemas, en el tema de despidos o cambios de puesto en el ámbito BYOD.	NO
	La organización utilizan estos KPI's para la optimización y mejora continua.	NO
Control de Accesos	La organización tiene asignación de acceso y políticas de privilegios por cargos para dispositivos BYOD.	NO
	La organización asignación la información secreta "Contraseñas", mediante algoritmos de encriptación para los dispositivos BYOD	NO
	La organización realiza revisión de los permisos asignados a los dispositivos BYOD.	NO
	La organización tiene herramientas o sistemas de información para adicionar o retirar permisos o privilegios al personal que utilice dispositivos BYOD.	NO
	En la organización los usuarios conocen la exigencia sobre las prácticas de autenticación existentes que rigen para dispositivos BYOD.	NO
	En la organización existen métodos y procedimientos de control de acceso para dispositivos BYOD, de acuerdo a la política de control de acceso.	NO

	En la organización se tienen procedimientos para el inicio de sesión a aplicativos o sistemas de la compañía desde BYOD.	NO
	En la organización los sistemas de gestión de contraseñas también gestionan conexiones de dispositivos BYOD.	NO
	En la organización se tienen documentados todos los procedimientos asociados a la gestión de accesos en el ámbito BYOD.	NO
	La organización cuenta con KPI's para los procedimientos establecidos para el control de Acceso en el ámbito BYOD.	NO
	La organización utilizan estos KPI's para la mejora de los procesos de control de Acceso.	NO
Cifrado	La organización tiene una política y métodos para la gestión de claves específicas para los dispositivos BYOD.	NO
	La organización tiene documentada la política de cifrado para los BYOD.	NO
	La organización tiene KPI's para la política de cifrado en el ámbito BYOD.	NO
	La organización utilizan estos KPI's para la optimización de la política cifrado.	NO
Seguridad Física y Ambiental	En la organización existen políticas y metodologías que especifiquen las medidas de seguridad generales (robo, incendios, pérdidas) para dispositivos BYOD relacionados a la organización.	NO
	En la organización existen políticas, métodos o sistemas de información para proteger los activos usados fuera de las instalaciones de la compañía por dispositivos BYOD.	NO
	En la organización existen políticas, métodos o sistemas de información para proteger los dispositivos BYOD usados en tareas de la compañía y fuera de la misma.	NO
	En la organización se tienen métodos o sistema de información para la eliminación de datos sensibles o software de la compañía en los dispositivos BYOD.	NO
	En la organización existen métodos o sistemas para asegurar que los dispositivos personales de los usuarios desatendidos cuentan con la protección adecuada.	NO
	La organización tiene métodos o sistemas de información para puesto de trabajo despejado y bloque de pantalla enfocado en los dispositivos BYOD.	NO

	La organización tiene documentados las políticas, métodos y uso de los sistemas informáticos para la protección de dispositivos BYOD y otro asociado a la seguridad física ambiental.	NO
	La organización tiene KPI's para la políticas métodos y sistemas de información en el ámbito BYOD.	NO
	La organización utilizan estos KPI's para la mejora del proceso de seguridad física y ambiental.	NO
Procedimientos y responsabilidades operacionales	La organización exige o se entrega software Antivirus en los dispositivos BYOD.	NO
	La organización realiza el registro de los eventos de seguridad y se toman medidas para contrarrestar en el ámbito BYOD.	NO
	La organización toma medidas para mitigar las vulnerabilidades en los sistemas de información detectadas en el ámbito BYOD.	NO
	La organización cuenta con la documentación de los procedimientos operacionales en el ámbito BYOD.	NO
	La organización tiene KPI's para los procedimientos operacionales en el ámbito BYOD.	NO
	La organización utilizan estos KPI's para mejorar y monitoreo los procedimientos operacionales.	NO
Gestión de incidentes de seguridad de la información y mejoras	La organización cuenta con mecanismos para reportar eventos de seguridad.	SI
	La organización cuenta con mecanismos para reportar debilidades de seguridad.	SI
	La organización ha divulgado los procedimientos para el reporte de debilidades o eventos de seguridad.	NO
	La organización tiene KPI's para los reportes de las debilidades y eventos de seguridad.	NO
	La organización utilizan estos KPI's para mejorar y monitorear la gestión de incidentes de seguridad.	NO

Nota: Fuente Propia

Tabla 17: Resultados de la Evaluación de Seguridad

MODELO DE MADUREZ		
RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE SEGURIDAD		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**DESCRIPCION DE RESULTADOS**	
	ASPECTOS POSITIVOS	**ASPECTOS POR MEJORAR**

Seguridad Ligada a los recursos humanos	Capacitar a los colaboradores para el uso consciente de sus dispositivos personales para desempeñar tareas de su trabajo
	Implementar métodos, esquemas, para proteger los activos de información del uso de dispositivos personales, cuando se presenta un despido o un cambio de puesto.
	Documentar las evidencias de capacitaciones a colaboradores y los métodos para el cambio de puesto o despido de personal en el ámbito BYOD.
	Definir indicadores de medición para medir la efectividad de capacitaciones.
	Definir indicadores de medición para medir la efectividad de los métodos y esquemas, en el tema de despidos o cambios de puesto en el ámbito BYOD.
	Utilizar los indiciadores de medición para la optimización y mejora continua.
Control de Accesos	Asignar el acceso y las políticas de privilegios por cargos para dispositivos BYOD.
	Controlar la asignación de la información secreta "Contraseñas", mediante algoritmos de encriptación para dispositivos BYOD.
	Realizar revisión de los permisos asignados a los dispositivos BYOD.
	Utilizar herramientas o sistemas de información para adicionar o retirar permisos o privilegios al personal que utilice dispositivos BYOD.
	Divulgar a los usuarios la exigencia sobre las prácticas de autenticación existentes que rigen para dispositivos BYOD.
	Definir métodos y procedimientos de control de acceso para dispositivos BYOD, de acuerdo a la política de control de acceso.
	Definir procedimientos para el inicio de sesión a aplicativos o sistemas de la compañía desde BYOD.
	Utilizar los sistemas de gestión de contraseñas para gestionar las conexiones de dispositivos BYOD.

	Documentar todos los procedimientos asociados a la gestión de accesos en el ámbito BYOD.
	Definir indiciadores de medición para el procedimiento establecidos para el control de Acceso en el ámbito BYOD?
	Utilizar los indiciadores de medición para la mejora de los procesos de control de Acceso?
Cifrado	Definir una política y métodos para la gestión de claves específicas para los dispositivos BYOD.
	Documentar la política de cifrado para los BYOD.
	Definir indiciadores de medición para la política de cifrado en el ámbito BYOD.
	Utilizar los indiciadores de medición para la optimización de la política cifrado.
Seguridad Física y Ambiental	Definir las políticas y metodologías que especifiquen las medidas de seguridad generales (robo, incendios, pérdidas) para dispositivos BYOD relacionados a la organización.
	Definir las políticas, métodos o sistemas de información para proteger los activos usados fuera de las instalaciones de la compañía por dispositivos BYOD.
	Definir las políticas, métodos o sistemas de información para proteger los dispositivos BYOD usados en tareas de la compañía y fuera de la misma.
	Definir los métodos o sistema de información para la eliminación de datos sensibles o software de la compañía en los dispositivos BYOD.
	Definir métodos o sistemas para asegurar que los dispositivos personales de los usuarios desatendidos cuentan con la protección adecuada.
	Definir métodos o sistemas de información para puesto de trabajo despejado y bloque de pantalla enfocado en los dispositivos BYOD.
	Documentar las políticas, métodos y uso de los sistemas informáticos para la protección de dispositivos BYOD y otro asociado a la seguridad física ambiental.
	Definir indicadores de medición para las políticas métodos y sistemas de información en el ámbito BYOD.
	Utilizar los indicadores de medición para la mejora del proceso de seguridad física y ambiental.

Procedimientos y responsabilidades operacionales		Exigir o entregar software Antivirus a los dispositivos BYOD.
		Realizar el registro de los eventos de seguridad y tomar medidas para contrarrestar en el ámbito BYOD.
		Tomar medidas para mitigar las vulnerabilidades en los sistemas de información detectadas en el ámbito BYOD.
		Documentar los procedimientos operacionales en el ámbito BYOD.
		Definir indicadores de medición para los procedimientos operacionales en el ámbito BYOD?
		Utilizar los indicadores de medición para mejorar y monitoreo los procedimientos operacionales.
Gestión de incidentes de seguridad de la información y mejoras	La organización cuenta con mecanismos para reportar eventos de seguridad. La organización cuenta con mecanismos para reportar debilidades de seguridad.	Divulgar los procedimientos para el reporte de debilidades o eventos de seguridad a toda la organización.
		Definir indiciadores de medición para los reportes de las debilidades yeventos de seguridad
		Utilizar los indiciadores de medición para mejorar y monitorear la gestión de incidentes de seguridad.

Nota: Fuente Propia

5.3.4 Dimensión de Infraestructura

Después de realizar las encuestas para la calificación del MMP en la dimensión de Seguridad, se determinó las actividades que se ejecutan con respecto a los Dominios de “Gestión de Activos” , “Control de Accesos y “Gestión de seguridad de red” que corresponden a esta dimensión (Tabla 18).

Para el Dominio “Gestión de Activos” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “Control de Accesos” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

Para el Dominio “gestión de seguridad de red” no se ejecuta ninguna actividad que aplique del marco de referencia propuesto, por lo tanto su nivel de madurez es 1.

La interpretación de los resultados para esta dimensión se muestra en la tabla 19, en el formato “***RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE INFRAESTRUCTURA”***

Tabla 18: Actividades de Infraestructura

MODELO DE MADUREZ		
CUMPLIMIENTO DE ACTIVIDADES DE INFRAESTRUCTURA		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**PREGUNTAS**	**SE EJECUTA**
Gestión de Activos	La organización tiene registro de todos los activos de la organización y están relacionados a u su posible uso desde BYOD.	NO
	La Organización tiene identificados responsables para los activos de información que sean utilizados por los BYOD.	NO
	La organización ha informado y capacitado a los responsables de la información para un uso aceptable desde los BYOD.	NO
	La organización tiene implementados herramientas o sistemas de información para asegurar los activos de información en los dispositivos BYOD cuando se presente un cese laboral.	NO
	La organización tiene documentados todos los controles asociados a esta gestión de activos en el ámbito BYOD.	NO
	La organización tienen KPI's para medir la efectividad de la medidas en la gestión de activos en el ámbito BYOD.	NO
	La organización utiliza estos KPI para la mejora optimización y mejora continua en la Gestión de Activo.	NO

Control de Accesos	En la política de control de Acceso de la organización está incluido el acceso de los BYOD.	NO
	La organización tiene control de acceso a redes internas y aplicativas de la compañía para dispositivos BYOD.	NO
gestión de seguridad de red	La organización cuenta con controles de RED para los BYOD.	NO
	La organización cuenta con controles para la conexión a la RED para los dispositivos BYOD (Firewall, Autenticación).	NO
	La organización cuenta con segregación de red (VLAN) de acuerdo a la necesidad de servicios que desean acceder los BYOD.	NO
	La organización cuenta con la documentación y los empleados conocen los controles de RED para los BYOD.	NO
	La organización cuenta con un KPI para los controles de RED en el ámbito BYOD.	NO
	La organización utiliza los KPI para mejorar y monitorear la gestión de RED en el ámbito BYOD.	NO

Nota: Fuente Propia

Tabla 19: Actividades de Infraestructura

MODELO DE MADUREZ		
RESULTADOS DE LA EVALUACION DE MADUREZ DE LA DIMENSION DE INFRAESTRUCTUA		
Empresa	Del sector Solidario	
Realizado Por:	Robin Lopez y Ramiro Lopez	
DOMINIOS	**DESCRIPCION DE RESULTADOS**	
	ASPECTOS POSITIVOS	**ASPECTOS POR MEJORAR**
Gestión de Activos		Registrar todos los activos de la organización y su relacionados a u su posible uso desde BYOD.
		Identificar los responsables para los activos de información que sean utilizados por los BYOD.

	Informar y capacitar a los responsables de la información para un uso aceptable desde los BYOD.
	Implementar herramientas o sistemas de información para asegurar los activos de información en los dispositivos BYOD cuando se presente un cese laboral.
	Documentar todos los controles asociados a esta gestión de activos en el ámbito BYOD.
	Definir indiciadores de medición para medir la efectividad de las medidas en la gestión de activos en el ámbito BYOD.
	Utilizar los indiciadores de medición para la mejora optimización y mejora continua en la Gestión de Activo.
Control de Accesos	Incluir en la política de control de Acceso de la organización el acceso de los BYOD.
	Tener el control de acceso a redes internas y aplicativos de la compañía para dispositivos BYOD.
gestión de seguridad de red	Implementar controles de RED para los BYOD.
	Implementar controles para la conexión a la RED para los dispositivos BYOD (Firewall, Autenticación).
	Realizar segregación de red (VLAN) de acuerdo a la necesidad de servicios que desean acceder los BYOD.
	Documentar y divulgar los controles de RED para los BYOD.
	Definir indiciadores de medición para los controles de RED en el ámbito BYOD.
	Utilizar los indiciadores de medición para mejorar y monitorear la gestión de RED en el ámbito BYOD.

Nota: Fuente Propia

5.4 ESCENARIOS DE MEJORA

Debido a los resultados obtenidos en la evaluación del Modelo de Madurez realizado a la empresa Del sector Solidario y a las entrevistas realizadas al

personal seleccionado. Se elaboraron tres (3) escenarios progresivos de acuerdo a los resultados obtenidos para lograr un alto impacto en la seguridad de la información para mejorar el uso de BYOD.

5.4.1 Escenario 1 – Corto Plazo

Se recomienda este escenario para que se implemente en un periodo no mayor a doce (12) meses: se deben fortalecer los dominios Diagnóstico situación Actual, Identificar las Necesidad de los Usuarios, Política de Seguridad y Aspectos Organizativos, Seguridad Ligada a los recursos humanos y Gestión de Activos los cuales son la bases de las Políticas para el uso de BYOD en la organización, incorporado adicionalmente el área de recursos humanos.

Tabla 20 Escenario No 1

PERFIL	DOMINIO	CALIFICACION	Escenario 1	MAXIMO
GOBIERNO	Diagnostico situación Actual	1	2	5
	Identificar las Necesidad de los Usuarios	1	2	5
	Política de Seguridad y Aspectos Organizativos	1	3	5
	Revisiones de Seguridad de la Información	1	1	5
Desarrollo y Arquitectura	Requerimientos de Seguridad de Sistemas de Información	3	3	5
SEGURIDAD	Seguridad Ligada a los recursos humanos	1	2	5
	Procedimientos y responsabilidades operacionales"	1	1	5
	Cifrado	1	1	5
	Seguridad Física y Ambiental	1	1	5
	Procedimientos y responsabilidades operacionales	1	1	5
	Gestión de incidentes de seguridad de la información y mejoras	2	2	5
Infraestructura	Gestión de Activos	1	2	5
	Control de Accesos	1	1	5
	gestión de seguridad de red	1	1	5

Fuente: Propia

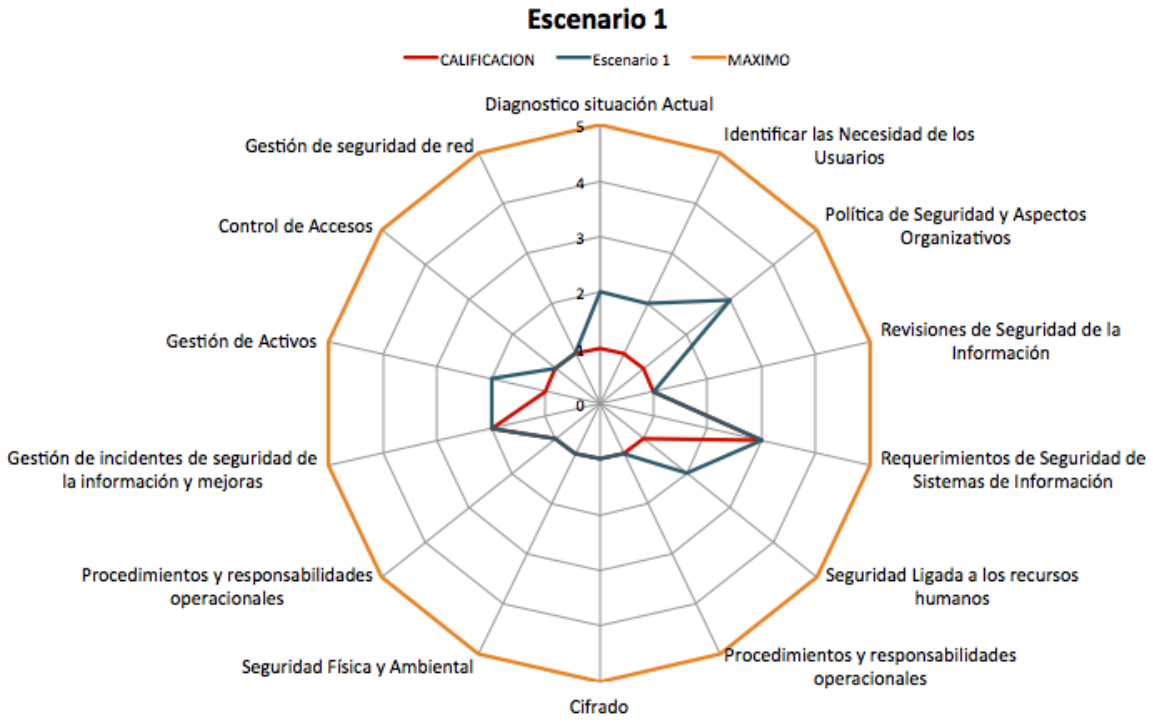

Imagen 15 Propuesta de Escenario 1
Fuente: propia

5.4.2 Escenario 2 – Mediano Plazo

Se recomienda este escenario para que se implemente en un periodo no mayor a dieciocho (18) meses: se deben fortalecer los dominios Revisiones de Seguridad de la Información, Requerimientos de Seguridad de Sistemas de Información, Procedimientos y responsabilidades operacionales, Cifrado, Seguridad Física y Ambiental, Procedimientos y responsabilidades operacionales, Gestión de incidentes de seguridad de la información y mejoras, Control de Accesos y gestión de seguridad de red.

Tabla 21 Escenario No 2

PERFIL	DOMINIO	CALIFICACION	Escenario 2	MAXIMO
GOBIERNO	Diagnostico situación Actual	1	2	5
	Identificar las Necesidad de los Usuarios	1	2	5
	Política de Seguridad y Aspectos Organizativos	1	3	5
	Revisiones de Seguridad de la Información	1	3	5
Desarrollo y Arquitectura	Requerimientos de Seguridad de Sistemas de Información	3	3	5
SEGURIDAD	Seguridad Ligada a los recursos humanos	1	2	5
	Procedimientos y responsabilidades operacionales"	1	2	5
	Cifrado	1	2	5
	Seguridad Física y Ambiental	1	2	5
	Procedimientos y responsabilidades operacionales	1	2	5
	Gestión de incidentes de seguridad de la información y mejoras	2	3	5
Infraestructura	Gestión de Activos	1	2	5
	Control de Accesos	1	2	5
	gestión de seguridad de red	1	2	5

Nota: Fuente Propia

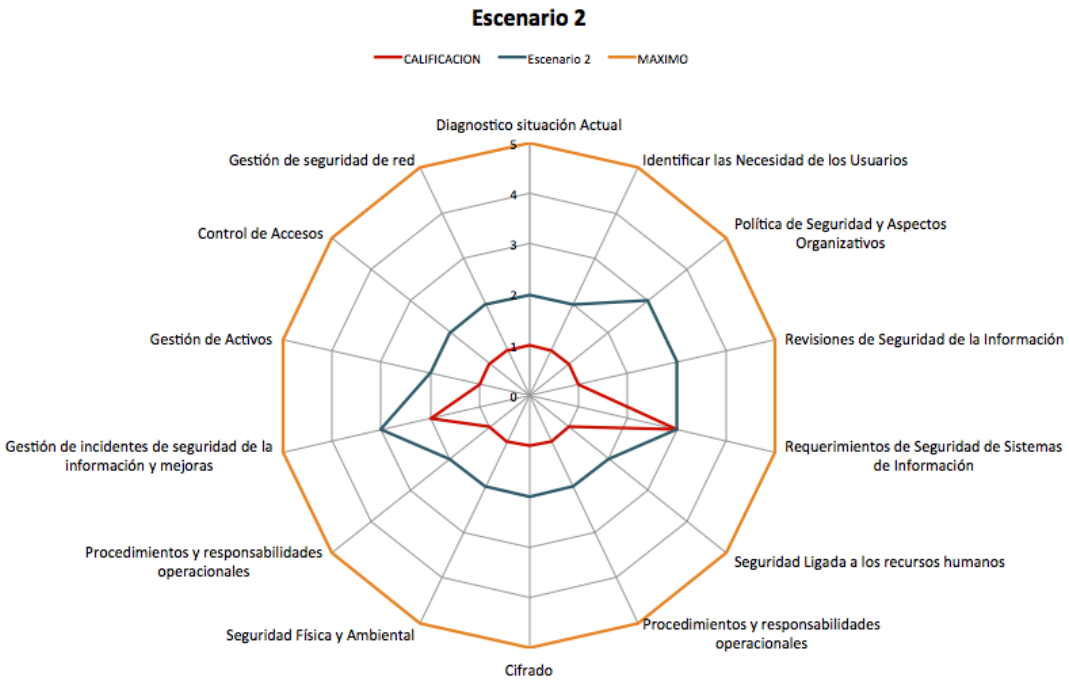

Imagen 16 Propuesta de Escenario 2
Fuente: Propia

5.4.3 Escenario 3 – Largo Plazo

Se recomienda este escenario para que se implemente en un periodo no mayor a veinticuatro (24) meses, se deben fortalecer todos los dominios.

Tabla 22 Escenario No 3

PERFIL	DOMINIO	CALIFICACION	Escenario 3	MAXIMO
GOBIERNO	Diagnostico situación Actual	1	4	5
	Identificar las Necesidad de los Usuarios	1	4	5
	Política de Seguridad y Aspectos Organizativos	1	5	5
	Revisiones de Seguridad de la Información	1	5	5
Desarrollo y Arquitectura	Requerimientos de Seguridad de Sistemas de Información	3	5	5
SEGURIDAD	Seguridad Ligada a los recursos humanos	1	4	5
	Procedimientos y responsabilidades operacionales"	1	4	5
	Cifrado	1	4	5
	Seguridad Física y Ambiental	1	4	5
	Procedimientos y responsabilidades operacionales	1	4	5
	Gestión de incidentes de seguridad de la información y mejoras	2	5	5
Infraestructura	Gestión de Activos	1	4	5
	Control de Accesos	1	4	5
	gestión de seguridad de red	1	4	5

Fuente: Propia

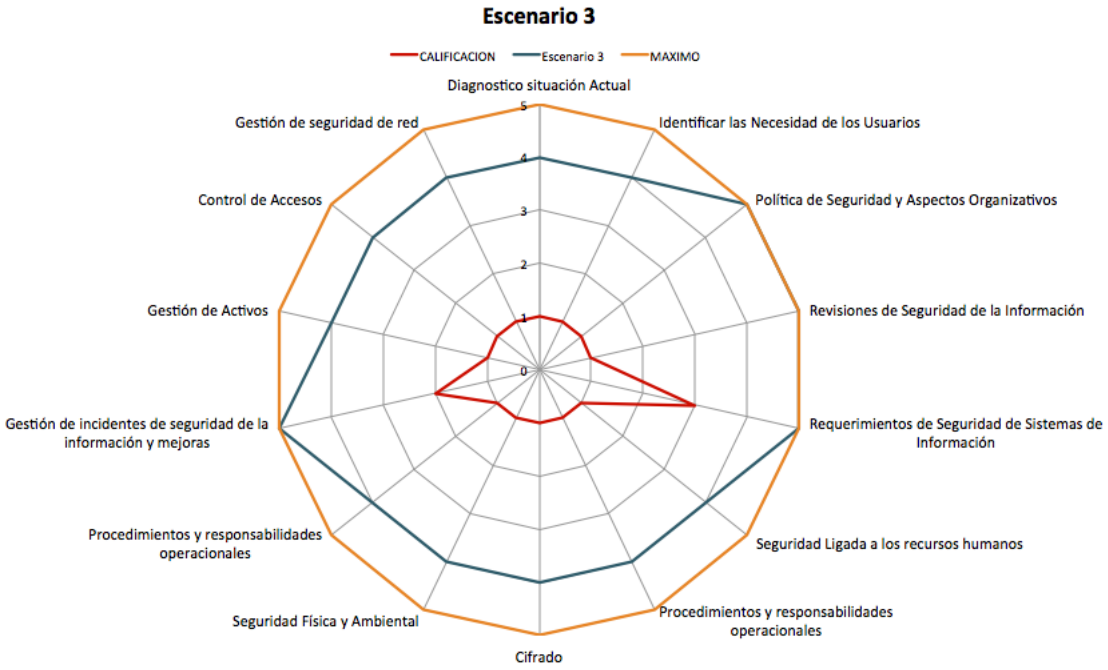

Imagen 17 Propuesta de Escenario 3
Fuente Propia

6. CONCLUSIONES Y FUTURO TRABAJO

El presente trabajo contempla el proceso de revisión a fondo del marco ISO/IEC 27002:2013 identificando y adicionando en el mismo los controles que impactan directamente en el BYOD, con estos controles se determinó un modelo de madurez con el cual las empresas puedan determinar el estado de madurez de seguridad para el adecuado uso de BYOD en las organizaciones.

Bajo el análisis y revisión del marco de referencia ISO/IEC 27002:2013 como de la creciente tendencia de BYOD se determinó que 12 dominios y 43 controles aplicaban a los dispositivos cubiertos por esta tendencia, además se complementa el marco adicionando 2 dominios y 2 controles que no se contemplan en ISO/IEC 27002:2013, teniendo finalmente una declaración de aplicabilidad para BYOD.

Uno de los grandes aportes de este trabajo para las organizaciones, es que bajo el modelo propuesto las empresas pueden identificar de manera ágil el nivel de madurez que tienen frente al riesgo latente de los dispositivos personales BYOD en la seguridad de la información. Adicionalmente en los anexos se encuentra la encuesta que al momento de ser diligenciada arroja de manera grafica el nivel de madurez.

La validación del modelo propuesto se realizó en una empresa del sector solidario, evidenciando que esta organización no se ha concientizado sobre los posibles problemas de seguridad que conlleva el uso de BYOD, por lo tanto se proponen tres escenarios que permitirán abarcar de manera progresiva el uso adecuado de esta tecnología sin poner en riesgo los activos de información.

El creciente auge de la utilización de dispositivos personales en el entorno empresarial, justifica la implementación de este marco de referencia, asegurando así una adecuada implementación de esta tecnología en las organizaciones.

Las organizaciones no pueden ser ajenas a la gestión adecuada de la seguridad de la información con referente a los BYOD, debido a que se ha constituido en un elemento innato para las organizaciones considerando que su uso y administración se realiza de manera informal y desorganizada.

Con la elaboración del modelo de madurez se identifican los ítems donde las empresas no están preparadas para afrontar adecuadamente esta tendencia, para trabajos futuros se propone la elaboración de un plan de despliegue que abarque los controles propuestos en este documento.

7. Bibliografía

Cisco Systems. (2013). *Cisco Bring Your Own Device Device Freedom Without Compromising the IT Network.* Cisco Systems, Inc.

International Standard. (2013). *Information technology - Security techniques - Code of practice for information security controls.* Switzerland: ISO/IEC.

Mathias, C. J. (enero de 2014). *Como crear una politica de BYOD*. Recuperado el 21 de octubre de 2014, de http://searchdatacenter.techtarget.com/: http://searchdatacenter.techtarget.com/es/consejo/Como-crear-una-politica-de-BYOD

Fernando C., B. A. (2012). *Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización.* Cali: ICESI.

Martínez, E. A. (2012). *redyseguridad.fi-p.unam.mx*. Recuperado el 25 de 10 de 2014, de http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/3-gestion-de-claves/31-politicas-de-gestion-de-claves?showall=&start=1

Software Engineering Institute. (2010). *CMMI para Desarrollo, Versiòn 1.3.* Carnegie Mellon University.

MAP., A. C. (s.f.). *Herramientas pas la Gestion de Proyecots*. Recuperado el 27 de 11 de 2014, de PROJECT - TOOLS: projectools.wordpress.com/modelos-de-madurez-en-gestion-de-proyectos

International Organization for Standardization. (2005). *ISO/IEC 27001.*

International Organization for Standardization. (2005). *ISO/IEC 27002.*

GOOGLE. (09 de 06 de 2014). *OWR MOBILE PLANET*. Obtenido de http://think.withgoogle.com/: http://think.withgoogle.com/mobileplanet/es/graph/?country=ar&country=br&country=ca&country=us&country=mx&category=DETAILS&topic=Q00&stat=Q00_1&wave=2011&wave=2012&wave=2013&age=all&gender=all&chart_type=bar&active=gender

Cisco IBSG Horizons. (2012). BYOD y Virtualizacion.

Forrester Reseach. (2012). Forrsingts Workforce Employee Survey Q4 2012.

GARTNER. (01 de 05 de 2014). *www.gartner.com*. Obtenido de http://www.gartner.com: http://www.gartner.com/it/content/2538500/2538515/august_14_bring_your_own_device_byod_dwillis.pdf?userId=73210080

Ann Cavaukian, P. (11 de 12 de 2013). BYOD (Bring Your Ownd Device) Is Your Organization Ready? Ontario, Canada.

ISACA. (s.f.). *ISACA.ORG*. Recuperado el 01 de 05 de 2014, de Information Systems Audit and Control Association: http://www.isaca.org/Blogs/282270/archive/2011/04/27/ProteccióndeActivosdeInformación.aspx

Vera, E. (s.f.). *ISO 27001. EL inventario de activos en la implementacion de la norma*. Recuperado el 20 de 04 de 2014, de http://www.isotools.org: http://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

International Organization for Standardization. (2013). *ISO/IEC 27001*.

Ministerio de tecnologias de la Informacion y las comunicaciones. (14 de 03 de 2014). Boletin Trimestral de las TIC Banda Ancha Cifras Cuarto trimestre de 2013.

Chrissis, M. B. (2011). *CMMI for Development: Guidelines for Process Integration and Product Improvement* (3rd Edition ed.).

ANEXOS

Anexo 1 Matriz de Aplicabilidad ISO 27002:2013 SOA

ISO 27001:2013 Controles de Seguridad			Comentarios (Justificación de Exclusión)	Comentarios (Visión general de la implementación)
Cláusula	**Sección**	**Objetivo de Control / Control**		
Diagnóstico situación Actual	N/A	Diagnosticar la situación actual del uso de BYOD en la organización		Esto permitirá identificar rápidamente qué activos de información están siendo accedidos y de qué forma se está realizando el acceso desde los BYOD. El diagnóstico de la situación actual incluye la revisión y análisis de los procesos operativos y tecnológicos que conllevan el uso de BYOD en el ambiente empresarial, permitiendo la identificación de oportunidades de mejora en estos dos ítems.
Identificar las Necesidad de los Usuarios	N/A	Identificar las necesidades de los usuarios para acceder a recursos de la organización desde sus dispositivos personales.		Consiste en realizar una caracterización de necesidades de acuerdo a las necesidades de utilización de BYOD.
5 Políticas de Seguridad	5,1	Dirección de la Alta Gerencia para la Seguridad de la Información		
	5.1.1	Políticas de Seguridad de la Información		En este control se Formaliza lo estipulado por la alta dirección sobre BYOD (Permite el uso, determina limites, o Prohíbe)

	5.1.2	Revisión de las Políticas de Seguridad de la Información		En este control se revisa, evalúa y se ajusta las políticas de BYOD de acuerdo a lo definido por la alta dirección.
6 Organización de la Seguridad de la Información	6,1	Organización Interna		
	6.1.1	Roles y Responsabilidad de Seguridad de la Información	En este control se asignan los responsables de los activos de Información	
	6.1.2	Contacto con autoridades	Consiste en el reporte de Fallas o falencias en las regulación legales	
	6.1.3	Contacto con grupos de interés especial	Consiste en estar informado con grupos de interés de seguridad	
	6.1.4	Seguridad de la Información en la gestión de proyectos	Consiste en como la seguridad de la información debería abordarse en la gestión de proyectos	
	6.1.5	Segregación de deberes	Consiste en la distribución de responsabilidades con respecto a los Activos de Información	
	6,2	Dispositivos móviles y teletrabajo		
	6.2.1	Política de dispositivos móviles		Establece la Política y da apoyo a las medidas de seguridad que se adoptan para la gestión de riesgos por la introducción de dispositivos móviles incluyendo los BYOD
	6.2.2	Teletrabajo		Consiste en la Política y apoyo a las medidas de seguridad para proteger los activos de información para los sitios de trabajo a distancias, por involucrar dispositivos Personales o de terceros este Control aplica a BYOD
7 Seguridad en los Recursos Humanos	7,1	Previo al Empleo		
	7.1.1	Verificación de antecedentes	Consiste en la verificación de Antecedentes de los Empleados	
	7.1.2	Términos y condiciones del empleo	Consiste en los acuerdos contractuales con los empleados y contratistas	
	7,2	Durante el Empleo		

	7.2.1	Responsabilidades de la Alta Gerencia	Consiste en que la Alta gerencia debe de exigir a todos los empleados y contratistas aplicar la seguridad de información	
	7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información		Consiste en concientizar, educar y formar en las políticas y procedimientos en seguridad de la información a los empleados y contratistas sobre el uso de BYOD
	7.2.3	Proceso disciplinario	Consiste en la creación de un proceso formal y comunicado para medidas disciplinarias para empleados y contratistas que cometan violación de seguridad	
	7,3	Terminación y Cambio de Empleo		
	7.3.1	Termino de responsabilidades o cambio de empleo		Consiste en las responsabilidades de seguridad de la Información y deberes después de la terminación o cambio de empleo con respecto a los activos de información que tenía acceso a través de su dispositivo.
8 Gestión de Activos	8,1	Responsabilidad de los Activos		
	8.1.1	Inventario de activos		Consiste en identificar, redactar y mantener el inventario de Activos de Información, esto ayuda a asegurar que la protección de activos de Información sea efectiva se ejecute para el uso de BYOD
	8.1.2	Propiedad de activos		Consiste en la asignación a un propietario los activos de información, el cual es responsable de la correcta gestión del activo durante todo su ciclo de vida, El dueño es responsable de la entrega incluyendo la operación del Activo en los BYOD

	8.1.3	Uso aceptable de los activos		Consiste en las normas para el uso aceptable de los activos de Información . Se debe concientizar de los requisitos de seguridad a los empleados y contratistas que utilicen o tengan acceso a los Activos de Información a través de BYOD
	8,2	Clasificación de la Información		
	8.2.1	Clasificación de la información	Consiste en la clasificación de la Información en términos de requisitos legales, el valor, criticidad y sensibilidad.	
	8.2.2	Etiquetado de la información	Consiste en la clasificación de la información con el esquema de clasificación aprobada por la organización	
	8.2.3	Manejo de activos	Consiste en el procedimiento para el manejo de activos de información de acuerdo a su calificación	
	8,3	Manejo de Medios		
	8.3.1	Gestión de medios removibles	Consiste en el procedimiento para la gestión de Medios Removibles de acuerdo con la clasificación.	
	8.3.2	Eliminación de medios	Consiste en la eliminación de los medios de comunicación cuando ya no son necesarios.	
	8.3.3	Transporte de medios físicos	Consiste en la protección contra el acceso no autorizado, uso indebido o corrupción durante el transporte de medios que contienen información	
9 Control de Acceso	9,1	Requerimientos de Negocio para el Control de Acceso		

	9.1.1	Política de control de acceso		Consiste en la creación de una política para el control de acceso, donde se determinan las reglas de control de acceso apropiadas, derechos de acceso y restricción para roles de usuario, aquí se determina el alcance de acceso de BYOD en la organización
	9.1.2	Política en el uso de servicios de red		Consiste en la creación de una política de uso de redes y servicios de red. Los usuarios solo deben contar con acceso a los servicios de red y de la red a los cuales han sido autorizados en la organización
	9,2	Gestión de Accesos de Usuario		
	9.2.1	Registro y baja del usuario	Consiste en el proceso formal de registro de usuario y la cancelación del registro para permitir la asignación de derechos de acceso	
	9.2.2	Gestión de privilegios		Consisten en el proceso formal de aprovisionamiento de acceso de usuario, para asignar o revocar permisos de acceso a todos los sistemas y servicios.
	9.2.3	Gestión de los derechos de acceso privilegiado		Consiste en la restricción y control de la asignación y utilización de los derechos de acceso privilegiados con uso de BYOD
	9.2.4	Gestión de información de autenticación secreta de usuarios		Consiste en el control de la asignación de la información secreta "Contraseñas"
	9.2.5	Revisión de derechos de acceso de usuarios		Consiste en la revisión periódica de los permisos asignados para los BYOD
	9.2.6	Eliminación o ajuste de derechos de acceso		Los permisos de accesos de empleados o contratitas para uso de BYOD deberán ser retirados a la terminación de contrato o ajustes a cambios.
	9,3	Responsabilidades del Usuario		

	9.3.1	Uso de información de autenticación secreta		Consiste que los usuarios deben de seguir las prácticas de la organización sobre el uso de la contraseña de autenticación.
	9,4	Control de Acceso de Sistemas y Aplicaciones		
	9.4.1	Restricción de acceso a la información		Consiste en la limitación de acceso a la información y aplicaciones para los BYOD de acuerdo a la política de control de Acceso
	9.4.2	Procedimientos de conexión segura		Consiste en que el acceso a los sistemas usando BYOD sean controlados por un procedimiento de inicio de sesión seguro cuando la política lo exija
	9.4.3	Sistema de gestión de contraseñas		Consiste en tener un sistema de gestión de contraseñas para los BYOD el cual debe ser interactivo y asegurarse de contraseñas de calidad.
	9.4.4	Uso de programas y utilidades privilegiadas		Consiste en la restricción y control de uso de programas y utilidades que puedan ser capaces de anular sistemas y aplicaciones, esto no podrán estar instalados en los BYOD
	9.4.5	Control de acceso al código fuente del programa	Consiste en la restricción de acceso al código fuente y a los elementos asociados de los programas.	
10 Criptografía	10,1	Controles Criptográficos		
	10.1.1	Política en el uso de controles criptográficos	Consiste en el desarrollo e implementación de una política sobre el uso de controles criptográficos para la protección de la información	
	10.1.2	Gestión de llaves		Consiste en el desarrollo e implementación de una política sobre el uso, la protección y la duración de las claves de cifrado que usarán los BYOD
11	11,1	Áreas Seguras		

Seguridad Física y del Entorno	11.1.1	Perímetro de seguridad físico	Consiste en la definición del perímetro de seguridad	
	11.1.2	Controles físicos de entrada	Consiste en la protección usando controles de acceso de entrada a las áreas seguras para permitir el acceso a personal autorizado	
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Consiste en el diseño e implementación de la seguridad físicas para oficinas , sales e instalaciones	
	11.1.4	Protección contra amenazas externas y del ambiente	Consiste en el diseño es implementación de la protección física contra los desastres naturales, ataques maliciosos o accidentes	
	11.1.5	Trabajo en áreas seguras	Consiste en diseño e implementación de procedimientos para trabajar en áreas de seguridad.	
	11.1.6	Áreas de entrega y carga	Consiste en el control y aislamiento de puntos en lo que personas no autorizadas pueden entrar.	
	11,2	Equipo		
	11.2.1	Instalación y protección de equipo		Consiste en el lugar y protección de los equipos BYOD para reducir los riesgos de amenazas y peligros ambientales y oportunidades para el acceso no autorizado.
	11.2.2	Servicios de soporte	Consiste en la protección de los equipos contra fallas de energía y otras fallas en apoyo a los servicios públicos.	
	11.2.3	Seguridad en el cableado	Consiste en la protección del cableado eléctrico y telecomunicaciones de intercepciones, interferencias o daños.	
	11.2.4	Mantenimiento de equipos	Consiste en realizar los mantenimientos adecuados para asegurar su disponibilidad	
	11.2.5	Retiro de activos		Consiste en el control para equipos, información o software para ser utilizados fuera de las instalaciones por los BYOD

	11.2.6	Seguridad del equipo		Consiste en la seguridad que debe ser aplicada a equipos y activos fuera de las instalaciones considerando los riesgos de trabajar fuera de la organización utilizando BYOD
	11.2.7	Eliminación segura o reusó del equipo		Consiste en la verificación para asegurar la eliminación de datos sensibles y software con licencia en equipos de empleados o contratistas personales cuando ya no sean requeridos.
	11.2.8	Equipo de usuario desatendido		Consiste que todos los usuarios que utilicen BYOD desentendido deberán asegurarse de que el equipo tienen la protección adecuada
	11.2.9	Política de escritorio limpio y pantalla limpia	Consiste en el desarrollo e implementación de una política para el manejo de impresiones o información sensible en papel e información en las pantallas cuando no sean necesarias o cuando no se esté en la oficina.	
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades		
	12.1.1	Documentación de procedimientos operacionales	Consiste en la documentación de los procedimientos operativos	
	12.1.2	Gestión de cambios	Consiste en el proceso donde se controlan los cambios en los procesos de negocio, instalaciones de procesamiento de información y los sistemas que afectan a la seguridad de la información.	
	12.1.3	Gestión de la capacidad	Consiste en el monitoreo, ajuste y proyección de las necesidades actuales y futuras de capacidad para asegurar el rendimiento requerido.	

12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Consiste en la separación de entornos de Desarrollo, pruebas y producción para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.	
12,2	Protección de Software Malicioso		
12.2.1	Controles contra software malicioso		Consiste en la implementación de controlase para la detección, prevención y recuperación contra Malware en los BYOD
12,3	Respaldo		
12.3.1	Respaldo de información	Consiste en el desarrollo e implementación en la ejecución de copias de seguridad y su validación.	
12,4	Registro y Monitoreo		
12.4.1	Registro de eventos		Consiste en tener registro de eventos de las actividades de los usuarios, excepciones, errores y eventos de seguridad que se ejecuten en los BYOD.
12.4.2	Protección de registros de información	Consiste en la protección contra manipulación y acceso no autorizado a los log de servicios y log de información	
12.4.3	Registros de Administrador y Operador	Consiste en la protección de los registros del sistema por parte de los usuarios con privilegios y el registro de sus actividades.	
12.4.4	Sincronización de relojes	Consiste en la sincronización de los relojes de todos los sistemas a partir de una única fuente de tiempo de referencia	
12,5	Control de Software Operacional		
12.5.1	Instalación de software en sistemas operacionales	Consiste en el procedimiento para controlar la instalación de software en los sistemas operativos, lo cual no es viable en BYOD ya que los equipos son de los empleados o contratistas.	
12,6	Gestión de Vulnerabilidades		

		Técnicas		
	12.6.1	Gestión de vulnerabilidades técnicas		Consiste en la obtención oportuna de las vulnerabilidades técnicas que conlleven el uso de BYOD para tomar medidas adecuadas para afrontar los riesgos asociados
	12.6.2	Restricciones en la instalación de software	La notas que rigen la instalación de Software no aplican a BYOD ya que el dispositivo no es de la organización	
	12,7	Consideraciones de Auditoría de Sistemas de información		
	12.7.1	Controles de Auditoría de Sistemas de Información	Consiste en los requisitos y las actividades relacionadas con la auditorías las cuales deben ser planificadas y acordadas, esto no está dirigido a dispositivos finales.	
13 Seguridad en las Comunicaciones	13,1	Gestión de Seguridad en Red		
	13.1.1	Controles de red		Consiste en la gestión y control de la red la cual es fundamental para el acceso de los BYOD
	13.1.2	Seguridad de los servicios en red		Consiste en la gestión de la seguridad de los servicios de Red que sean utilizados para el acceso de los BYOD
	13.1.3	Segregación de redes.		Consiste en la segregación de la red de acuerdo a grupos de servicios de información, los usuarios o sistemas de información, para reducir los riesgos de acceso no autorizados desde los BYOD.
	13,2	Transferencia de Información		
	13.2.1	Políticas y procedimientos para la transferencia de información	Consiste en el desarrollo e implementación de una política para la transferencia de información.	
	13.2.2	Acuerdos en la transferencia de información	Consiste en los acuerdos acordados para la transferencia segura de información comercial entre la organización y las partes externas.	

	13.2.3	Mensajería electrónica	Consiste en la protección de la mensajería electrónica.	
	13.2.4	Acuerdos de confidencialidad o no-revelación	Consiste en los acuerdos de confidencialidad o no divulgación de información cuando se realice transferencia de información	
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de Seguridad de Sistemas de Información		
	14.1.1	Análisis y especificación de requerimientos de seguridad		Consiste en el análisis de los requisitos relacionados con la seguridad de la información para nuevos sistemas de información, principalmente el acceso desde BYOD.
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas		Consiste en el aseguramiento de los servicios de aplicaciones que pasaran por redes públicas, cuando se utilice BYOD.
	14.1.3	Protección de transacciones de servicios de aplicación		Consiste en la protección en las transacciones ejecutadas desde los BYOD para prevenir la transmisión incompleta, alteración, divulgación, duplicidad.
	14,2	Seguridad en el Proceso de Desarrollo y Soporte		
	14.2.1	Política de desarrollo seguro	Consiste en el desarrollo e implementación de reglas para el desarrollo de software	
	14.2.2	Procedimientos de control de cambios	Consiste en el procedimiento formal de control de cambios en el ciclo de vida de desarrollo.	
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Consiste en la revisión y pruebas de las aplicaciones críticas de negocio cuando se cambia plataformas operativas.	
	14.2.4	Restricción de cambios a paquetes de software	Consiste en el control en las modificaciones y cambios en los paquetes de software	
	14.2.5	Procedimientos de desarrollo de sistemas	Consiste en los procedimientos para el desarrollo de sistemas	

			seguros.	
	14.2.6	Entorno de desarrollo seguro	Consiste en el establecimiento y protección de los entornos de desarrollo.	
	14.2.7	Desarrollo tercerizado	Consiste en la supervisión y control de las actividades de desarrollo tercerizado.	
	14.2.8	Pruebas de seguridad del sistema	Consiste en las pruebas de la funcionalidad de seguridad durante el desarrollo.	
	14.2.9	Pruebas de aceptación del sistema	Consiste en el programa de pruebas de aceptación de sistemas.	
	14,3	Datos de Prueba		
	14.3.1	Protección de datos de prueba	Consiste en la protección y control de los datos de prueba.	
15 Relaciones con Proveedores	15,1	Seguridad en Relaciones con el Proveedor		
	15.1.1	Política de Seguridad de la Información para relaciones con proveedores	Consiste en el desarrollo e implementación de una política de seguridad de la información para proveedores.	
	15.1.2	Atención de tópicos de seguridad dentro de los acuerdos con proveedores	Consiste en establecer y acordar los requisitos de seguridad de la información con cada proveedor.	
	15.1.3	Cadena de suministros de TIC	Consiste en los acuerdos con proveedores sobre los requisitos de seguridad de información asociados a los servicios de información y tecnologías de comunicaciones y cadena de suministros.	
	15,2	Gestión de Entrega de Servicios de Proveedor		
	15.2.1	Monitoreo y revisión de servicios de proveedor	Consiste en el control, revisión y auditoría de proveedores	
	15.2.2	Gestión de cambios a servicios de proveedor	Consiste en la administración en los cambios en prestación de servicios por parte del proveedor.	

16 Gestión de Incidentes de Seguridad de la Información	16,1	Gestión de Incidentes de Seguridad de la Información y Mejoras		
	16.1.1	Responsabilidades y Procedimientos	Consiste en estableces responsabilidad y procedimientos para los incidentes de seguridad de información.	
	16.1.2	Reporte de eventos de Seguridad de la Información		Consiste en el reporte de los eventos de seguridad de la información
	16.1.3	Reporte de debilidades de Seguridad de la Información		Consiste en el reporte por parte de las empleados o contratistas de debilidades de seguridad observados
	16.1.4	Valoración y decisión de eventos de Seguridad de la Información	Consiste en la evaluación y toma de decisiones de los eventos de seguridad	
	16.1.5	Respuesta a incidentes de Seguridad de la Información	Consiste en la respuesta de los incidentes de seguridad	
	16.1.6	Aprendizaje de incidentes de Seguridad de la Información	Consiste en la utilización de los conocimientos adquiridos para analizar y resolver incidentes de seguridad futuros.	
	16.1.7	Colección de evidencia	Consiste en el procedimiento para la identificación, recopilación, adquisición y conservación de evidencia que pueda servir como prueba.	
17 Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio	17,1	Seguridad de la Información en la Continuidad		
	17.1.1	Planeación de Seguridad de la Información en la continuidad	Consiste en el desarrollo e implementación de una política para la continuidad de la gestión de seguridad en condiciones adversas	
	17.1.2	Implementación de Seguridad de la Información en la continuidad	Consiste en establecer, documentación, implementar los procesos, procedimientos y controles necesarios de continuidad para la seguridad de la información.	

	17.1.3	Verificación, revisión y evaluación de Seguridad de la Información en la continuidad	Consiste en la verificación de los controles de continuidad de seguridad de la información.	
	17,2	Redundancias		
	17.2.1	Disponibilidad de facilidades de procesamiento de información	Consiste en la redundancia suficiente para satisfacer los requisitos de disponibilidad.	
18 Cumplimiento	18,1	Revisiones de Seguridad de la Información		
	18.1.1	Revisión independiente de Seguridad de la Información		Consiste en la revisión independiente a intervalos planificados o cuando se produzcan cambios significativos de la gestión y aplicación de la seguridad de la información si esto afecta a los BYOD.
	18.1.2	Cumplimiento con políticas y estándares de seguridad		Consiste comprobar periódicamente el cumplimiento de las políticas y estándares de seguridad a los BYOD.
	18.1.3	Inspección de cumplimiento técnico		Consiste en la revisión regular de los sistemas de información para el cumplimiento de las políticas y normas de seguridad de la información.
	18,2	Cumplimiento con Requerimientos Legales y Contractuales		
	18.2.1	Identificación de legislación aplicable y requerimientos contractuales	Consiste en la identificación de la legislación pertinente	
	18.2.2	Derechos de propiedad intelectual (IPR)	Consiste en los procedimientos para garantizar el cumplimento legal sobre los derechos de propiedad intelectual	
	18.2.3	Protección de información documentada	Consiste en la protección contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada de conformidad a los requisitos legales.	

	18.2.4	Privacidad y protección de información personal identificable	Consiste en la privacidad y protección de la información de identificación personal	
	18.2.5	Regulación de controles criptográficos	Consiste en la utilización de controles criptográficos cumpliendo con los acuerdos pertinentes, legislaciones y reglamentos.	

Anexo 2 Matriz de Calificación ISO/IEC 27002:2013 SOA para BYOD

	DOMINIO	OBJ DE CONTROL	CONTROLES	PROMEDIO	RAMIRO	ROBIN	JUAN MANUEL
5. POLÍTICAS DE SEGURIDAD.	5						
5.1 Directrices de la Dirección en seguridad de la información.		5,1					
5.1.1 Conjunto de políticas para la seguridad de la información			5.1.1	**3,5**	4	3	**SI**
5.1.2 Revisión de las políticas para la seguridad de la información			5.1.2	**3,5**	4	3	**SI**
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	6						
6.1 Organización interna.		6,1					
6.1.1 Asignación de responsabilidades para la segur. de la información.			6.1.1	**1**	1	1	**NO**
6.1.2 Segregación de tareas.			6.1.2	**1,5**	2	1	**NO**
6.1.3 Contacto con las autoridades.			6.1.3	**1**	2	0	**NO**
6.1.4 Contacto con grupos de interés especial.			6.1.4	**0,5**	1	0	**NO**
6.1.5 Seguridad de la información en la gestión de proyectos.			6.1.5	**1,5**	1	2	**NO**
6.2 Dispositivos para movilidad y teletrabajo.		6,2					
6.2.1 Política de uso de dispositivos para movilidad.			6.2.1	**5**	5	5	**SI**
6.2.2 Teletrabajo.			6.2.2	**5**	5	5	**SI**

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7						
7.1 Antes de la contratación.		7,1					
7.1.1 Investigación de antecedentes.			7.1.1	**0**	0	0	**NO**
7.1.2 Términos y condiciones de contratación.			7.1.2	**0**	0	0	**NO**
7.2 Durante la contratación.		7,2					
7.2.1 Responsabilidades de gestión.			7.2.1	**0**	0	0	**NO**
7.2.2 Concienciación, educación y capacitación en segur. de la informac.			7.2.2	**4**	5	3	**SI**
7.2.3 Proceso disciplinario.			7.2.3	**0**	0	0	**NO**
7.3 Cese o cambio de puesto de trabajo.		7,3					
7.3.1 Cese o cambio de puesto de trabajo			7.3.1	**4**	3	5	**SI**
8. GESTIÓN DE ACTIVOS.	8						
8.1 Responsabilidad sobre los activos.		8,1					
8.1.1 Inventario de activos.			8.1.1	**3,5**	4	3	**SI**
8.1.2 Propiedad de los activos.			8.1.2	**4,5**	4	5	**SI**
8.1.3 Uso aceptable de los activos.			8.1.3	**4**	3	5	**SI**
8.1.4 Devolución de activos.			8.1.4	**4**	3	5	**SI**
8.2 Clasificación de la información.		8,2					
8.2.1 Directrices de clasificación.			8.2.1	**0,5**	0	1	**NO**
8.2.2 Etiquetado y manipulado de la información.			8.2.2	**0,5**	0	1	**NO**
8.2.3 Manipulación de activos.			8.2.3	**1**	0	2	**NO**
8.3 Manejo de los soportes de almacenamiento.		8,3					
8.3.1 Gestión de soportes extraíbles.			8.3.1	**1**	1	1	**NO**
8.3.2 Eliminación de soportes.			8.3.2	**1**	1	1	**NO**
8.3.3 Soportes físicos en tránsito			8.3.3	**0**	0	0	**NO**
9. CONTROL DE ACCESOS.	9						
9.1 Requisitos de negocio para el control de accesos.		9,1					
9.1.1 Política de control de accesos.			9.1.1	**4,5**	4	5	**SI**
9.1.2 Control de acceso a las redes y servicios asociados.			9.1.2	**5**	5	5	**SI**

9.2 Gestión de acceso de usuario.		9,2					
9.2.1 Gestión de altas/bajas en el registro de usuarios.			9.2.1	**0,5**	1	0	**NO**
9.2.2 Gestión de los derechos de acceso asignados a usuarios.			9.2.2	**4,5**	4	5	**SI**
9.2.3 Gestión de los derechos de acceso con privilegios especiales.			9.2.3	**4,5**	4	5	**SI**
9.2.4 Gestión de información confidencial de autenticación de usuarios.			9.2.4	**5**	5	5	**SI**
9.2.5 Revisión de los derechos de acceso de los usuarios.			9.2.5	**4,5**	4	5	**SI**
9.2.6 Retirada o adaptación de los derechos de acceso			9.2.6	**4,5**	4	5	**SI**
9.3 Responsabilidades del usuario.		9,3					
9.3.1 Uso de información confidencial para la autenticación.			9.3.1	**4**	3	5	**SI**
9.4 Control de acceso a sistemas y aplicaciones.		9,4					
9.4.1 Restricción del acceso a la información.			9.4.1	**4,5**	4	5	**SI**
9.4.2 Procedimientos seguros de inicio de sesión.			9.4.2	**4**	3	5	**SI**
9.4.3 Gestión de contraseñas de usuario.			9.4.3	**4**	4	4	**SI**
9.4.4 Uso de herramientas de administración de sistemas.			9.4.4	**3,5**	4	3	**SI**
9.4.5 Control de acceso al código fuente de los programas			9.4.5	**1**	2	0	**NO**
10. CIFRADO.	10						
10.1 Controles criptográficos.		10,1					
10.1.1 Política de uso de los controles criptográficos.			10.1.1	**1**	1	1	**NO**
10.1.2 Gestión de claves.			10.1.2	**4**	4	4	**SI**
11. SEGURIDAD FÍSICA Y AMBIENTAL.	11						
11.1 Áreas seguras.		11,1					
11.1.1 Perímetro de seguridad física.			11.1.1	**0,5**	0	1	**NO**
11.1.2 Controles físicos de entrada.			11.1.2	**0**	0	0	**NO**

11.1.3 Seguridad de oficinas, despachos y recursos.			11.1.3	**0**	0	0	**NO**
11.1.4 Protección contra las amenazas externas y ambientales.			11.1.4	**0**	0	0	**NO**
11.1.5 El trabajo en áreas seguras.			11.1.5	**0**	0	0	**NO**
11.1.6 Áreas de acceso público, carga y descarga.			11.1.6	**0**	0	0	**NO**
11.2 Seguridad de los equipos.		11,2					
11.2.1 Emplazamiento y protección de equipos.			11.2.1	**3,5**	4	3	**SI**
11.2.2 Instalaciones de suministro.			11.2.2	**1**	2	0	**NO**
11.2.3 Seguridad del cableado.			11.2.3	**0,5**	1	0	**NO**
11.2.4 Mantenimiento de los equipos.			11.2.4	**0**	0	0	**NO**
11.2.5 Salida de activos fuera de las dependencias de la empresa.			11.2.5	**4**	3	5	**SI**
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.			11.2.6	**4**	3	5	**SI**
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.			11.2.7	**4**	3	5	**SI**
11.2.8 Equipo informático de usuario desatendido.			11.2.8	**4**	4	4	**SI**
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.			11.2.9	**0,5**	1	0	**NO**
12. SEGURIDAD EN LA OPERATIVA.	12						
12.1 Responsabilidades y procedimientos de operación.		12,1					
12.1.1 Documentación de procedimientos de operación.			12.1.1	**0,5**	1	0	**NO**
12.1.2 Gestión de cambios.			12.1.2	**0,5**	1	0	**NO**
12.1.3 Gestión de capacidades.			12.1.3	**0,5**	1	0	**NO**
12.1.4 Separación de entornos de desarrollo, prueba y producción.			12.1.4	**0,5**	1	0	**NO**
12.2 Protección contra código malicioso.		12,2					
12.2.1 Controles contra el código malicioso.			12.2.1	**4,5**	4	5	**SI**
12.3 Copias de seguridad.		12,3					
12.3.1 Copias de seguridad de la información.			12.3.1	**1**	2	0	**NO**

12.4 Registro de actividad y supervisión.		12,4					
12.4.1 Registro y gestión de eventos de actividad.			12.4.1	**4,5**	5	4	**SI**
12.4.2 Protección de los registros de información.			12.4.2	**0,5**	0	1	**NO**
12.4.3 Registros de actividad del administrador y operador del sistema.			12.4.3	**0**	0	0	**NO**
12.4.4 Sincronización de relojes.			12.4.4	**0,5**	1	0	**NO**
12.5 Control del software en explotación.		12,5					
12.5.1 Instalación del software en sistemas en producción.			12.5.1	**0**	0	0	**NO**
12.6 Gestión de la vulnerabilidad técnica.		12,6					
12.6.1 Gestión de las vulnerabilidades técnicas.			12.6.1	**4**	4	4	**SI**
12.6.2 Restricciones en la instalación de software.			12.6.2	**2**	4	0	**NO**
12.7 Consideraciones de las auditorías de los sistemas de información.		12,7					
12.7.1 Controles de auditoría de los sistemas de información.			12.7.1	**0,5**	0	1	**NO**
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	13						
13.1 Gestión de la seguridad en las redes.		13,1					
13.1.1 Controles de red.			13.1.1	**3,5**	4	3	**SI**
13.1.2 Mecanismos de seguridad asociados a servicios en red.			13.1.2	**3,5**	4	3	**SI**
13.1.3 Segregación de redes.			13.1.3	**3,5**	4	3	**SI**
13.2 Intercambio de información con partes externas.		13,2					
13.2.1 Políticas y procedimientos de intercambio de información.			13.2.1	**1**	1	1	**NO**
13.2.2 Acuerdos de intercambio.			13.2.2	**1,5**	2	1	**NO**
13.2.3 Mensajería electrónica.			13.2.3	**1,5**	1	2	**NO**
13.2.4 Acuerdos de confidencialidad y secreto			13.2.4	**1**	1	1	**NO**
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	14						

14.1 Requisitos de seguridad de los sistemas de información.		14,1					
14.1.1 Análisis y especificación de los requisitos de seguridad.			14.1.1	**4**	4	4	**SI**
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes publicas			14.1.2	**4**	4	4	**SI**
14.1.3 Protección de las transacciones por redes telemáticas.			14.1.3	**4,5**	5	4	**SI**
14.2 Seguridad en los procesos de desarrollo y soporte.		14,2					
14.2.1 Política de desarrollo seguro de software.			14.2.1	**0**	0	0	**NO**
14.2.2 Procedimientos de control de cambios en los sistemas.			14.2.2	**0**	0	0	**NO**
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo			14.2.3	**0,5**	1	0	**NO**
14.2.4 Restricciones a los cambios en los paquetes de software.			14.2.4	**0,5**	1	0	**NO**
14.2.5 Uso de principios de ingeniería en protección de sistemas.			14.2.5	**0**	0	0	**NO**
14.2.6 Seguridad en entornos de desarrollo.			14.2.6	**0**	0	0	**NO**
14.2.7 Externalización del desarrollo de software.			14.2.7	**0**	0	0	**NO**
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.			14.2.8	**0**	0	0	**NO**
14.2.9 Pruebas de aceptación.			14.2.9	**0**	0	0	**NO**
14.3 Datos de prueba.		14,3					
14.3.1 Protección de los datos utilizados en pruebas.			14.3.1	**0,5**	0	1	**NO**
15. RELACIONES CON SUMINISTRADORES.	15						
15.1 Seguridad de la información en las relaciones con suministradores.		15,1					
15.1.1 Política de seguridad de la información para suministradores.			15.1.1	**0,5**	1	0	**NO**
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.			15.1.2	**0,5**	1	0	**NO**

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.			15.1.3	**0,5**	1	0	**NO**
15.2 Gestión de la prestación del servicio por suministradores.		15,2					
15.2.1 Supervisión y revisión de los servicios prestados por terceros.			15.2.1	**0,5**	1	0	**NO**
15.2.2 Gestión de cambios en los servicios prestados por terceros.			15.2.2	**0,5**	1	0	**NO**
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16						
16.1 Gestión de incidentes de seguridad de la información y mejoras.		16,1					
16.1.1 Responsabilidades y procedimientos.			16.1.1	**0,5**	0	1	**NO**
16.1.2 Notificación de los eventos de seguridad de la información.			16.1.2	**5**	5	5	**SI**
16.1.3 Notificación de puntos débiles de la seguridad.			16.1.3	**4**	4	4	**SI**
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.			16.1.4	**0,5**	0	1	**NO**
16.1.5 Respuesta a los incidentes de seguridad.			16.1.5	**1**	1	1	**NO**
16.1.6 Aprendizaje de los incidentes de seguridad de la información.			16.1.6	**1**	1	1	**NO**
16.1.7 Recopilación de evidencias.			16.1.7	**0,5**	0	1	**NO**
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17						
17.1 Continuidad de la seguridad de la información.		17,1					
17.1.1 Planificación de la continuidad de la seguridad de la información.			17.1.1	**0,5**	0	1	**NO**
17.1.2 Implantación de la continuidad de la seguridad de la información.			17.1.2	**0**	0	0	**NO**
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la informacion			17.1.3	**0**	0	0	**NO**
17.2 Redundancias.		17,2					

17.2.1 Disponibilidad de instalaciones para el procesamiento de la informacion			17.2.1	**0**	0	0	**NO**
18. CUMPLIMIENTO.	18						
18.1 Cumplimiento de los requisitos legales y contractuales.		18,1					
18.1.1 Identificación de la legislación aplicable.			18.1.1	**0,5**	0	1	**NO**
18.1.2 Derechos de propiedad intelectual (DPI).			18.1.2	**1**	0	2	**NO**
18.1.3 Protección de los registros de la organización.			18.1.3	**0,5**	0	1	**NO**
18.1.4 Protección de datos y privacidad de la información personal.			18.1.4	**1,5**	1	2	**NO**
18.1.5 Regulación de los controles criptográficos.			18.1.5	**0,5**	0	1	**NO**
18.2 Revisiones de la seguridad de la información.		18,2					
18.2.1 Revisión independiente de la seguridad de la información.			18.2.1	**4,5**	4	5	**SI**
18.2.2 Cumplimiento de las políticas y normas de seguridad.			18.2.2	**4,5**	4	5	**SI**
18.2.3 Comprobación del cumplimiento.			18.2.3	**4,5**	4	5	**SI**