PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial

Tesis Para optar por el Título de Ingeniero Informático que presenta el bachiller:

Ramon Simón Bruderer Vega

Asesor: Mg. Moisés Antonio Villena Aguilar

Lima, Julio de 2019

Resumen

En los últimos años los dispositivos móviles se han vuelto una herramienta muy valiosa para las organizaciones porque por medio de ellas se puede manejar información muy valiosa para las mismas. Sin embargo, debido al valor de la información manejada estos dispositivos se han vuelto blanco de diversos tipos de ataques con el fin de afectar la confidencialidad, integridad o disponibilidad de la información manejada por dichos dispositivos.

Por esta razón para el presente proyecto de fin de carrera se recopilara información de los estándares de NIST y de la ISO 27032 para elaborar un modelo de ciberseguridad que permita establecer controles para proteger los dispositivos móviles y la información manejada por ellos.

Este modelo estará conformado por la lista de componentes, la lista de categorías, la lista de subcategorías (objetivos de control), los niveles de prioridad de cada subcategoría, las precondiciones del modelo, los indicadores del modelo, la guía de implementación del modelo y el procedimiento que se seguirá para la validación del modelo.

En la guía de implementación se encontrara las estructuras de gobierno sugeridas, una lista de amenazas de ciberseguridad para dispositivos móviles y el procedimiento que se seguirá para realizar una evaluación previa para determinar el estado actual de la seguridad de la organización y determinar los controles que faltan implementar para lograr el nivel de protección deseado. Además al final de la guía se encontrara las actividades recomendadas para implementar controles asociados a las subcategorías.

Este modelo ha sido validado a través del juicio experto y además este modelo ha participado en la 11th IADIS International Conference on Information System 2018 en Lisboa, Portugal. (Bruderer, Villena, Tupia, & Bruzza, 2018)

Tema FCI

Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial

Tabla de Contenido

Índice de Ilustraciones

Índice de Tablas

Capítulo 1. Generalidades

Problemática

Hoy en día se viene presentando un incremento en los casos de ataques cibernéticos en varios países del mundo, esto a partir de la gran cantidad de casos que se hacen públicos donde se afecta a la disponibilidad, confidencialidad e integridad de la información de las personas u organizaciones. Entre estos casos se puede mencionar el caso de Stuxnet, en el que se usó un gusano informático conocido como Stuxnet, empleado para destruir las instalaciones de enriquecimiento de combustible de uranio en Irán (Berghel, 2015). Otro caso es el de hackers que accedieron a la red de una de las compañías que gestiona las plantas nucleares en Corea del Sur y robó información importante sobre el diseño de los reactores e información de los empleados de las plantas (News, 2015). Asimismo en Sony se sustrajo gran cantidad de información de la compañía relacionada con información de los empleados y documentos de planeación, además de infectar algunas computadoras de la empresa (Whyte, 2016). Estos casos son solo algunos, pero en realidad existen más, incluso una gran cantidad donde los ataques no se reportan. (Esterbrook, 2002) En la ilustración 1 se puede ver el crecimiento de ataques de malware durante el periodo de 2014 a 2015.

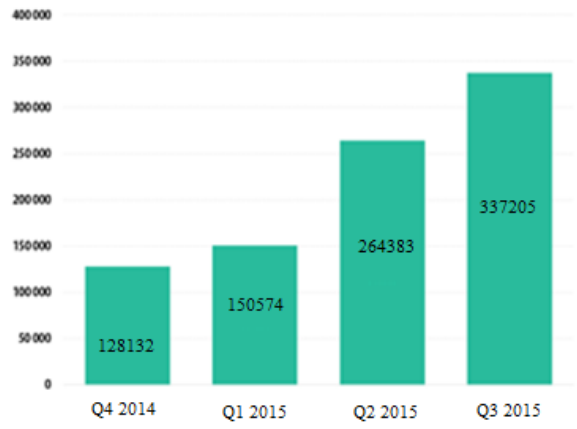


Ilustración 1- Grafico de crecimiento de ataques de malware del 2014 al 2015. Tomada de (Garnaeva, Wiel, Makrushin, Ivanov, & Namestnikov, 2015)

Además, estos ataques han aumentado su sofisticación llevando al desarrollo de nuevas formas de ataque como es el caso de los nuevos tipos de malware tales como el ransomware. El ransomware es un tipo de malware el cual tiene como objetivo modificar la información de un usuario dejándola inentendible o bloquear las operaciones normales del equipo infectado, esto lo hace con el fin de pedir cambio de

devolver la información o el equipo a su estado original el pago de un rescate. Además este malware puede ser usados para infectar también dispositivos móviles como laptops, tablets y celulares (Garnaeva, Wiel, Makrushin, Ivanov, & Namestnikov, 2015).

Para entender mejor el problema de los ataques cibernéticos, se definirá lo que es un ataque cibernético en sí. Según la US National Research Council apud (Pipyros, Mitrou, Gritzalis, & Apostolopoulos, 2016), los ataques cibernéticos son definidos como "acciones deliberadas para alterar, interrumpir, engañar, degradar o destruir los sistemas informáticos, redes o la información y/o programas residentes o en tránsito por estos sistemas o redes" .Otra definición de ataque cibernético es la de Ben-Asher y González, que define los ataques cibernéticos como "la disrupción del funcionamiento normal de las computadoras y la perdida de información sensible a través de una red maliciosa de eventos" (Ben-Asher & Gonzalez, 2015). A partir de lo citado respecto al concepto de ataque cibernético, se puede visualizar la amenaza que estos representan y la necesidad de plantear medidas para protegerse de ellos. Esta protección de sistema cibernéticos o redes frente a las amenazas cibernéticas o ataques cibernéticos se conoce como ciberseguridad o seguridad cibernética (Refsdal, Solhaug, & Stølen, 2015). Entre las medidas de ciberseguridad posibles están el uso de software de antivirus, detección de intrusos, antimalware, marcos, estándares. Entre los marcos se destaca el de NIST, que es un marco que se caracteriza por mejorar la infraestructura critica de ciberseguridad en una organización y la administración de los riesgos de ciberseguridad bajo un enfoque priorizado y flexible. (NIST, 2018)

Las organizaciones usan diversos tipos de dispositivos como son las laptop o las tablets pero ahora estos no son los únicos dispositivos usados sino que también se están usando los dispositivos móviles, los cuales incluso no son entregados por la propia organización así que no tienen medidas de protección implementadas. Estos equipos cuentan con una gran cantidad de vulnerabilidades que los hacen susceptibles a ataques cibernéticos, a pesar de esto las organizaciones permiten que un 74% de sus empleados usen sus dispositivos móviles en el trabajo. El problema es que las organizaciones que usan estos dispositivos no toman en cuenta que un 35% de las comunicaciones enviadas por ellos no está cifrada. Además los dispositivos móviles permiten acceder o almacenan información de las organizaciones que los usan pero estos al tener una serie de vulnerabilidades exponen a las organizaciones frente a las amenazas de ciberseguridad. (NowSecure, 2016).

En la ilustración 2 se muestra que las personas no toman las mínimas medidas de seguridad para protegerse de amenazas de ciberseguridad que tienen como objetivo dispositivos móviles, tal es el caso de tener un software antivirus, que un 45% no cuentan con este software. (Mani, Choo, & Mubarak, 2014)

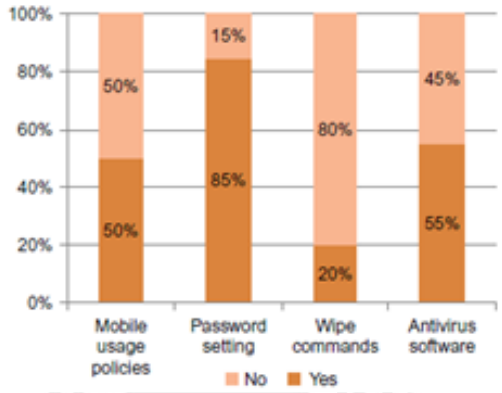


Ilustración 2 - Porcentaje de personas que toman medidas de protección para sus dispositivos móviles. Tomada de (Mani, Choo, & Mubarak, 2014)

En conclusión, los dispositivos móviles a pesar de ser muy útiles tienen varias vulnerabilidades propia de ellos y en el uso de ellos que los hace un objetivo atractivo para los atacantes cibernéticos para afectar la confidencialidad, integridad o disponibilidad de la información de las organizaciones, empleados o clientes. Por esta razón, para enfrentar este problema lo que se propone como proyecto de fin de carrera es diseñar un modelo de gestión de ciberseguridad para dispositivos móviles del sector empresarial.

Objetivos

1. Objetivo general

Diseñar un modelo de ciberseguridad para dispositivos móviles en el sector empresarial

2. Objetivos específicos

O 1. Definir los componentes del modelo.
O 2. Definir los procesos del modelo
O 3. Definir las métricas del modelo
O 4. Elaborar la guía de implementación del modelo
O 5. Validar el modelo por medio del juicio experto

3. Resultados esperados

R 1. Lista de Componentes del modelo (O1)

R 2. Lista de categorías a usar en el modelo (O2)

R 3. Lista de subcategorías asociadas a cada categoría (O2)

R 4. Los niveles de prioridad de cada subcategoría (O2)

R 5. Precondiciones del modelo (O3)

R 6. Los indicadores del modelo (O3)

R 7. Guía de implementación del modelo (O4)

R 8. Conformidad de los expertos (O5)

4. Mapeo de objetivos, resultados y verificación

Objetivo: Definir los componentes del modelo.		
Resultado	**Meta física**	**Medio de verificación**
Lista de Componentes del modelo	Documento	- Contrastación con los componentes del marco de NIST y juicio experto
Herramienta: NIST		

Objetivo: Definir los procesos del modelo		
Resultado	**Meta física**	**Medio de verificación**
Lista de categorías a usar en el modelo Lista de subcategorías asociadas a cada categoría Los niveles de prioridad de cada subcategoría	Documento	- Juicio experto
Herramienta: ISO 27032 y NIST		

Objetivo: Definir las métricas del modelo		
Resultado	**Meta física**	**Medio de verificación**
Los indicadores del modelo	Documento	- Juicio experto
Herramienta: ISO 27032 y NIST		

Objetivo: Elaborar la guía de implementación del modelo		
Resultado	**Meta física**	**Medio de verificación**
Guía de implementación del modelo	Documento	- Juicio experto
Herramienta: ISO 27032 y NIST		

Objetivo: Validar el modelo por medio del juicio experto		
Resultado	**Meta física**	**Medio de verificación**
Conformidad de los expertos	Documento	- Resultados de los cuestionarios
Herramienta: Juicio experto		

Herramientas y Métodos

Framework de NIST

Es un marco que contiene principios y prácticas de administración del riesgo que busca mejorar la seguridad de la infraestructura critica de una organización. Además, emplea una aproximación basada en riesgo para administrar los riesgos de ciberseguridad y está compuesto de tres (3) partes: el núcleo del marco, los niveles de implementación del marco y los perfiles del marco (NIST, 2018).

El núcleo del Marco: En el núcleo del marco se definen una serie de funciones que son la identificación, protección, detección, respuesta y recuperación. Por medio de estas se logra tener una visión estratégica del ciclo de vida de la administración del riesgo de ciberseguridad de la organización.

Ilustración 3 - Grafico de Marco de NIST 2 (NIST, 2018)

Las categorías son las subdivisiones de las funciones en grupos de resultados de ciberseguridad estrechamente ligadas con las necesidades programáticas y actividades particulares, El marco de *NIST* hace uso de 22 categorías.

La subcategoría es la división de una categoría en una actividad técnica o de gestión especifica. Estas subcategorías brindan resultados que permiten apoyar el logro de los resultados que se plantean en las categorías, el marco de *NIST* emplea 98 subcategorías.

Las referencias informativas son los estándares, guías y prácticas comunes relacionadas con la infraestructura de la organización que permiten colaborar en el logro de los resultados de las subcategorías. (NIST, 2018)

Los niveles de implementación del Marco: proporcionan un contexto de como una organización considera los riesgos de ciberseguridad y los procesos para gestionarlos,

pero estos niveles no representan niveles de madurez; por tanto un cambio a niveles más altos se da cuando un cambio reduce los riesgos de ciberseguridad, los niveles son: el 1 es parcial, el 2 es riesgo informado, e 3 es repetitivo y el 4 es adaptativo.

Para cada uno de estos niveles se revisa el proceso de administración de riesgos, el programa integrado de administración de riesgo y la participación externa.

El marco de *NIST* será usado para la elaboración de la estructura como para la elaboración de la lista de actividades de ciberseguridad que usara el marco a elaborar.

ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity

Es un estándar que provee guías para mejorar el estado de la ciberseguridad en las organizaciones, en el que se ven aspectos como la seguridad de la información, la seguridad de redes, seguridad de internet y protección de la estructura critica de la información. Además se hace una visión general de lo que es ciberseguridad, la relación que esta tiene con los otros tipos de seguridad que existen, una definición de los interesados y sus roles en la ciberseguridad, guía para abordar problemas relacionados con la ciberseguridad y un marco para permitir a los interesados colaborar en resolver problemas de ciberseguridad (ISO, 2012)

Juicio Experto

El juicio experto se da según (Benini, y otros, 2017) cuando “expertos dan sus opiniones en un contexto de toma de decisiones”. El proceso que se sigue para realizar el juicio experto consta de los siguientes pasos que se ven en la ilustración siguiente: (Benini, y otros, 2017)

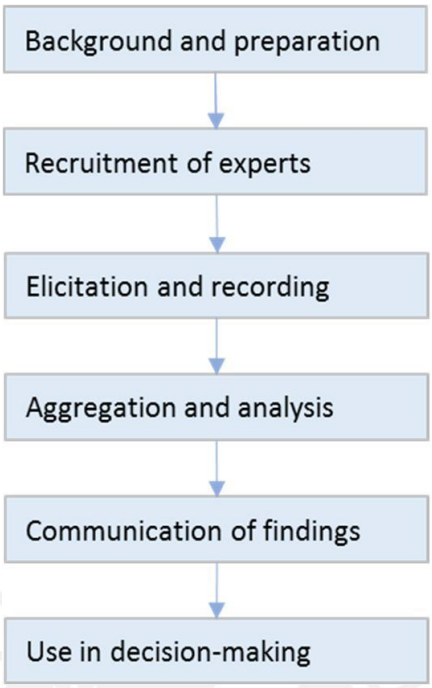


Ilustración 4 - Fases del Juicio Experto. Tomada de (Benini, y otros, 2017)

En estos pasos se tienen que definir el objetivo que se quiere lograr a través del juicio experto, los criterios que se seguirán para la selección de los expertos, la forma que se seguirá para recopilar información de los expertos, El modo que se seguirá para realizar el análisis de la información y la forma en que se comunicara los resultados del análisis a los expertos. (Benini, y otros, 2017)

Usos

Esta norma será usada como una herramienta para la elaboración de la clasificación de amenazas de ciberseguridad a las que están expuestos los dispositivos móviles, además también será usado en la elaboración del listado de las actividades que permitan la prevención de ataques cibernéticos a dispositivos móviles.

La norma ISO 27032 será usada tanto para la elaboración de la lista de amenazas de ciberseguridad que atacan dispositivos móviles como para la elaboración de la lista de amenazas de ciberseguridad para combatir las amenazas listadas.

Se extraerá información de ambas herramientas para la elaboración de todos los resultados excepto la validación por medio del juicio experto. Se usara primero el marco de NIST a la hora de definir la estructura del modelo (Categorías, Subcategorías, Prioridades), lo cual forma parte de la lista de componentes, además de las publicaciones especiales de NIST y el total de categorías se elaborara tanto las

categorías, subcategorías y la guía de implementación. La ISO 27032 se usara como fuente de información adicional a la hora de elaborar las subcategorías y la guía de implementación.

Por ultimo para obtener la conformidad de los expertos se hará uso del juicio experto que consistirá en la validación de una serie de objetivos que se definirán que permitan comprobar que el modelo propuesto funciona y su contenido es el adecuado.

Alcance y limitaciones

El alcance de este proyecto de fin de carrera abarcara el diseño de un modelo de ciberseguridad, el cual se basara en recopilación de información del modelo de NIST y la ISO 27032. Este proyecto está dirigido a las empresas que hagan uso de dispositivos móviles para manejar la información de sus empleados o procesos como en el caso del uso de BYOD en las empresas. Es decir este proyecto busca evitar la pérdida de la disponibilidad, integridad o confidencialidad la información en la organización por el desconocimiento o manejo inadecuado de equipos.

En caso una organización tenga alguna regulación vigente que lo obligue a proteger la información que se maneje por medio de los dispositivos móviles, este modelo le permitirá además de proteger los dispositivos móviles frente amenazas cibernéticas, apoyar de manera parcial al cumplimiento de dicha regulación.

Viabilidad

1. **Viabilidad Técnica**

Es viable técnicamente porque se cuenta con marcos de referencia y con estudios de software empleado por dispositivos móviles

2. **Viabilidad Temporal**

El proyecto se completara en el tiempo establecido del semestre y se le dedicara entre 2 a 3 horas diarias para la elaboración del proyecto

3. **Viabilidad Económica**

Se requerirá la norma ISO 27032 con las que cuenta la universidad en la biblioteca.

Alcance, Limitaciones y Riesgos

- Este proyecto abarca el diseño del modelo pero no se incluirá una prueba de este modelo en un ambiente real, es decir el modelo se probara no en una empresa u organización sino que se validara por medio del uso del juicio de expertos
- El modelo que se elaborara en este proyecto no evolucionara al mismo ritmo que evolucionan las amenazas cibernéticas

Riesgos del proyecto

Probabilidad/Impacto: 1(baja), 2(media), 3(alta) Severidad: Probabilidad x Impacto

Tabla 1 - Tabla de Riesgos del Proyecto

Riesgo	Probabilidad	Impacto	Severidad	Descripción	Síntomas	Mitigación	Contingencia
Falta de tiempo por el experto para evaluar el proyecto	Media(2)	Media(2)	Media(4)	El experto se toma demasiado tiempo para dar sus observaciones	Varios días sin responder ni entregar las observaciones	Comunicarse con el experto para tener claro los plazos	Previamente contar con tiempo extra en caso de que se presentase esta situación
Ausencia de Experto para la evaluación del proyecto	Media(2)	Alta(3)	Alta(6)	Que el experto que se encargara de evaluar el proyecto no pueda	Ausencia de comunicación con el experto	Conversar con mi asesor para verificar que el experto si pueda realizar su labor	Conversar con mi asesor para tener otras opciones
Cambios muy significativos en el proyecto propuesto por el experto	Baja(1)	Media(2)	Baja(2)	Retraso del proyecto debido a la gran cantidad de cambios propuesto por el experto	Fallas en los avances presentados	Completar con la menor cantidad de errores el proyecto	Dedicar más tiempo a completar los cambios propuestos
Retraso debido a algún problema de salud	Alta(3)	Baja(1)	Media(3)	Reducción del tiempo para el proyecto debido a una enfermedad	Malestar estomacal o de cabeza	Cuidarse adecuadamente para reducir la probabilidad de enfermarse	Ir a el doctor lo antes posible para tratarse y recuperarse lo antes posible
Retraso en la recolección de información para el proyecto	Media(2)	Media(2)	Media(4)	Retraso en la recolección de información para la elaboración del modelo	Retrasos en la búsqueda de información	Recolectar la mayor cantidad de información posible previamente	Dedicar más tiempo al proyecto hasta que se recolecte la información necesaria

Capítulo 2. Marco Legal/Regulatorio/Conceptual/otros

Marco Conceptual

1. Núcleo del marco

Según NIST “El núcleo del marco provee un juego de actividades para lograr resultados específicos de ciberseguridad, y ejemplos de referencia de guía para lograr estos resultados. El núcleo no es una lista de verificación de acciones a realizar. Este presenta los resultados de ciberseguridad claves identificados por la industria como útiles en la administración de riesgos de ciberseguridad. El núcleo comprime 4 elementos: función, categoría, subcategoría y referencia informativa”. (NIST, 2018) Este es otro de los componentes del marco de NIST.

2. Función

Según NIST “Organiza actividades de ciberseguridad básica a alto nivel. Estas funciones son identificar, proteger, detectar, responder y recuperar” (NIST, 2018)

3. Categorías

Según NIST (Agesic, 2016) como “Es las subdivisión de las actividades básicas de ciberseguridad en grupos de resultados de ciberseguridad estrechamente ligadas a las actividades funcionales y actividades particulares”. Ejemplos de Categoría son seguridad de datos, control de accesos y evaluación de riesgos. Las categorías están incluidas dentro del núcleo del marco de NIST que es uno de sus componentes,

4. Subcategorías

Según NIST (Agesic, 2016) como “Dividen las categorías en resultados concretos de las actividades técnicas y/o de gestión. Proporcionan un conjunto de resultados que ayudan al logro de resultados de cada categoría”. Un ejemplo de Subcategorías para la categoría de control de accesos seria acceso físico a los activos es administrado y protegido, también para esta misma categoría puede ser que el acceso remoto sea administrado.

5. Perfiles del marco

Según NIST “El perfil del marco puede ser caracterizado como la alineación de estándares, guías y prácticas a el núcleo del marco de NIST en un particular escenario de implementación. Estos pueden ser usados para identificar oportunidades para

mejorar la postura de ciberseguridad por comparar el perfil actual que se tiene con el perfil objetivo que se quiere llegar". (NIST, 2018) Este es otro de los componentes del marco de NIST.

6. Niveles de Implementación del marco

Según NIST "Provee un contexto sobre cómo ve la organización a los riesgos de ciberseguridad y el proceso en el lugar para administrar riesgo. Niveles describen el grado el cual las prácticas de gestión de riesgos de ciberseguridad de una organización exhibe las características definidas en el marco". (NIST, 2018). Este además es otro de los componentes del marco de NIST.

7. Juicio de Expertos

Según (Hora, 209):"el juicio de expertos involucra la ponderación de la evidencia disponible y llegar una conclusión equilibrada a partir de la evidencia. Se traen expertos para realizar estos juicios porque ellos desarrollan las herramientas mentales necesarias para hacer las sound evaluations."

8. **Modelo**

Un modelo es una representación de la realidad que es usado para facilitar la experimentación, evaluar diferentes escenarios y determinar la sensibilidad de una decisión tomada, para de esta forma mejorar la eficacia de la toma de decisiones. Un modelo permite asistir tanto en el diseño como en la elección de fases. Sin embargo, la confianza en los datos históricos y el grado de simplificación o abstracción son problemas que están asociados a la hora de construir un modelo. (Caine & Robson, 1993)

9. Ataques cibernéticos

Según US National Research Council apud (Pipyros, Mitrou, Gritzalis, & Apostolopoulos, 2016) los ataques cibernéticos son definidos como "acciones deliberadas para alterar, interrumpir, engañar, degradar o destruir los sistemas informáticos, redes o la información y/o programas residentes o en tránsito por estos sistemas o redes"

10. Ciberseguridad

Según (ISO, 2012) "Es la preservación de la disponibilidad, integridad y confidencialidad en el ciberespacio "

11. Amenaza

Según (ISO, 2012) “Causa potencial de un incidente no deseado que puede generar un daño en un individuo, sistema u organización “

12. Monitoreo Continuo de la seguridad

Según NIST apud (Agesic, 2016) “Los sistemas de información y los activos son monitoreados a intervalos discretos para identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección”

13. Gestión de Activos

Según NIST apud (Agesic, 2016) “Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación a los objetivos y la estrategia de riesgo de la organización “

14. Evaluación de Riesgos

Según NIST apud (Agesic, 2016) “La empresa comprende los riegos de ciberseguridad de sus operaciones, activos e individuos “

15. Estrategia para la gestión de riesgos

Según NIST apud (Agesic, 2016) “Se establecen las prioridades, restricciones, tolerancia al riesgo y supuestos de la organización y se utilizan para soportar las decisiones de los riesgos operacionales “

16. Control de Acceso

Según NIST apud (Agesic, 2016) “El acceso a los activos e instalaciones se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas”

17. Concientización y Formación

Según NIST apud (Agesic, 2016) “El personal de la organización y socios de negocios, reciben entrenamiento y concientización sobre seguridad de la información. Están adecuadamente entrenados para cumplir con sus obligaciones referentes a la seguridad de la información en alineación con las políticas, procedimientos y acuerdos existentes”

18. Seguridad de Datos

Según NIST apud (Agesic, 2016) “La información y registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información “

19. Procesos y procedimientos para la protección de información

Según NIST apud (Agesic, 2016) “Las políticas de seguridad, procesos y procedimientos que se mantienen y son utilizados para gestionar la protección de los sistemas de información y los activos”

20. Sanitización

Según NIST: “Sanitización se refiere a un proceso que hace imposible el acceso a los datos en los dispositivos para un determinado nivel de esfuerzo” Esto quiere decir que a los datos en un dispositivos se los alteraran de alguna forma que estos sean muy difícil o imposible de recuperar. Esto con el fin de garantizar la confidencialidad de la información destruida (Kissel, Regenscheid, Scholl, & Stine, 2014)

Marco Regulatorio

Ley °29733: Ley de Protección de datos personales

Ley dictada el 3 de julio de 2011 por el congreso de la república del Perú con el objetivo de garantizar el derecho fundamental a la protección de los datos personales. Esto a través de un adecuado tratamiento respetando los derechos fundamentales de estos datos. En esta ley se encuentran los principios rectores, las normas relacionadas al tratamiento de datos personales, los derechos del titular de datos personales, obligaciones del titular y del encargado del banco de datos personales, banco de datos personales, autoridad nacional de protección de datos personales e infracciones y sanciones administrativas. (Ley N° 29733, Ley de Proteccion de Datos Personales, 2011)

NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.

Esta norma fue publicada el 1 de diciembre de 2014 y fue elaborada por el comité de normalización de codificación e intercambio electrónico de datos. Esta norma reemplaza a la norma NTP ISO/IEC 27001:2008 y es una adopción de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27001:2013/COR 1. Esta norma tiene como objetivo proporcionar los requisitos para establecer, implementar, mantener y mejorar

continuamente un sistema de gestión de seguridad de la información. Esta norma está conformada de 7 secciones las cuales son contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejoras. (Comite-de-normalizacion-de-codificacion-e-intercambio-electronico-de-datos, 2014)

Capítulo 3. Estado del Arte

Revisión y discusión

El método que se siguió para la revisión sistemática del estado del arte consta de 4 pasos que son elaborar las preguntas de investigación, la estrategia de búsqueda, el proceso de búsqueda y la selección de los Papers. (Bruzza & Tupia, 2016) Luego de completar la revisión sistemática se buscaran los marcos o modelos de ciberseguridad usados o desarrollados por otros países.

Pasó 1: Elaborar las preguntas de investigación:

Pregunta 1:

¿Qué modelo o marco han sido usados a la hora de implementar ciberseguridad para dispositivos móviles?

Pregunta 2:

¿Qué modelos o marcos de ciberseguridad para dispositivos móviles se han basado en estándares o buenas prácticas internacionalmente aceptados?

Pasó 2: Decidir la estrategia de búsqueda:

La estrategia de búsqueda seria la elección de las cadenas de búsqueda a usar en el buscador debido a que la mayoría de los Papers están en ingles se usara las cadenas en inglés, La elección de las cadenas será relacionada a marcos o modelos de ciberseguridad o ciberseguridad para dispositivos móviles que serían las siguientes:

- Framework Cyber Security
- Cyber Security mobile device Framework

Pasó 3: Ejecutar el proceso de búsqueda:

Tabla 2 - Resultado de búsqueda de revisión sistematica

Base de Datos	Cadena de Búsqueda usada	Papers
ProQuest	(Framework Cyber Security MOBILE DEVICE) AND Framework Cyber Security)	19668

IEEE Explorer	((Framework Cyber Security MOBILE DEVICE) AND Framework Cyber Security)	71
Springer	(Framework Cyber Security)	26799

Pasó 4: Selección de los Papers:

En este paso se elaboraran los criterios de inclusión o exclusión:

Criterios de Inclusión: Que debe contener un paper para que pueda incluirse entre los Papers seleccionados

- Un Paper contiene información relacionada a la ciberseguridad de los dispositivos móviles
- Un Paper que proponga un marco de ciberseguridad para dispositivos móviles
- Un Paper que proponga un modelo de ciberseguridad para dispositivos móviles
- Un Paper que describa los componentes de un marco o modelo de ciberseguridad
- Un Paper que describa un software usado para evaluar un marco o modelo de ciberseguridad
- Un Paper que describa los factores críticos que debe tener un marco o modelo de ciberseguridad para dispositivos móviles

Criterios de Exclusión: Que carece o no tiene el paper por lo que no se seleccionara entre los paper

- Paper no muestra un marco o modelo de ciberseguridad
- Paper no contiene información relacionada a dispositivos móviles

Respuesta a preguntas

Pregunta 1:

¿Qué modelo o marco han sido usados a la hora de implementar ciberseguridad para dispositivos móviles?

Los modelos o marcos usados mayormente para mejorar la ciberseguridad de los dispositivos móviles son marcos de ciberseguridad generales que incluyen una parte temas de ciberseguridad para dispositivos móviles

Pregunta 2:

¿Qué modelos o marcos de ciberseguridad para dispositivos móviles se han basado en estándares o buenas prácticas internacionalmente aceptados?

No hay marcos de ciberseguridad para dispositivos móviles pero si hay marcos de ciberseguridad que se basen en estándares o buenas prácticas. Como son los marcos de Agesic de Uruguay y el marco de ciberseguridad de Italia los cuales se basan en NIST.

Papers y Frameworks seleccionados

A Practical Framework and Guidelines to Enhance Cyber Security and Privacy

Este marco está desarrollado para ayudar a los dueños de sistemas que contienen información privada a proteger sus sistemas, datos y privacidad de sus clientes. Este marco consiste en un juego de guía a seguir para mejorar la ciberseguridad de los sistemas y la privacidad de los usuarios y sus datos.

Las principales características de este marco son las siguientes:

- **Tecnología independiente**: Esto significa que el marco puede ser aplicado por cada organización en cada dominio. Esto quiere decir que este marco no es para un sector o tamaño específico.
- **Centrada en el usuario**: Esto significa que el marco se enfoca en los usuarios clave que son los dueños del sistema que contiene la información privada, los desarrolladores del sistema y ciudadanos.
- **Practicidad**: Esto significa que le marco lista las guías prácticas y controles a seguir para mejorar o comprobar si la organización está protegiendo la información de amenazas cibernéticas
- **Fácil de usar y amigable con el usuario**: No se enfoca en las tecnologías y no requiere un habilidad particular

(Choras, Kozik, Renk, & Holubowicz, 2015)

NICE Cybersecurity Worforce Framework

Este marco hace uso de 3 componentes que son las categorías, las áreas de especialidad y los roles de trabajo en el que se incluyen las tareas y las KSA (Knowledge, Skills, Abilities). El componente referido a las categorías se refiere al agrupamiento de alto nivel de funciones de ciberseguridad comunes. Las áreas de especialidad se refieren a las áreas de trabajo de ciberseguridad. Con respecto al componente de los roles de trabajo se refiere a los grupos detallados de TI, ciberseguridad que incluye conocimiento específico, capacidades y habilidades requeridas para realizar tareas específicas.

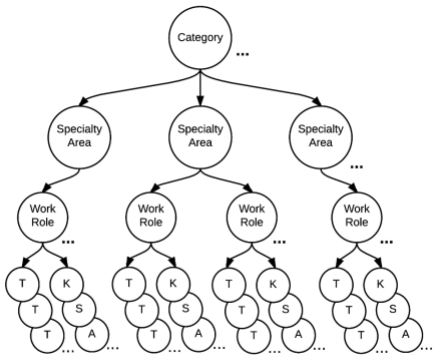


Figure 2 - Relationships among NCWF Components

Ilustración 5 - Relaciones entre componentes del NICE Cybersecurity Worforce Framework (Newhouse, Keith, Scribner, & Witte, 2016)

Además el marco cuenta con una guía para apoyar como aplicar este marco. (Newhouse, Keith, Scribner, & Witte, 2016)

Aquí se pueden ver las categorías y áreas de especialidad del marco.

Categorías:

Análisis: Responsable por altamente especializada revisión y evaluación de información de ciberseguridad entrante para determinar su utilidad para la inteligencia.

Áreas de Especialidad:

- Todas las fuentes de inteligencia
- Explotación de análisis
- Objetivos
- Análisis de amenazas

Recolección y Operación: Responsable por operaciones especializadas de denegación y decepción y colección de información de ciberseguridad que puede ser usada para desarrollar inteligencia.

Áreas de Especialidad:

- Colección de operaciones
- Ciberoperaciones
- Planeamiento de ciberoperaciones

Investigación: Son responsables por la investigación de cibereventos y crímenes de sistemas de TI, redes y evidencias digitales.

Áreas de Especialidad:

- Informática forense
- Investigación

Operación y Mantenimiento: Proveer soporte administración a mantenimiento necesario a asegurar efectiva y eficientemente sistemas de TI desempeño y seguridad.

Áreas de Especialidad:

- Servicio al cliente y soporte técnico
- Administración de datos
- Gestión del conocimiento
- Servicios de red
- Administración de sistemas
- Análisis de seguridad de sistemas

Vigilancia y Desarrollo: Proveer liderazgo, gestión, dirección y desarrollo y apoyo de tal forma que todos los individuos y la organización puedan conducir efectivamente trabajos de ciberseguridad.

Áreas de Especialidad:

- Educación y entrenamiento
- Operaciones de seguridad de sistemas de información
- Consejo y apoyo legal
- Gestión de programas de seguridad

- Planeamiento estratégico y política de desarrollo

Proteger y Defender: Identificación, análisis y mitigación a amenazas de sistemas o redes de TI internos.

Áreas de Especialidad:

- Análisis de defensa de redes de computadoras
- Soporte a la infraestructura de redes de computadoras
- Respuesta a incidentes
- Evaluación y gestión de vulnerabilidades

Aprovisionamiento seguro: Se refiere a la conceptualización, diseño y construcción seguro de sistemas de TI.

Áreas de Especialidad:

- Cumplimiento de la garantía de a información
- Garantía de software e ingeniería segura
- Desarrollo de sistemas
- Planeación de requerimientos de sistemas
- Arquitectura Segura de sistemas
- Investigación y desarrollo tecnológico
- Prueba y evaluación
  (Newhouse, Keith, Scribner, & Witte, 2016)

Framework Nazionale per la Cyber Security

Es un marco de ciberseguridad basado en NIST que deriva los tres (3) conceptos fundamentales del marco que son el núcleo, el perfil y los niveles. Lo adicional que plantea son niveles de prioridad para ayudar a las organizaciones y compañías a identificar las subcategorías a implementar para reducir sus niveles de riesgo. Estos niveles de prioridad son alta, media y baja. Además este marco presenta un modelo de madurez para poder medir el nivel de madurez de un proceso de seguridad o de la implementación de una tecnología especifica (Baldoni & Montanari, 2016)

Ilustración 6 - Grafico de Marco de Framework Nazionale de Italia (Baldoni & Montanari, 2016)

En este marco se aplican medidas para prevenir los ataques a dispositivos móviles que son actividades como la capacitación, la detección de un código móvil no autorizado, emplear las soluciones de detección de malware en los móviles y el uso de estos con licencias que permitan adquirir actualizaciones de seguridad.

Este marco cuenta con 3 componentes principales el primero es el núcleo donde se incluyen las categorías y subcategorías del marco. El segundo componente son los niveles de prioridad asociadas a cada subcategoría. El último componente son los niveles de madurez. Además también cuenta con guías para la implementación de las categorías de alta prioridad. (Baldoni & Montanari, 2016)

Marco de Ciberseguridad de AGESIC

Es un marco de ciberseguridad basado en el marco de seguridad de *NIST* haciendo uso de las cinco (5) funciones definido en el núcleo de NIST que son: identificar, proteger, detectar, responder y recuperar. Además se incluyen las categorías y subcategorías definidas en el núcleo aunque no todas las subcategorías definidas en NIST pueden estar incluidas. En este marco de ciberseguridad también se definen perfiles, prioridades para cada perfil y un modelo de madurez, además para cada subcategoría se establecen requisitos mínimos a cumplir. En la ilustración 1-3 se puede ver la estructura de este marco de ciberseguridad. (Agesic, 2016)

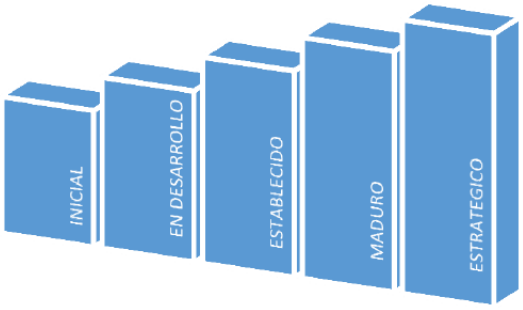


Ilustración 7 - Modelo de Madurez usado en marco de AGESIC (Agesic, 2016)

En la ilustración 1-3 se puede ver el modelo de madurez planteado para este marco de ciberseguridad. Consta de cinco (5) niveles que son: inicial, en desarrollo, establecido, maduro y estratégico. Además define cinco (5) niveles de prioridad de 1 a 4 y N/A si la subcategoría no se va aplicar. Los perfiles usados en este marco son tres (3) que son: básico, estándar y avanzado. En la ilustración 1-4 se puede ver la estructura del marco de ciberseguridad (Agesic, 2016)

Función	Categoría	Subcategoría	Prioridad x Perfil			Madurez				Ref.	Requisitos
			B	E	A	M1	M2	M3	M4		
Identificar											
Proteger											
Detectar											
Responder											
Recuperar											

Ilustración 8 - Grafico del Marco de AGESIC (Agesic, 2016)

Algunas de las actividades planteadas aquí son las que se emplean para tratar el problema de las amenazas de ciberseguridad en dispositivos móviles, tales como el monitoreo continuo de la seguridad para la detección de códigos maliciosos y el bloqueo de acceso a sitios web maliciosos por medio de dispositivos móviles, para de esta forma, prevenir los ataques cibernéticos por medio de estos dispositivos.

Este marco cuenta con 2 componentes que son el marco de ciberseguridad en si donde se incluyen las categorías, subcategorías, perfiles y prioridades del marco, El

segundo componente es el modelo de madurez. Además este marco tiene una guía de implementación del marco.

Como se puede notar la mayoría de los marcos de ciberseguridad que hay están orientados a ciberseguridad en general y no a proteger a los dispositivos móviles, por ende lo que se quiere lograr es apoyar a la mejora de esta deficiencia por medio del desarrollo de un marco de ciberseguridad orientado a dispositivos móviles.

Otros Papers relacionados

CRUMBS: a Cyber Security Framework Browser

Es una solución de análisis visual que provee a los usuarios con una homogénea y comprensible representación visual de todos los aspectos técnicos envueltos en el proceso de adopción de NIST a través del uso del Framework Nazionale per la Cyber Security. En la ilustración a continuación se puede ver un gráfico con el prototipo implementado de la solución. (Angelini, Lenti, & Santucci, 2017)

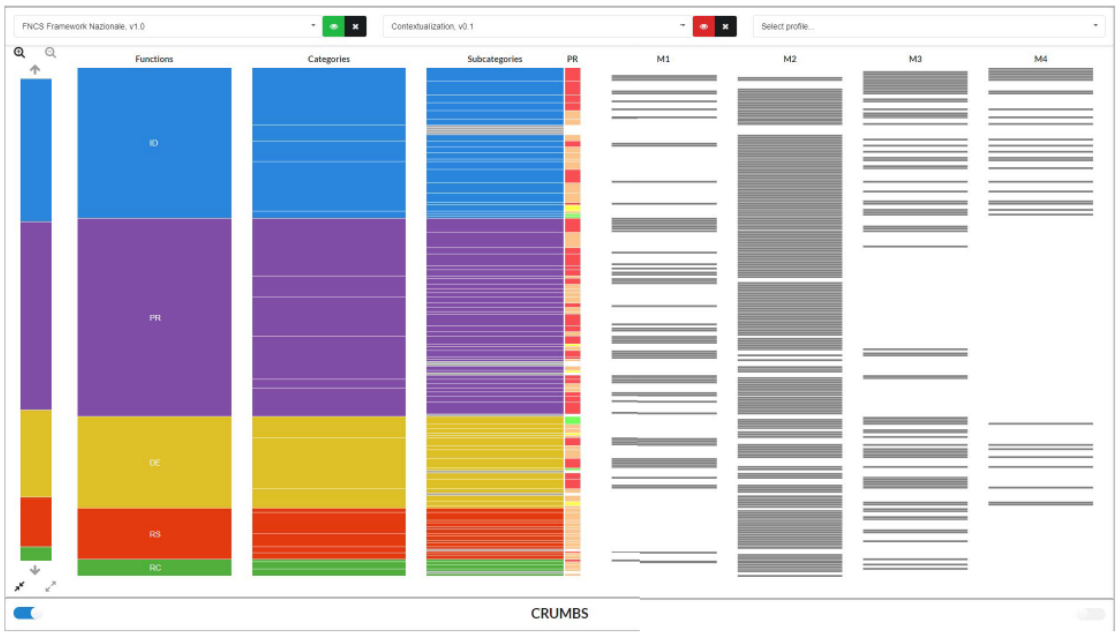


Ilustración 9 - Prototipo de CRUMBS (Angelini, Lenti, & Santucci, 2017)

Esta solución ha sido diseñada con el objetivo de ayudar a los administradores de seguridad a administrar, diseñar, implementar y revisar las actividades asociadas a cada subcategoría. (Angelini, Lenti, & Santucci, 2017)

Conclusiones

En conclusión la mayoría de los marco de ciberseguridad son muy pocos y no están orientados a aplicaciones o los dispositivos móviles en sí por lo que esto evidencia la necesidad de proponer este modelo. Además no todos los modelos o marcos hallados cuentan con algún software que permita administrar y revisar el avance y estado de la implementación del modelo.

Capítulo 4. Lista de Componentes (O1)

En este capítulo se describirán cada uno de los componentes del modelo como son los procesos del modelo, las métricas y la guía de implementación, los cuales se pueden ver en la ilustración 9.

Ilustración 10 - Diagrama de Componentes del modelo

Primero se definirá que es un dispositivo móvil. Un dispositivo móvil es definido como “Un dispositivo portable de computo que: tiene un pequeño factor forma que le permite ser cargado fácilmente por un individuo; es diseñado para operar sin una conexión física; posee local, no-removible o removible almacenamiento de datos e incluye un auto contenido fuente de poder. Los dispositivos móviles pueden incluir capacidades de comunicación de voz, sensores incorporados que permiten a los dispositivos capturar información, y/o características incorporadas para sincronizar datos locales con locaciones remotas. Ejemplos de dispositivos móviles incluyen Smart phones, tablets, a E-readers” (Brown, y otros, 2016)

A continuación se presenta la descripción de los componentes del modelo que se mencionaron previamente.

- **Componente 1: Procesos del modelo**

Los procesos del modelo están conformados por tres partes que son: las categorías del modelo, las subcategorías asociadas a las categorías y los niveles de prioridad del modelo.

a) Categorías del modelo: La primera parte de los procesos del modelo son las categorías del modelo. La definición de categoría según (Agesic, 2016) es “Es la subdivisión de las actividades básicas de ciberseguridad en grupos de

resultados de ciberseguridad estrechamente ligadas a las actividades funcionales y actividades particulares". Las actividades básicas de ciberseguridad son identificar, proteger, detectar, responder y recuperar. (Agesic, 2016)

Las categorías del modelo se tomaran del marco de ciberseguridad de NIST. Para determinar cuál categorías se usaran en el modelo primero se identificaran las subcategorías y luego sus categorías asociadas.

b) Subcategorías: Éstas dependen de las categorías seleccionadas puesto que su definición según (Agesic, 2016) como "Dividen las categorías en resultados concretos de las actividades técnicas y/o de gestión. Proporcionan un conjunto de resultados que ayudan al logro de resultados de cada categoría". Esto quiere decir que las subcategorías están asociadas a las categorías y que vendrían a ser los objetivos de control de una categoría. Para definir las subcategorías primero se seleccionaran los objetivos de seguridad y luego se recopilara información para la definición de las subcategorías que estén ligadas al logro de los objetivos de seguridad.
c) Niveles de prioridad: La asignación de los niveles de prioridad consiste en dos partes. Primero se priorizaran las categorías en función de las actividades de seguridad que se relacionan y luego de esto se ordenaran internamente cada subcategoría en función de diferentes criterios.
   Ejemplo:

Categoría	Subcategoría – Descripción (Objetivo de Control)	Nivel de prioridad
Seguridad de los datos	Protección de la información - Datos almacenados y transmitidos por los dispositivos móviles se encuentran protegidos	Ninguno[*]

[*] Esta categoría presenta una única subcategoría, por lo cual no requiere un nivel de prioridad.

- **Componente 2: Los Indicadores del modelo**

Los indicadores del modelo se usaran para evaluar el funcionamiento del modelo. Se definirán indicadores para las subcategorías del modelo, los cuales incluirán el objetivo del indicador. En función de los valores tomados de dichos indicadores se determinara la efectividad que está teniendo el modelo.

Ejemplo:

Nombre: % de lecciones aprendidas implementadas	
Propósito: Comprobar si se aprendiendo de incidentes pasados	Forma de medición: Numero de lecciones aprendidas implementadas/Total de lecciones aprendidas identificadas
Subcategoría – Descripción : Gestión del conocimiento - Lecciones aprendidas de los incidentes están implementadas	
Valor de referencia permitido: 50 % (Deben implementar al menos 50% de las lecciones aprendidas)	
Frecuencia de medición: trimestral	

- **Componente 3: La guía de implementación del modelo**

La guía de implementación del modelo es una guía que servirá para implementación del modelo, la cual contendrá una serie de actividades recomendadas para la implementación de cada una de las subcategorías del modelo. Estas actividades no solo estarán agrupadas por subcategorías sino también por las categorías. El orden que se seguirá para la implementación de dichas actividades se hará en función de los niveles de prioridad de las subcategorías y categorías del modelo. Además la guía contara con un procedimiento para hacer la autoevaluación del estado de la organización y también sugerirá una estructura de gobierno para implementar el modelo.

Capítulo 5. Lista de Categorías (O2)

Las categorías del modelo son una parte muy importante de los procesos de este modelo, por esta razón las categorías que usara este modelo son las categorías usadas en el marco de ciberseguridad de NIST (NIST, 2018). No obstante, debido que este modelo es específico para dispositivos móviles, no se incluirán todas las categorías del marco de NIST.

El procedimiento que se siguió para la selección de las categorías es el siguiente:

1. Definir previamente la lista de subcategorías
2. Revisar la lista de subcategorías e identificar a que categoría del total de categorías del marco de NIST pertenecen
3. Incluir las categorías identificadas previamente en la lista de categorías del modelo

   Luego de seguir este procedimiento (Ver anexo 3), se obtiene como resultado la siguiente lista de categorías. A la derecha de las categorías se indica el criterio a emplear para incluir una subcategoría como parte de una categoría especifica del modelo:

Tabla 3 - Categorías del Modelo (NIST, 2018)

Categorías	Criterio de Inclusión de subcategorías
Gobierno de ciberseguridad	Estructura, políticas y procedimientos asignados por la alta dirección para establecer buenas prácticas de seguridad sobre dispositivos móviles.
Gestión de Activos	Los datos, dispositivos, aplicaciones y usuarios que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente
Gestión de riesgo de TI	Permite comprender los riesgos de ciberseguridad de los dispositivos móviles y aplicaciones y gestionar los riegos de TI
Concientización y formación	El personal de la organización recibe entrenamiento y concientización sobre ciberseguridad de los dispositivos

Categorías	Criterio de Inclusión de subcategorías
	móviles y/o tecnologías relacionadas.
Seguridad de los datos	La información y datos son protegidos para garantizar la confidencialidad, integridad y disponibilidad de la información
Control de acceso	El acceso a información de la organización por medio de dispositivos móviles se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas
Procesos y procedimientos para la protección de la información	Las políticas de seguridad, procesos y procedimientos se mantienen y son utilizados para garantizar la protección de la información
Tecnología de protección	Las tecnologías para la seguridad se gestionan para garantizar la seguridad y resistencia de los dispositivos móviles y aplicaciones de la organización frente a eventos de seguridad cibernética, en consonancia con las políticas, procedimientos y acuerdos
Monitoreo continuo de la seguridad	Los dispositivos móviles, la seguridad de los mismos y las actividades anómalas son monitoreados a intervalos discretos para identificar eventos de seguridad cibernética
Planificación de Respuesta	Los procesos y procedimientos de respuesta se ejecutan y se mantienen garantizando una respuesta oportuna para durante un evento de ciberseguridad
Comunicación	Las actividades para coordinar la respuesta y recuperación de incidentes con las partes interesadas internas y externas
Planificación de Recuperación	Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración

Categorías	Criterio de Inclusión de subcategorías
	oportuna de los sistemas o activos afectados por eventos de ciberseguridad
Mejora	Las actividades de respuesta de la organización, los planes y procesos de recuperación, los planes de comunicación y los controles establecidos se mejoran incorporando las lecciones aprendidas y las nuevas innovaciones

Capítulo 6. Lista de Subcategorías del modelo (O2)

Las subcategorías (objetivos de control) del modelo se elaborara a partir de la recolección de información de los estándares de NIST que guarden relación a la administración de los dispositivos móviles o riesgos asociados a ellos y la ISO 27032. Las fuentes utilizadas son los siguientes:

- NIST SP 800-124 Rev 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise (Souppaya & Scarfone, 2013)
- NIST SP 800-164 : Guidelines on Hardware-Rooted Security in Mobile Devices (Chen, Franklin, & Regenscheid, 2012)
- NIST SP 800-163: Vetting the Security of Mobile Applications (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015)
- NIST SP 800-61 Rev 2 (Draft): Computer Security Incident Handling Guide (Karen, Tom, Grance, & Paul, 2012)
- NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery (Bartock, et al., 2016)
- NIST Special Publication 800-118: Guide to Enterprise Password Management (Draft) (Scarfone & Souppaya, 2009)
- NIST Special Publication 800-121 Revision 2 (Draft): Guide to Bluetooth Security (Padgette, y otros, 2016)
- NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization (Kissel, Regenscheid, Scholl, & Stine, 2014)
- NIST Special Publication 800-45 Version 2: Guidelines on Electronic Mail Security (Tracy, Jansen, Scarfone, & Butterfield, 2007)
- ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity (ISO, 2012)
- NIST. (10 de Enero de 2017). *Framework for Improving Critical Infrastructure Cybersecurity.* (NIST, 2018)
- NIST, S. (2003). 800-53. *Recommended Security Controls for Federal Information Systems*, 800-53

El procedimiento que se seguirá para elaborar la lista de subcategorías es el siguiente:

1. Definir los objetivos de seguridad que se buscan lograr con las subcategorías

2. Recopilar información de las fuentes mencionadas previamente
3. Usar la información para definir las subcategorías que colaboren al logro de los objetivos previamente definidos

Los objetivos de seguridad que se quieren lograr se han obtenido de NIST SP 800-124 Rev 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise (Souppaya & Scarfone, 2013) y son los siguientes:

- Confidencialidad: Los datos transmitidos y almacenados no pueden ser leídos por personas no autorizadas (Souppaya & Scarfone, 2013)
- Integridad: Detectar cualquier cambio intencional o accidental de los datos almacenados o transmitidos (Souppaya & Scarfone, 2013)
- Disponibilidad: Asegurarse que los usuarios puedan acceder a los recursos usando dispositivos móviles (Souppaya & Scarfone, 2013)

Con los objetivos de seguridad previamente definidos. Se presenta a continuación la lista de subcategorías del modelo alineadas a su categoría correspondiente. El análisis de esta selección se encuentra en el anexo 3:

Lista de subcategorías del Modelo

Tabla 4 - Subcategorías del modelo

Categoría	Subcategoría	Descripción de Subcategoría	Referencia
Gestión de Activos	**Roles y Responsabilidades**	las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas	NIST SP 800-124, ISO 27032
	Control de Activos	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados	NIST SP 800-124, ISO 27032, NIST SP 800-53, NIST SP 800-45, NIST SP 800-121, NIST SP 800-164, NIST SP 800-118

Categoría	Subcategoría	Descripción de Subcategoría	Referencia
Gobierno de ciberseguridad	**Políticas de ciberseguridad para dispositivos móviles**	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	NIST SP 800-124, NIST SP 800-164, NIST SP 800-118, NIST SP 800-61
Gestión de riesgo de TI	**Riesgos de TI**	Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	NIST SP 800-163, NIST SP 800-124, ISO 27032
Concientización y formación	**Capacitación**	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	NIST SP 800-118, NIST SP 800-124, ISO 27032
	Concientización	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	NIST SP 800-61, NIST SP 800-121, NIST SP 800-124
Control de acceso	**Autenticación**	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos	NIST SP 800-124
Seguridad de los datos	**Protección de la información**	Datos almacenados y transmitidos por los dispositivos móviles se encuentran protegidos	NIST SP 800-124, NIST SP 800-118,NIST SP 800-45
Tecnología de protección	**Conectividad**	Las redes a las que se conectan los dispositivos móviles se encuentran administradas	NIST SP 800-124, ISO 27032, NIST SP 800-121

Categoría	Subcategoría	Descripción de Subcategoría	Referencia
Procesos y procedimientos para la protección de la información	**Desarrollo y mantenimiento de aplicaciones**	El desarrollo y mantenimiento de aplicaciones esta administrado	NIST SP 800-124, NIST SP 800-88, ISO 27032
	Limpieza de información de los dispositivos móviles	La limpieza de información de los dispositivos móviles está administrada	NIST SP 800-124, NIST SP 800-88
Monitoreo continuo de la seguridad	**Monitoreo de anomalías y amenazas**	Seguridad de los dispositivos móviles se encuentra monitoreada	NIST SP 800-124, ISO 27032
	Monitoreo del cumplimiento de las políticas y procedimientos	El cumplimiento de las políticas y procedimientos de seguridad para dispositivos móviles se encuentra monitoreada	NIST SP 800-124, ISO 27032
Planificación de Respuesta	**Respuesta a incidentes**	El procedimiento de respuesta incidentes esta implementado	NIST SP 800-61, ISO 27032
Comunicación	**Mesa de Ayuda**	Mesa de ayuda para el reporte de incidentes esta implementada	NIST SP 800-184, ISO 27032
	Planificación de comunicación	Plan de comunicación esta implementado	NIST SP 800-184, ISO 27032
Planificación de Recuperación	**Recuperación de incidentes**	El procedimiento de recuperación de incidentes esta implementado	NIST SP 800-184, ISO 27032
Mejora	**Gestión del Conocimiento**	Lecciones aprendidas están implementadas	NIST SP 800-61

Categoría	Subcategoría	Descripción de Subcategoría	Referencia
	Evaluación y Auditoría	Categorías se encuentren auditadas periódicamente	NIST SP 800-163
	Innovación	Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas	ISO 27032

Asimismo, se presenta la lista de relaciones entre subcategorías y los objetivos de seguridad:

Lista de relaciones entre subcategorías del modelo y objetivos de seguridad

Tabla 5 - Subcategorías del modelo con sus objetivos de seguridad

Subcategoría	Confidencialidad	Integridad	Disponibilidad
Roles y Responsabilidades	X	X	X
Control de Activos	X	X	X
Políticas de ciberseguridad para dispositivos móviles	X	X	X
Riesgos de TI	X	X	X
Capacitación	X	X	X
Concientización	X	X	X
Autenticación	X		
Protección de la información	X	X	
Conectividad	X		X

Desarrollo y mantenimiento de aplicaciones	X	X	X
Limpieza de información de los dispositivos móviles	X		
Monitoreo de anomalías y amenazas	X	X	X
Monitoreo del cumplimiento de las políticas y procedimientos	X	X	X
Respuesta a incidentes	X	X	X
Mesa de Ayuda	X		
Planificación de comunicación	X		
Recuperación de incidentes		X	X
Gestión del Conocimiento	X	X	X
Evaluación y Auditoría	X	X	X
Innovación	X	X	X

Capítulo 7. Los niveles de prioridad de cada subcategoría (O2)

Los niveles de prioridad servirán para determinar el orden de implementación de las categorías y subcategorías del modelo. Aquí se sugiere de forma referencial, la asignación de prioridades a las categorías, pero este orden no es fijo sino que puede variar según el nivel de exposición al riesgo por parte de la organización. La asignación de las prioridades a las subcategorías que se presentara aquí se hará en dos partes. Primero la priorización de la categorías y luego de las subcategorías dentro de cada categoría. La priorización de categorías se hará por medio de múltiples criterios uno de ellos es el modo de priorización usado en el marco de ciberseguridad de AGESIC que es según la actividad básica de ciberseguridad asociada a ellas, estas prioridades delimitan el orden de implementación de las categorías.

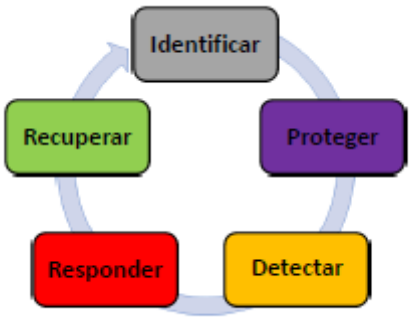


Ilustración 11 - Grafico de flujo de actividades de seguridad de marco de AGESIC (Agesic, 2016)

Otro criterio para priorizar ahora las categorías asociadas a cada actividad seria por el orden cronológico entre categorías es decir que para poder realizar una categoría requiere previamente que el anterior este ya implementada.

El orden cronológico se basara en el orden de que aparece en la implementación de la ISO 27001 en la que primero estaría toda la parte de políticas, y luego estaría la gestión de riesgo para la cual previamente se necesita contar con la gestión de activos para eso. Además las actividades de mejora y comunicación son las que se hacen al final así que dichas subcategorías estarían al final. (ISO, 2013)

Las categorías restantes están asociadas a la actividad de protección, para ordenar estas actividades primero se basara en la dificultad de su implementación. En este caso como Concientización y formación es una categoría que no necesita manejo de software para implementarse esta seria primero y al contrario como la categoría de tecnologías de implementación es la que tiene más categorías que requieren manejo de software esta sería el último. Para el resto de las 3 categorías se hará primero sería la de seguridad de los datos para garantizar que aun cuando se acceda a los datos no puedan ser leídos, luego seria de control de acceso para evitar que se acceda a estos datos y por ultimo Procesos y procedimientos para la protección de la información para evitar el filtrado de alguno de estos datos. Al final la tabla resultante sería esta:

Tabla 6 - Categorías ordenadas según su orden de implementación

Actividad Básica de Ciberseguridad	Categorías
Identificar	**Gobierno de ciberseguridad**
	Gestión de Activos
	Gestión de riesgo de TI
Proteger	**Concientización y formación**
	Seguridad de los datos
	Control de acceso
	Tecnología de protección
	Procesos y procedimientos para la protección de la información
Detectar	**Monitoreo continuo de la seguridad**
Responder	**Planificación de Respuesta**

Actividad Básica de Ciberseguridad	Categorías
	Comunicación
Recuperar	**Planificación de Recuperación**
	Mejora

Luego de tener priorizadas las categorías del modelo se priorizaran las subcategorías dentro de cada categoría asignándole un numero de prioridad entre las subcategorías dentro de cada categoría. Los criterios para asignar las prioridades entre las categorías no aplicaran a todas las subcategorías sino que se usaran diferentes cantidades o criterios por cada subcategoría y serán los siguientes:

- Facilidad de implementación: complejidad técnica de implementar la totalidad de la subcategoría (Baldoni & Montanari, 2016)
- Orden Cronológico entre subcategorías: La actividad debe realizarse en un momento específico o requiere que otra actividad se haya hecho antes en el tiempo
- Ninguno: Si solo cuenta con una sola subcategoría no se debe priorizar sus subcategorías

Estos criterios se aplicaran a las subcategorías de las categorías de la forma siguiente:

Tabla 7 - Categorías con sus criterios para ordenar sus subcategorías

Actividad Básica de Ciberseguridad	Categorías	Criterios para priorizar subcategorías
Identificar	**Gobierno de ciberseguridad**	Ninguno [*]
	Gestión de Activos	Orden Cronológico

Actividad Básica de Ciberseguridad	Categorías	Criterios para priorizar subcategorías
	Gestión de riesgo de TI	Ninguno [*]
Proteger	**Concientización y formación**	Orden Cronológico
	Seguridad de los datos	Ninguno [*]
	Control de acceso	Ninguno [*]
	Tecnología de protección	Ninguno [*]
	Procesos y procedimientos para la protección de la información	Orden Cronológico
Detectar	**Monitoreo continuo de la seguridad**	Facilidad de implementación
Responder	**Planificación de Respuesta**	Ninguno [*]
	Comunicación	Facilidad de implementación
Recuperar	**Planificación de Recuperación**	Ninguno [*]
	Mejora	Orden Cronológico

[*] Esta categoría presenta una única subcategoría, por lo cual no requiere un criterio para priorizar subcategorías.

Gestión de Activos: Se le asigna orden cronológico porque antes hacer los inventarios primero se tienen que asignar quien se va ocupar de ese rol

Concientización y formación: Se le asigna orden cronológico porque antes porque se obtiene un mayor beneficio si los usuarios están concientizados antes de ser capacitados

Procesos y procedimientos para la protección de la información: Se usa el orden cronológico ya que los procesos de limpieza al final del uso de los dispositivos móviles, es decir esta subcategoría iría al después

Monitoreo continuo de la seguridad: Se usa facilidad de implementación porque uno implica monitorear una mayor cantidad de objetivos que otro

Comunicación: Es más fácil elaborar una mesa de ayuda que elaborar el plan de comunicación ya que se tienen que revisar varios tipos de escenarios

Mejora: Se usa orden cronológico porque monitoreo de novedades debe hacerse de manera regular, lecciones aprendidas luego de incidentes y auditoria al final de todos los procesos

Lista de prioridades por subcategoría será el siguiente:

Tabla 8 - Subcategorías con prioridades

Categoría	Subcategoría	Orden por Categoría
Gobierno de ciberseguridad	**Políticas de ciberseguridad para dispositivos móviles**	Ninguno
Gestión de Activos	**Roles y Responsabilidades**	Prioridad 1
	Control de Activos	Prioridad 2
Gestión de riesgo de TI	**Riesgos de TI**	Ninguno
Concientización y formación	**Capacitación**	Prioridad 2
	Concientización	Prioridad 1
Seguridad de los datos	**Protección de la información**	Ninguno
Control de acceso	**Autenticación**	Ninguno
Tecnología de protección	**Conectividad**	Ninguno
Procesos y procedimientos para la protección de la información	**Desarrollo y mantenimiento de aplicaciones**	Prioridad 1
	Limpieza de información de los dispositivos móviles	Prioridad 2

Categoría	Subcategoría	Orden por Categoría
Monitoreo continuo de la seguridad	**Monitoreo de anomalías y amenazas**	Prioridad 1
	Monitoreo del cumplimiento de las políticas y procedimientos	Prioridad 2
Planificación de Respuesta	**Respuesta a incidentes**	Ninguno
Comunicación	**Mesa de Ayuda**	Prioridad 1
	Planificación de comunicación	Prioridad 2
Planificación de Recuperación	**Recuperación de incidentes**	Ninguno
Mejora	**Gestión del Conocimiento**	Prioridad 2
	Evaluación y Auditoría	Prioridad 3
	Innovación	Prioridad 1

Capítulo 8. Precondiciones del modelo (O3)

Para poder implementar el modelo previamente se requerirá de tener implementado un procedimiento de gestión de incidentes, porque sin tener este procedimiento no se podría diferenciar adecuadamente los tipos de incidentes y sin esa diferenciación no se podrían medir adecuadamente los valores requeridos en los indicadores del modelo. Para implementar la gestión de incidentes se recomienda usar algún modelo o metodología reconocido internacionalmente que te indique los pasos a seguir para implementar la gestión de incidentes en una organización. Aquí se sugerirá algunas indicaciones para implementar la gestión de incidentes basándose en el NIST SP 800-61 Rev 2 (Draft): Computer Security Incident Handling Guide (Karen, Tom, Grance, & Paul, 2012) . Las fases para la gestión de incidentes están agrupadas en 4 y son las siguientes: la fase de preparación; detección y análisis; contención, erradicación y recuperación, y Actividades post-incidentes. En el grafico siguiente se puede notar el flujo de las fases.

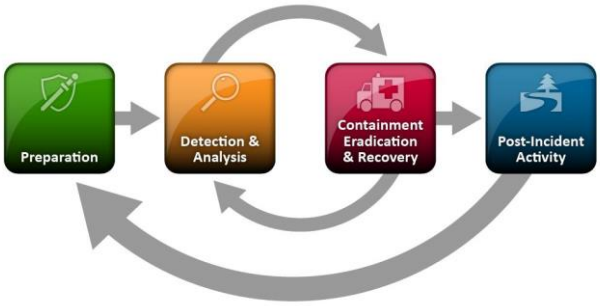


Ilustración 12 - Fases de la gestión de incidentes. Tomada de (Karen, Tom, Grance, & Paul, 2012)

Aquí se establecerán las indicaciones por fases para la implementación de la gestión de incidentes:

Fase de Preparación

- Establecer una política de gestión de incidentes (Karen, Tom, Grance, & Paul, 2012)
- Elaborar un plan de respuesta a incidentes (Karen, Tom, Grance, & Paul, 2012)
- Establecer un equipo de respuesta a incidentes asignándole a los mismos las responsabilidades y actividades de las que se encargaran (Karen, Tom, Grance, & Paul, 2012)

- Adquirir o establecer mecanismos de comunicación y coordinación para la gestión de incidentes como el uso de mecanismos de reporte de incidentes (teléfonos, correo, sistemas de mensajería instantánea seguros), uso de sistemas de rastreo de problemas (Usados para rastrear información de incidentes), uso de smartphones (para comunicarse en caso de que se requiera soporte fuera del horario laboral) y el establecimiento de un área de almacenamiento seguro (para almacenar evidencias y otros materiales sensibles) (Karen, Tom, Grance, & Paul, 2012)
- Adquirir hardware y software para análisis de incidentes como la adquisición de estaciones de trabajo forenses digitales (para crear imágenes de los discos, preservar los archivos de los log y almacenar otros datos relevantes de los incidentes), uso de laptops (para analizar datos, paquetes de sniff y escribir reportes), uso de software forense digital (para analizar las imágenes de los discos) y uso de herramientas para adquirir evidencias (cámaras digitales, grabadoras de sonido, bolsas para almacenar evidencias) (Karen, Tom, Grance, & Paul, 2012).
- Estos procedimientos se podrían tercerizar pero se tendrían que establecer acuerdos con la entidad contratada para que garanticen la confidencialidad de la información que ellos obtengan, su participación en los procedimientos de mejora del modelo y establecer de manera clara las funciones que debe cumplir la entidad contratada

Fase detección y análisis

- Establecer procedimientos para manejar incidentes de vectores de ataques conocidos como es el incumplimiento de los procesos o políticas establecidas (Karen, Tom, Grance, & Paul, 2012)
- Uso de herramientas para detectar signos de ataques como software de detección de intrusos, software para la gestión de eventos y seguridad de la información, software antivirus y antispam y software para comprobar la integridad de los archivos (Karen, Tom, Grance, & Paul, 2012)
- Establecer procedimientos manuales para poder reportar incidentes detectados por los usuarios (Karen, Tom, Grance, & Paul, 2012)

- Realizar el análisis y validación de los incidentes a través del uso de los perfiles de redes y sistemas, Entender el comportamiento normal de los sistemas, creación de una política de retención de log, realizar una correlación de eventos y filtrar los datos (Karen, Tom, Grance, & Paul, 2012)
- Llevar un registro sobre todos los hechos relacionados a los incidentes (Karen, Tom, Grance, & Paul, 2012)
- Priorizar los incidentes en función del impacto funcional del incidentes, el impacto en la información del incidente y la capacidad de recuperación del incidente (Karen, Tom, Grance, & Paul, 2012)
- Incluir en las políticas de respuesta a incidentes disposiciones relacionada a la notificación de incidentes (A quien y como se notifican los incidentes según el incidente) (Karen, Tom, Grance, & Paul, 2012)

Fase de contención, erradicación y recuperación

- Seleccionar las estrategias de contención según el tipo de incidente, daño potencial y robo de recursos, disponibilidad de los recursos, necesidad de preservación de la evidencia, eficacia de la estrategia y duración de la solución (Karen, Tom, Grance, & Paul, 2012)
- Establecer procedimientos para la recolección y retención de evidencias de incidentes (Karen, Tom, Grance, & Paul, 2012)
- Establecer actividades para la identificación de los atacantes como la validación de la dirección de IP del atacante, el uso de bases de datos de incidentes o el monitoreo de los posibles canales de comunicación de los atacantes (Karen, Tom, Grance, & Paul, 2012)
- Establecer procedimientos para erradicar los componentes de los incidentes como son los malware o cuentas usados en el incidente (Karen, Tom, Grance, & Paul, 2012)
- Establecer un plan para la recuperación de incidentes (Karen, Tom, Grance, & Paul, 2012)

Fase de actividades post-incidentes

- Establecer reunión sobre las lecciones aprendidas de los incidentes para analizar los incidentes y establecer mejoras en los procedimientos

de respuesta a incidentes y elaborar programa de capacitación en función de dicho análisis (Karen, Tom, Grance, & Paul, 2012)

- Recolectar información de los datos de los incidentes requeridos para la medición de los indicadores del modelo
- Establecer políticas sobre cuánto tiempo las evidencias de los incidentes deben ser retenidas (Karen, Tom, Grance, & Paul, 2012)

Capítulo 9. Indicadores del Modelo (O3)

El modelo contara con indicadores que permitan comprobar si están mejorando la seguridad de los dispositivos móviles en la organización o no. Estos indicadores contaran con un nombre que los identificara, una forma de medición, frecuencia de medición, la subcategoría asociada y el propósito del indicador. Los incidentes referidos en los indicadores son los incidentes relacionados a los dispositivos móviles no se incluyen todos los incidentes de seguridad.

Los valores de referencia y frecuencia de medición son recomendaciones no son valores que se deban seguir de manera estricta, ya que distintas organizaciones debido a las características propias de la empresa puede que manejen otros valores. Estos indicadores con sus valores de referencia se usaran posteriormente para un procedimiento de autoevaluación previa antes de implementar la guía del modelo. Los indicadores son los siguientes:

Categoría: Gestión de Activos

1) Subcategoría: Roles y Responsabilidades

Nombre: # de roles no asignados a los usuarios	
Propósito: Comprobar si todos los roles que se han creado han sido asignados	Forma de medición: Conteo del número de personas por cada rol e identificar y contar aquellos roles que no han asignados a nadie
Descripción de subcategoría: las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas	
Valor de referencia permitido: 0 roles (no deberían haber roles sin asignar)	
Frecuencia de medición: anual	

Nombre: # de incidentes producidos por incumplimiento de las responsabilidades asignadas a los usuarios	
Propósito: Comprobar si los usuarios cumplen con sus responsabilidades o no	Forma de medición: Conteo del número de incidentes por incumplimiento de las responsabilidades de los usuarios
Descripción de subcategoría: las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas	
Valor de referencia permitido: 5 incidentes (No debería haber de 5 incidentes)	
Frecuencia de medición: trimestral	

2) Subcategoría: Control de Activos

Nombre: # de aplicaciones y dispositivos desconocidos	
Propósito: Comprobar si se realizó correctamente los inventarios	Forma de medición: Conteo del número de dispositivos y aplicaciones que no se encuentran en los inventarios
Descripción de subcategoría: Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados	
Valor de referencia permitido: 10 aplicaciones (No se debe permitir más de 10)	
Frecuencia de medición: trimestral	

Nombre: # de errores en la clasificación	
Propósito: Comprobar si todos los dispositivos y aplicaciones están correctamente clasificados	Forma de medición: Conteo del número de dispositivos y aplicaciones que han sido clasificados de manera incorrecta
Descripción de subcategoría: Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados	
Valor de referencia permitido: 5 errores (No se debe permitir más de 5)	
Frecuencia de medición: trimestral	

Nombre: # de fallas detectadas en la seguridad de los dispositivos móviles	
Propósito: Comprobar si están asegurando correctamente los dispositivos móviles	Forma de medición: Conteo de número de fallas detectadas en la seguridad de los dispositivos móviles*
Descripción de subcategoría: Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados	
Valor de referencia permitido: 8 fallas (No se debe permitir más de 8)	
Frecuencia de medición: trimestral	

[*] Se cuenta como una falla en la seguridad si un dispositivo móvil no tiene instalada alguna medida de protección (configurado, con un antivirus o tecnologías para prevenir perdida de datos)

Categoría: Gobierno de ciberseguridad

1) Subcategoría: Políticas de ciberseguridad para dispositivos móviles

Nombre: Estado de la política (aprobada, formalizada, difundida, implementada)	
Propósito: Comprobar el estado de avance de la implementación de a las políticas	Forma de medición: Se comprobara si la política se encuentra aprobada, formalizada, difundida o implementada
Descripción de subcategoría: Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	
Valor de referencia permitido: La política debe estar aprobada, formalizada, difundida e implementada	
Frecuencia de medición: trimestral	

Nombre: # de violaciones a las políticas	
Propósito: Comprobar si las políticas están siendo de utilidad o si son solo documentos	Forma de medición: Conteo de número de violaciones de las políticas
Descripción de subcategoría: Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	
Valor de referencia permitido: 10 violaciones a las políticas (No se debe permitir más de 10)	
Frecuencia de medición: mensual	

Categoría: Gestión de riesgo de TI

1) Subcategoría: Riesgos de TI

Nombre: # de incidentes materializados por riesgos aceptados	
Propósito: Comprobar si los riesgos han sido tratados lo suficientemente bien	Forma de medición: Conteo de número de incidentes asociados a riegos tratados
Descripción de subcategoría: Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	
Valor de referencia permitido: 8 incidentes (No se debe permitir más de 8)	
Frecuencia de medición: trimestral	

Nombre: # de incidentes materializados por riesgos cuyo impacto fue mal evaluado	
Propósito: Comprobar si los riesgos han sido evaluados correctamente	Forma de medición: Conteo de número de incidentes ocurridos cuyo impacto fue mayor al esperado
Descripción de subcategoría: Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	
Valor de referencia permitido: 5 incidentes (No se debe permitir más de 8)	
Frecuencia de medición: trimestral	

Nombre: # de incidentes materializados por riesgos no identificados	
Propósito: Comprobar si se identificaron todos los riesgos	Forma de medición: Conteo de número de incidentes que no están asociados a ningún riesgo identificado
Descripción de subcategoría: Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	
Valor de referencia permitido: 4 incidentes (No se debe permitir más de 4)	
Frecuencia de medición: trimestral	

Categoría: Concientización y formación

1) Subcategoría: Capacitación

Nombre: # de errores de los usuarios durante los procesos de respuesta o recuperación de incidentes	
Propósito: Comprobar si se realizó correctamente la capacitación	Forma de medición: Conteo de número de errores presentados en los procesos de respuesta, recuperación o comunicación de incidentes
Descripción de subcategoría: Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	
Valor de referencia permitido: 8 errores (No se debe permitir más de 15)	
Frecuencia de medición: mensual	

Nombre: % de aprobados del total de capacitados	
Propósito: Comprobar si se está entendiendo la capacitación	Forma de medición: Número de aprobados de la capacitación/total de capacitados
Descripción de subcategoría: Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	
Valor de referencia permitido: 90% (Debe haber al menos un 90% de aprobados de las capacitaciones)	
Frecuencia de medición: semestral	

2) Subcategoría: Concientización

Nombre: # de incidentes producidos no reportados o mal reportados	
Propósito: Comprobar si los usuarios están concientizados	Forma de medición: Conteo de número de incidentes que se produjeron que no se reportaron o fueron mal reportados
Descripción de subcategoría: Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	
Valor de referencia permitido: 10 incidentes (No se debe permitir más de 10)	
Frecuencia de medición: mensual	

Categoría: Control de acceso

1) Subcategoría: Autenticación

Nombre: # de accesos no autorizados

Propósito: Comprobar si las medidas de seguridad para control de acceso son suficientes	Forma de medición: Conteo de número de accesos no autorizados
Descripción de subcategoría: Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos	
Valor de referencia permitido: 2 accesos no autorizados (No se debe permitir más de 2)	
Frecuencia de medición: mensual	

Categoría: Seguridad de los datos

1) Subcategoría: Protección de la información

Nombre: # de filtraciones de información	
Propósito: Comprobar si los datos están correctamente protegidos	Forma de medición: Conteo de número de filtraciones de información
Descripción de subcategoría: Datos almacenados y transmitidos se encuentran protegidos	
Valor de referencia permitido: 2 filtraciones (No se debe permitir más de 2)	
Frecuencia de medición: mensual	

Nombre: # de alteraciones en el flujo de información de cada dispositivo móvil	
Propósito: Comprobar si los datos están correctamente protegidos	Forma de medición: Conteo de número de alteraciones irregulares en el flujo de información

Descripción de subcategoría: Datos almacenados y transmitidos se encuentran protegidos
Valor de referencia permitido: 2 alteraciones (No se debe permitir más de 2)
Frecuencia de medición: mensual

Categoría: Tecnología de protección

1) Subcategoría: Conectividad

Nombre: # de dispositivos no autorizados conectados a la red	
Propósito: Comprobar si se está monitoreando y protegiendo adecuadamente las redes a las que se conectan los dispositivos moviles	Forma de medición: Conteo de número de dispositivos no autorizados que se encuentran conectados a la red
Descripción de subcategoría: Las redes a las que se conectan los dispositivos móviles se encuentran administradas	
Valor de referencia permitido: 5 dispositivos detectados (No se debe permitir más de 5)	
Frecuencia de medición: mensual	

Categoría: Procesos y procedimientos para la protección de la información

1) Subcategoría: Desarrollo y mantenimiento de aplicaciones

Nombre: # de aplicaciones que no tienen suficientes medidas de seguridad implementadas	
Propósito: Comprobar si las aplicaciones cuenta con las medidas de seguridad que garanticen la seguridad de la información manejada por ellos	Forma de medición: Conteo de número de aplicaciones a las que se comprueba que no tienen todas las medidas de seguridad necesarias

Descripción de subcategoría: El desarrollo y mantenimiento de aplicaciones esta administrado
Valor de referencia permitido: 3 aplicaciones (No se debe permitir más de 3)
Frecuencia de medición: semestral

Nombre: # de actualizaciones de seguridad de las aplicaciones desarrolladas realizadas	
Propósito: Comprobar si las aplicaciones están correctamente desarrolladas o si necesitan parcharse de manera constante	Forma de medición: Conteo de número de actualizaciones de seguridad hechas a las aplicaciones
Descripción de subcategoría: El desarrollo y mantenimiento de aplicaciones esta administrado	
Valor de referencia permitido: 3 actualizaciones (No se debe permitir más de 3)	
Frecuencia de medición: semestral	

2) Subcategoría: Limpieza de información de los dispositivos móviles

Nombre: # de fallas en el proceso de limpieza de información de los dispositivos móviles	
Propósito: Comprobar si la información de los dispositivos está correctamente borrada	Forma de medición: Conteo de número de dispositivos en los que no se borró correctamente la información
Descripción de subcategoría: La limpieza de información de los dispositivos móviles está administrada	

Valor de referencia permitido: 2 dispositivos (No se debe permitir más de 2)
Frecuencia de medición: trimestral

Categoría: Monitoreo continuo de la seguridad

1) Subcategoría: Monitoreo de anomalías y amenazas

Nombre: # de cambios no autorizados en la configuración de los dispositivos móviles no detectados a tiempo	
Propósito: Comprobar que los dispositivos no han sido sufrido cambios no autorizados en su configuración	Forma de medición: Conteo del numero de cambios no autorizados en la configuración no detectados a tiempo
Descripción de subcategoría: Seguridad de los dispositivos móviles se encuentra monitoreada	
Valor de referencia permitido: 4 cambios (No se debe permitir más de 4)	
Frecuencia de medición: trimestral	

2) Subcategoría: Monitoreo del cumplimiento de las políticas y procedimientos

Nombre: # de incumplimientos a las políticas o procedimientos no detectadas a tiempo	
Propósito: Comprobar si los procedimientos de monitoreo se están haciendo de manera correcta	Forma de medición: Conteo de número de incumplimientos a las políticas o procedimientos no detectadas a tiempo
Descripción de subcategoría: El cumplimiento de las políticas y procedimientos de seguridad para dispositivos móviles se encuentra monitoreada	
Valor de referencia permitido: 10 incumplimientos (No se debe permitir más de 10)	
Frecuencia de medición: mensual	

Categoría: Planificación de Respuesta

1) Subcategoría: Respuesta a incidentes

Nombre: # de retrasos en la respuesta a incidentes	
Propósito: Comprobar si se están respondiendo con la rapidez necesaria	Forma de medición: Conteo de número de retrasos en la respuesta a incidentes
Descripción de subcategoría: El procedimiento de respuesta incidentes esta implementado	
Valor de referencia permitido: 10 retrasos (No se debe permitir más de 10)	
Frecuencia de medición: mensual	

Nombre: # de incidentes no controlados adecuadamente	
Propósito: Comprobar si se están respondiendo correctamente a los incidentes	Forma de medición: Conteo de número de incidentes no controlados adecuadamente
Descripción de subcategoría: El procedimiento de respuesta incidentes esta implementado	
Valor de referencia permitido: 5 incidentes (No se debe permitir más de 5)	
Frecuencia de medición: mensual	

Categoría: Comunicación

1) Subcategoría: Mesa de Ayuda

Nombre: # de veces que se reportan ocupada la mesa de ayuda	
Propósito: Comprobar si la mesa de ayuda funciona adecuadamente	Forma de medición: Conteo de número de veces que se reporta ocupada la mesa de

	ayuda
Descripción de subcategoría: Mesa de ayuda para el reporte de incidentes esta implementada	
Valor de referencia permitido: 10 veces (No se debe permitir más de 10)	
Frecuencia de medición: mensual	

2) Subcategoría: Planificación de comunicación

Nombre: # de filtraciones de información durante la comunicación de la ocurrencia de un incidente	
Propósito: Comprobar si el plan de comunicación está funcionando correctamente	Forma de medición: Conteo del número de filtraciones de información durante la comunicación de la ocurrencia de incidentes
Descripción de subcategoría: Plan de comunicación esta implementado	
Valor de referencia permitido: 2 filtraciones (No se debe permitir más de 10)	
Frecuencia de medición: semestral	

Categoría: Planificación de Recuperación

1) Subcategoría: Recuperación de incidentes

Nombre: # de fallas en la recuperación	
Propósito: Comprobar si se están recuperando de los incidentes correctamente	Forma de medición: Conteo de número de fallas ocurridas en la recuperación
Descripción de subcategoría: El procedimiento de recuperación de incidentes esta implementado	

Valor de referencia permitido: 5 fallas (No se debe permitir más de 5)
Frecuencia de medición: mensual

Nombre: # de recuperaciones retrasadas	
Propósito: Comprobar si se están recuperando de los incidentes correctamente	Forma de medición: Conteo de número de recuperaciones retrasadas
Descripción de subcategoría: El procedimiento de recuperación de incidentes esta implementado	
Valor de referencia permitido: 10 recuperaciones retrasadas (No se debe permitir más de 10)	
Frecuencia de medición: mensual	

Categoría: Mejora

1) Subcategoría: Gestión del Conocimiento

Nombre: % de lecciones aprendidas implementadas	
Propósito: Comprobar si se aprendiendo de incidentes pasados	Forma de medición: Numero de lecciones aprendidas implementadas/Total de lecciones aprendidas identificadas
Descripción de subcategoría: Lecciones aprendidas de los incidentes están implementadas	
Valor de referencia permitido: 50% (Deben implementar al menos 50% de las lecciones aprendidas)	
Frecuencia de medición: trimestral	

2) Subcategoría: Evaluación y Auditoría

Nombre: # de auditorías realizadas al modelo	
Propósito: Comprobar si se están realizando auditorias para comprobar el funcionamiento del modelo [*]	Forma de medición: Conteo de número de auditorías realizadas
Descripción de subcategoría: Categorías se encuentren auditadas periódicamente	
Valor de referencia permitido: 4 auditorias (Deben haber al menos 4 auditorías al año)	
Frecuencia de medición: anual	

[*] Son auditorías al modelo implementado a una organización con el fin de detectar y proponer mejoras

3) Subcategoría: Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas

Nombre: % de innovaciones para la seguridad de los dispositivos móviles implementadas	
Propósito: Comprobar si se están manteniendo al día con las innovaciones de seguridad	Forma de medición: Porcentaje de innovaciones implementadas/total de innovaciones identificadas
Descripción de subcategoría: Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas	
Valor de referencia permitido: 30% (Deben implementar al menos 30% de las innovaciones de seguridad identificadas	
Frecuencia de medición: anual	

Capítulo 10. Guía de Implementación del modelo (O4)

Esta guía estará compuesta de varias partes: primero esta una estructura de gobierno sugerida para implementar el modelo la cual se encontrara en el anexo, Luego contara con una lista de amenazas de ciberseguridad que ayudara a identificar a que amenazas se encuentra expuesta la organización al usar los dispositivos móviles, Luego se contara con un procedimiento de autoevaluación que se hará por medio de una lista de verificación que se encontrara como un anexo (Anexo 1) en el cual se marcara que subcategorías cuyos controles ya están implementados, falta implementar o requieren mejoras, Luego en función de las categorías ya implementadas se permitirá determinar el estado actual de la seguridad de la organización y por ultimo para aquellas categorías que falten implementar o que requieran mejoras se presentara las actividades requeridas para la implementación de los controles para cada subcategoría. Estas actividades estarán ordenadas de forma descendente según las prioridades previamente asignadas a cada subcategoría y categoría.

Los pasos para implementar el modelo primero serán los siguientes:

1. Primero se comprobara si se cuenta con la estructura de gobierno adecuada para implementar el modelo. Las estructuras de gobierno sugeridas se encuentran en el anexo 1, Si se cuenta con las estructuras se pasa al siguiente paso
2. Segundo se ayudaran a identificar las amenazas de ciberseguridad que están expuestas los dispositivos móviles de la organización por medio de una lista de amenazas de ciberseguridad de los dispositivos móviles que se encuentra más adelante en la guía
3. Tercero se hará un autoevaluación para identificar que subcategorías ya se encuentra implementado y si dicha implementación si existiese necesita o no mejoras. Para esto se cuenta con un lista de verificación en el anexo 2 el cual se usara para que subcategorías ya cuenta con controles implementados y en función del valor de referencia asociado a los indicadores de la subcategoría determinar si estos controles son los adecuados o no. Para aquellas subcategorías que faltasen se usaran los controles sugeridos más adelante para la subcategoría que considere necesario

4. Cuarto en función de grupo de categorías que ya se han implementado, más adelante en el modelo se propondrá una serie de niveles para medir el estado actual de la protección que se tiene y se pueda ver las categorías que faltan para pasar de un nivel a otro
5. Por último, se implementaran los controles que falten según el nivel de seguridad que se busca alcanzar, Los controles sugerido del modelo se encuentran al final de la guía

1. Identificación de estructura de gobierno

Se deberá identificar la idoneidad de contar con una estructura de gobierno que cubra los siguientes objetivos y funciones en la organización. Ver anexo 1.

2. Identificación de amenazas de ciberseguridad

Identificar las amenazas de ciberseguridad que están expuestas los dispositivos móviles de la organización por medio de una lista de amenazas de ciberseguridad de los dispositivos móviles. Se presenta a continuación, el catálogo de amenazas de ciberseguridad de dispositivos móviles:

Catálogo de Amenazas de ciberseguridad de dispositivos móviles

El catálogo de amenazas tendrá un número asignado a cada una, la descripción o nombre de la misma y una categoría o característica. Este catálogo de amenazas se elaborara a partir del análisis de las amenazas de los dispositivos móviles obtenidos del catálogo amenazas de NIST (NIST, 2016). Este análisis se hizo para determinar cuáles amenazas del catálogo son amenazas de ciberseguridad y cuáles están con algunas de las características definidas como criterios para la selección de su ingreso al catálogo.

Las características o categorías de las amenazas que se revisaron en el catálogo de NIST son aquellas amenazas relacionadas al uso y presencia de aplicaciones en dispositivos móviles. La segunda característica está relacionada a la autenticación o manejo de credenciales de acceso y las últimas son las amenazas relacionadas a conexión y uso de las redes como Wifi o bluetooth, también aquí se incluirá la conexión directa de este dispositivo con otros equipos, la misma que se llamara conectividad. Los nombres de las características o categorías que aparecen en el catálogo son aplicación, conectividad y autenticación.

Las amenazas que se presentan a continuación son tomadas del (NIST, 2016):

Tabla 9 - Amenazas de Ciberseguridad de dispositivos móviles. Basado de (NIST, 2016)

Numero de Amenaza	Nombre o Descripción de Amenaza	Categoría
1	Filtración de información transmitida por los dispositivos móviles a través redes Wi-fi	Conectividad
2	Filtración de información o robo de credenciales por conexión de los dispositivos móviles a redes Wi-fi maliciosas enmascaradas como redes de Wi-fi legitimas	Conectividad
3	Filtración de información transmitida por los dispositivos móviles a través paquetes NFC (tecnología de comunicación inalámbrica de corto alcance)	Conectividad
4	Instalación de malware o virus en los dispositivos móviles por la lectura etiquetas NFC maliciosas o códigos QR maliciosos	Conectividad
5	Filtración de información privada o envió de spam a los dispositivos móviles que tengan activados el bluetooth (Tecnología inalámbrica de transmisión de voz y datos) de los dispositivos	Conectividad
6	Instalación de aplicaciones potencialmente maliciosas como malware sin conocimiento del usuario por conexión USB a una PC infectada	Conectividad
7	Instalación de actualizaciones maliciosas que pueden afectar la confidencialidad y disponibilidad de la información por fallar en la verificación de la identidad de las actualizaciones de las aplicaciones del dispositivo móvil	Autenticación
8	Robo de credenciales por medio instalación de aplicaciones falsas	Autenticación
9	Robo de credenciales por acceder a páginas web falsas a	Autenticación

Numero de Amenaza	Nombre o Descripción de Amenaza	Categoría
	través de un dispositivo móvil	
10	Robo de credenciales por medio de acceso a correos que redirigen a aplicaciones o páginas web maliciosas	Autenticación
11	Filtración de información confidencial o instalación de malware al ingresar a una página web y hacer clic en un botón falso que aparenta una acción especifica	Aplicación
12	Filtración de información o instalación de malware por el uso de aplicaciones con vulnerabilidades	Aplicación
13	Perdida de disponibilidad e integridad de la información por el encriptamiento de la misma debido a la instalación de malware (Ransomware)	Aplicación
14	Filtración de información por uso de aplicaciones con fallas (Escriben información sensible de manera accidental en los logs del sistema, almacenan archivos con permisos inseguros o en una localización desprotegida en el dispositivo)	Aplicación
15	Filtración de información por uso de Aplicaciones que han sido removidas de la tienda de aplicaciones por vulnerabilidades o fallas de seguridad	Aplicación
16	Robo de información de los usuarios por medio de aplicaciones maliciosas	Aplicación
17	Instalación de aplicaciones falsas o maliciosas a través del cambio de links asociada a las aplicaciones originales	Aplicación
18	Instalación de aplicaciones falsas o maliciosas a través del cambio de links asociada a las aplicaciones originales	Aplicación
19	Filtración de información como ubicación, audio o mensajes	Aplicación

Numero de Amenaza	Nombre o Descripción de Amenaza	Categoría
	de texto a través de aplicaciones maliciosas	
20	Perdida de disponibilidad de la información por instalación de aplicaciones que proveen control remoto de los dispositivos móviles	Aplicación
21	Perdida de confidencialidad e integridad de la información por la instalación de aplicaciones alteradas que contienen funciones maliciosas	Aplicación

3. Identificación de la aplicabilidad del modelo y autoevaluación inicial

Se recomienda efectuar una autoevaluación para identificar que subcategorías ya se encuentra implementado y si dicha implementación si existiese necesita o no mejoras.

Para este fin, emplear la lista de verificación del anexo 2

4. Niveles de seguridad del modelo y definición de hacia dónde quieres llegar

Los niveles de seguridad son 4: Informado, Protegido, Monitoreado y Adaptativo.

Para poder alcanzar adecuadamente cada uno de estos niveles se requiere que se implemente las categorías asociadas a cada uno de dichos niveles. Además, los niveles de seguridad son acumulativos, es decir, para alcanzar un nivel adaptativo primero se debe haber alcanzado un nivel informado, protegido y monitoreado. Para implementar una categoría se tiene que implementar adecuadamente controles para las subcategorías asociadas a dicha categoría.

Inicial

- No cuenta con ninguna categoría implementada

Informado: Significa que la organización es consiente y está capacitada sobre los riesgos y vulnerabilidades a las que se encuentra expuesta

- Gobierno de ciberseguridad
- Gestión de Activos
- Gestión de riesgo de TI
- Concientización y formación

Protegido: Significa que la organización ya cuenta con medidas protección implementadas

- Control de acceso
- Procesos y procedimientos para la protección de la información
- Seguridad de los datos
- Tecnología de protección

Monitoreado: Significa que la organización está preparada en caso de que fallara las medidas de protección implementadas

- Monitoreo continuo de la seguridad
- Anomalías y Eventos
- Planificación de Respuesta
- Comunicación
- Planificación de Recuperación

Adaptativo: Significa que la seguridad de la organización está actualizándose y mejorando de manera constante

- Mejora

5. Actividades Recomendadas para implementar las categorías del modelo en base al estado deseado

Gobierno de ciberseguridad

a) Políticas de ciberseguridad para dispositivos móviles

- Definir una política de seguridad de la información para dispositivos móviles en la que especifique a que información se puede acceder por medio de los dispositivos móviles según el tipo de sistema operativo de este o su versión de dicho sistema. (Souppaya & Scarfone, 2013) Además también deben contener todos los requerimientos para la administración de dispositivos móviles (Souppaya & Scarfone, 2013), para la seguridad de las aplicaciones (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015) y para el uso de bluetooth (Padgette, y otros, 2016). Es recomendable que estas políticas sean revisadas tanto por las autoridades legales, de privacidad y recursos humanos de la organización. (Kissel, Regenscheid, Scholl, & Stine, 2014).
- La política de seguridad de la información para dispositivos móviles debe incluir también criterios para la gestión de contraseñas donde se especifiquen los requerimientos para almacenar, transmitir y composición de las contraseñas. Además se deben incluir los requisitos para reiniciar una contraseña o la duración de una contraseña antes de que se necesite renovar por una nueva. (Scarfone & Souppaya, 2009)
- La política de seguridad de la información para dispositivos móviles debe incluir también la forma de priorizar incidentes, los roles y responsabilidades, el alcance de las políticas, sus objetivos y las medidas para evaluar su rendimiento. (Karen, Tom, Grance, & Paul, 2012)
- Esta políticas deben ser formalizadas, difundidas e implementadas

Gestión de Activos

a) Roles y Responsabilidades

- Definir y comunicar los roles (Quien se va encargar de las capacitaciones, de la auditoria, del análisis de riesgos, de hacer y actualizar los inventarios, del aseguramiento de los dispositivos móviles, del monitoreo de la

seguridad y procedimientos) y responsabilidades que tienen a los usuarios de los dispositivos móviles (ISO, 2012)

b) Control de Activos

- Realizar el inventario de los dispositivos móviles (Id, Nombre, descripción, sistema operativo, versión del sistema operativo, marca, tiene bluetooth, tiene NFC), las aplicaciones usadas en estos dispositivos (id, nombre, descripción, versión, permisos requeridos) y sus usuarios (Id, nombre, apellidos, teléfono, dispositivo asignado) (Souppaya & Scarfone, 2013)
- Clasificar y categorizar la información que se manejara por medio de los dispositivos móviles, los dispositivos en sí y las aplicaciones según el tipo de dispositivos , la confidencialidad de la información que se maneje y el software del dispositivo (ISO, 2012)
- Implementar tecnologías para administrar la seguridad de los dispositivos móviles de manera centralizada. (Se puede adquirir un software que permita administrar de manera centralizada los dispositivos móviles, permitiendo tanto la limpieza, bloqueo y desbloqueo remoto de un dispositivo móvil) (Souppaya & Scarfone, 2013)
- Desarrollar un proceso para reiniciar y dar acceso de manera remota a un dispositivo móvil, (Souppaya & Scarfone, 2013) que además permita verificar adecuadamente la identidad de quien quiere solicitar el reinicio de su contraseña (Scarfone & Souppaya, 2009)
- Desarrollar un proceso para bloquear de manera remota los dispositivos móviles (Souppaya & Scarfone, 2013)
- Configurar dispositivos que usen Bluetooth con el modo de seguridad de Bluetooth más fuerte con el que disponen (Padgette, y otros, 2016)
- Configurar permisos de las aplicaciones de los dispositivos móviles que se entregan a los usuarios (Souppaya & Scarfone, 2013)
- Establecer controles de seguridad en función de la políticas establecidas (Scarfone & Souppaya, 2009)
- Configurar los dispositivos móviles para que limiten el número de intentos o el tiempo de espera entre intentos permitido para desbloquear un dispositivo móvil (Scarfone & Souppaya, 2009)

- Establecer controles de seguridad suplementarios como antivirus y tecnologías para la prevención de perdida de datos (Souppaya & Scarfone, 2013)

Gestión de riesgo de TI

a) Riesgos de TI

- Realizar un inventario de las vulnerabilidades de los dispositivos móviles (Id, descripción de la vulnerabilidad, dispositivo asociado) y las aplicaciones (Id, descripción de la vulnerabilidad, aplicación asociada) (ISO, 2012)
- Realizar un inventario de las amenazas de seguridad de los dispositivos móviles y las aplicaciones usadas (Id, descripción de la amenaza, vulnerabilidad a explotar) (Souppaya & Scarfone, 2013)
- Evaluar los riesgos de los dispositivos móviles, las aplicaciones usadas y sus actualizaciones a instalar (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015) en función de la frecuencia e impacto de la materialización de ellos sean estos de terceros o de la misma organización (ISO, 2012)
- Establecer controles que permitan mitigar los riesgos y garanticen el cumplimiento de los requerimientos de seguridad definidos en las políticas para los dispositivos móviles y las aplicaciones usadas (ISO, 2012), Además de listas negras determinar qué tipos de dispositivos móvil, aplicaciones o contenidos no pueden usarse o acceder por medio de los dispositivos móviles
- Coordinar y establecer acuerdos y procedimientos con proveedores y suministradores de dispositivos móviles o servicios consumidos por estos que permitan garantizar los requisitos de seguridad definidas en las políticas para los dispositivos móviles y aplicaciones usadas. (NIST, 2018)

Concientización y formación

a) Concientización

- Realizar campañas de concientización sobre las políticas de seguridad que se usan (Karen, Tom, Grance, & Paul, 2012), sobre las responsabilidades de seguridad al momento de usar los dispositivos móviles por parte de los usuarios (Padgette, y otros, 2016) y sobre las amenazas a los dispositivos móviles y el comportamiento de las mismas (Souppaya & Scarfone, 2013)

b) Capacitación

- Realizar campañas de capacitación sobre las políticas de seguridad que se usan, sobre la forma que se sigue para detectar, reportar, responder y recuperarse de los incidentes (Karen, Tom, Grance, & Paul, 2012) y sobre las acciones recomendadas para controlar los ataques cibernéticos o escenarios de riesgo (Souppaya & Scarfone, 2013)
- Evaluar el resultado de las capacitaciones para comprobar si esta tuvo éxito (ISO, 2012)

Seguridad de los datos

a) Protección de la información

- Encriptar los datos almacenados en los dispositivos móviles y los datos transmitidos por estos (Souppaya & Scarfone, 2013)
- Restringir el acceso a los archivos o carpetas que contengan las contraseñas para acceder información de la organización o información confidencial (Scarfone & Souppaya, 2009)
- Encriptar la comunicación de los dispositivos móviles con la organización con protocolos de comunicación que permitan proteger las contraseñas (Scarfone & Souppaya, 2009)

Control de acceso

a) Autenticación

- Establecer un proceso para firmar digitalmente un correo para asegurar la integridad del mismo y poder comprobar la identidad del que lo envía (Tracy, Jansen, Scarfone, & Butterfield, 2007)

- Establecer múltiples métodos de autenticación para poder acceder a la información por medio de dispositivos móviles (usar contraseñas para desbloquear el dispositivo, para acceder a aplicaciones, para acceder a información con mayor nivel de confidencialidad) (Souppaya & Scarfone, 2013)
- Configurar los dispositivos móviles para que se bloqueen de manera automática luego de un determinado tiempo de inactividad (Souppaya & Scarfone, 2013)

Tecnología de protección

a) Conectividad

- Identificar y segregar las interfaces de red para comunicaciones internas y externas (Scarfone & Souppaya, 2009) y restringir el acceso a la red según el tipo de usuario que quiera conectarse
- Deshabilitar todas las interfaces de red que no son necesarias para los dispositivos (Souppaya & Scarfone, 2013)
- Usar software de administración de redes para monitorear y gestionar las interfaces de red (Esto para detectar comportamiento anómalos y quienes están o quieren conectarse a las interfaces de red de la organización, permitiéndole además bloquear el acceso a la red según su comportamiento) (ISO, 2012)

Procesos y procedimientos para la protección de la información

a) Desarrollo y mantenimiento de aplicaciones

- Establecer un proceso para probar la seguridad de las aplicaciones (comprobar si cuenta con las medidas de protección adecuadas, revisión si cuenta con todas las medidas de protección y prueba por medio de una simulación de un ataque) (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015)
- Establecer un proceso para garantizar la identidad de las aplicaciones instaladas o por instalar por medio de la verificación de firmas digitales (Souppaya & Scarfone, 2013)

- Documentar los pasos a seguir al diseñar y desarrollar aplicaciones de tal forma que estas tengan los niveles de seguridad solicitados y que no permitan el filtrado de información (Souppaya & Scarfone, 2013)
- Tener documentado y actualizado un registro sobre el comportamiento de las aplicaciones, sus manuales de usuario (ISO, 2012)

b) Limpieza de información de los dispositivos móviles

- Establecer un proceso de saneamiento que permita sanear los dispositivos móviles según el tipo de dispositivo y la información contenida (definir si para un dispositivo basta con borrar la aplicación, requiere formatear todo el dispositivo, requiere el uso de un software especial para borrar dicha información o si se debe destruir por completo el dispositivo) (Kissel, Regenscheid, Scholl, & Stine, 2014)
- Establecer un proceso de verificación que permita comprobar el adecuado saneamiento de un dispositivo móvil (Se puede usar un software para recuperar datos borrados para comprobar la posibilidad de recuperación de los mismos) (Kissel, Regenscheid, Scholl, & Stine, 2014)

Monitoreo continuo de la seguridad

a) Monitoreo de anomalías y amenazas

- Definir intervalos de tiempo recomendados para detectar cambios en la configuración de los dispositivos o signos de la ocurrencia de un incidente
- Monitorear la aparición de actualizaciones y parches para las aplicaciones o los sistemas operativos de los dispositivos móviles, adquirirlos, probarlos y luego desplegarlos (Souppaya & Scarfone, 2013)
- Monitorear la presencia de anomalías en los dispositivos móviles por medio de la comprobación de cambios no autorizados en la configuración de los equipos (Souppaya & Scarfone, 2013)
- Monitorear la ocurrencia de incidentes de seguridad de los dispositivos móviles a través de software de detección de intrusos u otro software de monitoreo

- Llevar un registro de las anomalías detectadas en el comportamiento de las aplicaciones y los dispositivos móviles (Souppaya & Scarfone, 2013)

b) Monitoreo del cumplimiento de las políticas y procedimientos

- Definir intervalos de tiempo recomendados para detectar incumplimientos a las políticas o procedimientos de seguridad
- Actualizar activamente los inventario de los dispositivos móviles, sus aplicaciones y usuarios (Souppaya & Scarfone, 2013)
- Monitorear el cumplimiento de los procedimientos establecidos de respuesta, recuperación y comunicación de incidentes y reportar cuando una violación de las políticas ocurre (Souppaya & Scarfone, 2013)
- Realizar pruebas para comprobar el funcionamiento de los procedimientos, planes de seguridad y el nivel de capacitación y concientización de los usuarios (ISO, 2012)

Planificación de Respuesta

a) Respuesta a incidentes

- Definir una estrategia y hacer un plan de respuesta a incidentes (en el plan establecer los tiempos limite y objetivo para responder a los incidentes) (Karen, Tom, Grance, & Paul, 2012), una guía para resolver incidentes de vectores de ataques conocidos (Karen, Tom, Grance, & Paul, 2012) y una guía para priorizar los incidentes tomando como factores el impacto funcional del incidente, el impacto en la información del incidente y la posibilidad de recuperación del incidente (Karen, Tom, Grance, & Paul, 2012)
- Formar un equipo de respuesta a incidente tomando en cuenta factores como la disponibilidad 24/7 del equipo, el tipo de personal que lo conformara, la moral del equipo, el costo y la habilidad del equipo, además definir los servicios que ofrecerá el equipo de respuesta a incidentes (Karen, Tom, Grance, & Paul, 2012)
- Crear procedimientos que indiquen los pasos como responder incidentes, estos procedimientos se deben basar en las políticas y el plan de respuesta a incidentes (Karen, Tom, Grance, & Paul, 2012)

Comunicación

a) Mesa de Ayuda

- Implementar un mesa de ayuda para responder consultas y que permita comunicar adecuadamente la ocurrencia de incidentes (Esto puede ser por medio de teléfonos o chats) (ISO, 2012)

b) Planificación de comunicación

- Hacer un plan de comunicación tomando en cuenta la regulación vigente, el receptor y destinatario de la información y las formas de comunicación alternativas (Bartock, et al., 2016)
- Realizar simulacros de prueba del plan de comunicación para comprobar el correcto funcionamiento de plan (Bartock, et al., 2016)
- Desplegar avisos con resúmenes de las políticas esenciales y los cambios que se den en ellas para mantener informado a los usuarios (ISO, 2012)

Planificación de Recuperación

a) Recuperación de incidentes

- Definir una estrategia y elaborar un plan para la recuperación de los incidentes (en el plan establecer los tiempos limite y objetivo para recuperarse de los incidentes) (Bartock, et al., 2016)
- Elaborar una guía para priorizar la recuperación de incidentes
- Formar un equipo de recuperación de incidentes
- Crear procedimientos para la recuperación de incidentes basándose en el plan y políticas de recuperación de incidentes

Mejora

a) Innovación

- Participar en comunidades o foros de la industria relevantes para mantenerse al día con las mejores prácticas y últimas vulnerabilidades y por medio de la implementación de dichas prácticas o controles cubrir las nuevas vulnerabilidades que se detecten. (ISO, 2012)

b) Gestión del Conocimiento

- Realizar reuniones sobre las lecciones aprendidas donde se ven la efectividad de los procesos de respuesta a incidentes y las opciones de mejora de estos (Karen, Tom, Grance, & Paul, 2012)
- Usar la información de las reuniones de lecciones aprendidas para identificar y corregir las deficiencias y debilidades en las políticas, controles y procedimientos de respuesta, comunicación y recuperación de incidentes (Karen, Tom, Grance, & Paul, 2012)

c) Evaluación y Auditoría

- Realizar auditorías periódicamente y evaluar el funcionamiento de las categorías y subcategorías del modelo para determinar si se están cumpliendo o no con los valores de referencia permitidos
- Proponer mejoras en función de los resultados de las auditorias que permitan mejorar la seguridad de los dispositivos, los procedimientos de respuesta, comunicación y recuperación de incidentes y que permitan lograr el cumplimiento de las subcategorías

Capítulo 11. Conformidad de los Expertos (O5)

Para obtener la conformidad de los expertos y terminar de dar por validado el modelo se recurrirá al juicio experto. Por esta razón se realizarán las fases que conforman el juicio experto que son las siguientes:

Ilustración 13 - Fases del Juicio Experto. Tomada de (Benini, y otros, 2017)

La Fase de preparación: Aquí se definirán los objetivos que se quieren lograr a través de este proceso (Benini, y otros, 2017)

Los objetivos del juicio experto son los siguientes:

- Validar que la guía permita implementar el modelo desarrollado
- Validar que las métricas asignadas miden adecuadamente el cumplimiento de los objetivos de los controles (subcategorías)
- Validar la pertinencia de las subcategorías definidas

La Fase de reclutamiento de expertos: En esta fase es donde se seleccionan a los expertos que se encargaran del juicio experto (Benini, y otros, 2017)

Para la selección de los expertos se hará por medio de la disponibilidad de tiempo de los expertos y área de especialidad de los expertos que en este caso vendría a ser de

tecnologías de información. En función de estos criterios se contaran con 2 expertos que son los siguientes:

Expertos:

- Manuel Tupia
- Diana Lepage

La Fase de elicitación: En esta fase se establecerá y ejecutara el relevamiento de información de los expertos con respecto al objeto de estudio o validación (Benini, y otros, 2017)

El procedimiento para la elicitación para el juicio experto que se seguirá se hará a través del uso de cuestionario. Habrá 3 cuestionarios para cada uno de los objetivos y se harán preguntas en cada cuestionario que permitan alcanzar el logro de dichos objetivos. Las respuestas a cada pregunta se harán a través de escalas de 3 valores (Inadecuado, Poco Adecuado, Adecuado) que se marcaran para obtener su resultado. Estos cuestionarios se encontrarán en los anexos 3, 4 y 5.

La Fase de agregación: En esta fase se revisara la información extraída de la fase anterior y se sintetizara (Benini, y otros, 2017)

Esta fase consistirá en el análisis de las respuestas y observaciones tomadas de los cuestionarios respondidos de los expertos. En función de dicho análisis se elaborara un documento donde se especificara las acciones tomadas en función de los resultados de los valores tomados de los cuestionarios.

La Fase de Comunicación de descubrimientos: En esta fase se comunica los resultados finales del juicio experto (Benini, y otros, 2017)

Se entregara el documento a los expertos para que verifiquen el levantamiento de las observaciones planteadas por ellos.

La Fase de uso en la toma de decisiones: En esta fase se hará uso de los resultados del juicio experto para la toma de decisiones (Benini, y otros, 2017)

La fase de toma de decisiones se hará por parte de los expertos donde en caso ellos comprueben el levantamiento adecuado de las observaciones den por validado el modelo

El protocolo que se seguirá para ejecutar el juicio experto se encuentra en el anexo 4 y los resultados de las evaluaciones de los expertos se encuentran en el anexo 8.

Adicionalmente, en el anexo 9 se esta adjuntado el certificado de la participación del modelo en una conferencia internacional y los detalles de la conferencia. Esto sirve como un instrumento de validación adicional para probar la validez del modelo ya que para lograr la participación en estas conferencias se requiere pasar una evaluación hecha por varios expertos.

Capítulo 12. Conclusiones y trabajos futuros

Conclusiones

A partir del desarrollo del proyecto se concluye lo siguiente:

- Se concluye que el modelo reducirá significativamente los riesgos de ciberseguridad asociados a los dispositivos móviles puesto que varias fuentes usadas en la elaboración del mismo cuentan con una validez comprobada como son la ISO 27032 y los estándares de NIST. Además este modelo permitirá facilitar la implementación del mismo al agrupar de un modo más ordenado los objetivos de los controles y los controles al usar la estructura de los componentes del marco de ciberseguridad de NIST
- Se concluye que en el componente de procesos del modelo que abarca tanto las categorías, subcategorías y niveles de prioridad se encontrara la información clave del modelo ya que en este componente estarán todos los temas que abarcara el modelo. Además también se concluye que dentro de las categorías es necesario una categoría de mejora que abarque temas como las lecciones aprendidas de los incidentes, seguimiento continuo de los desarrollos tecnológicos y procedimientos de auditoría. Esto con la finalidad de que el modelo propuesto se mantenga vigente en el tiempo
- Se concluye que en caso de que se requieran definir indicadores que manejen los incidentes de formas distintas es necesario previamente tener implementado la gestión de incidentes dentro de la organización como una precondición antes de implementar el modelo
- Se concluye que el componente que corresponde a los indicadores del modelo es necesario ya que este permite comprobar el correcto funcionamiento del modelo. Por esta razón para cada una de las subcategorías de este modelo, que vendrían a ser los objetivos de control, se requiere que se cuente con al menos un indicador para poder medir su funcionamiento
- Se concluye que el modelo se podrá aplicar a empresas tanto públicas o privadas mientras que estas cuenten con alguna de las estructuras de gobierno sugeridas y que cuenten con los fondos necesarios para la implementación del modelo. En caso de empresas pequeñas mientras que cuenten con los fondos

necesarios para la implementación de las subcategorías que necesiten para alcanzar el nivel de protección deseado pueden aplicar el modelo

- Se concluye que es necesario que los empleados y la alta dirección sean conscientes de la importancia de la implementación del modelo. En el caso de los empleados, porque la falta de disposición de los mismos puede retrasar la implementación del modelo o incluso ser un riesgo en si para el modelo. En el caso de la alta dirección, porque se necesita que ellos dicten nuevas políticas relacionadas a temas de ciberseguridad y brinden los fondos necesarios para implementar los controles requeridos ya que sin estos resulta imposible implementar el modelo.
- Se concluye que para implementar un modelo no solo basta con incluir las actividades recomendadas para implementar el modelo sino también se necesita un procedimiento de autoevaluación que permita identificar si parte del modelo se encuentra ya implementado o no y poder apoyarme a la hora de indicarme hacia donde quiero ir. Para que luego con esto claro se pueda decidir qué actividades necesito implementar. Además también se concluye que se requerirá el apoyo de auditorías externas e internas para evaluar si los procedimientos implementados son los adecuados o no
- Se concluye que el juicio experto es un procedimiento que para llevarse a cabo se necesita seguir una serie de pasos pero al completarlo permite dar por valido a aquello que se está evaluando que en este caso vendría a ser el modelo. Además, se concluye que para poder validar un modelo de manera adecuada no solo se necesita poder validar que se puede implementar el modelo en sí, sino que también se necesita que el contenido de los objetivos de los controles (subcategorías) y los indicadores sean los adecuados

Trabajos futuros

- Participar y validar el modelo a través de su participación en una conferencia internacional
- Implementar el modelo en una organización y validar el correcto funcionamiento del mismo en un ambiente real
- Desarrollar un software que permita monitorear el modelo para poder determinar si los valores establecidos para los indicadores se están cumpliendo o no
- Desarrollar un software que permita automatizar el procedimiento de autoevaluación

Referencias

Ley N° 29733, Ley de Proteccion de Datos Personales. (3 de Julio de 2011). *El Peruano*. Obtenido de http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf

News. (2015). *Computer*, 14-20.

Agesic. (1 de Septiembre de 2016). *Agesic*. Obtenido de Agesic: http://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad.html

Angelini, M., Lenti, S., & Santucci, G. (2017). CRUMBS: a Cyber Security Framework Browser. *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)* (págs. 1-8). Phoenix, AZ, USA : IEEE.

Baldoni, R., & Montanari, L. (2016, Febrero). *Framework Nazionale per la Cyber Security.* Retrieved from Framework Nazionale per la Cyber Security: www.cybersecurityframework.it/

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for Cybersecurity Event Recovery.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 51-61.

Benini, A., Chataigner, P., Noumri, N., Parham, N., Sweeney, J., & Tax, L. (Agosto de 2017). Recuperado el 28 de Septiembre de 2017, de ACAPS: https://www.acaps.org/sites/acaps/files/resources/files/acaps_expert_judgment_-_full_study_august_2017.pdf

Berghel, H. (2015). Cyber Chutzpah: The Sony Hack and the Celebration of Hyperbole. *Computer*, 77 - 80.

Brown, C., Dog, S., Franklin, J. M., McNab, N., Voss-Northrop, S., Peck, M., & Stidham, B. (2016). *Assessing Threats to Mobile Devices & Infrastructure.* Gaithersburg: NIST (National Institute of Standards and Technology).

Bruderer, R., Villena, M., Tupia, M., & Bruzza, M. (2018). A CYBERSECURITY MODEL FOR MOBILE DEVICES AIMED AT SMES THAT USE FREELANCERS AND BYOD SCHEMES., (págs. 129-136). Lisboa.

Bruzza, M. M., & Tupia, M. A. (2016). A systematic review based on Kitchengam's criteria about use of specific models to implement egovernment solutions. *eDemocracy & eGovernment (ICEDEG), 2016 Third International Conference on* (págs. 75-80). Sangolqui, Ecuador: Pontificia Universidad Católica del Perú. doi:https://doi.org/10.1109/ICEDEG.2016.7461700

Caine, D. J., & Robson, A. J. (1993). Spreadsheet Modelling: Guidelines for Model Development. *Management Decision*, 17-23.

Chen, L., Franklin, J., & Regenscheid, A. (2012). *Guidelines on Hardware-Rooted Security in Mobile Devices.*

Choras, M., Kozik, R., Renk, R., & Holubowicz, W. (2015). A Practical Framework and Guidelines to Enhance Cyber Security and Privacy. *Advances in Intelligent Systems and Computing, 369*, 485-495.

Comite-de-normalizacion-de-codificacion-e-intercambio-electronico-de-datos. (2014). *NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.* (2 ed.). Lima: INDECOPI.

Esterbrook, J. (7 de Abril de 2002). *CBSNews*. Obtenido de CBSNews: http://www.cbsnews.com/news/many-hack-attacks-go-unreported/

Garnaeva, M., Wiel, J. v., Makrushin, D., Ivanov, A., & Namestnikov, Y. (15 de Diciembre de 2015). *SECURELIST*. Obtenido de SECURELIST: https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

Hora, S. C. (209). *CREATE.* Obtenido de CREATE: http://create.usc.edu/sites/default/files/publications/expertjudgmentinriskanalysis_0.pdf

ISO. (2012). *ISO*. Obtenido de ISO: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375

ISO. (2012). *ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity.*

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

Karen, S., Tom, M., Grance, T., & Paul, C. (2012). *Computer Security Incident Handling Guide.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *Guidelines for Media Sanitization.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Mani, D., Choo, K.-K. R., & Mubarak, S. (2014). Information security in the South Australian real estate industry. *Information Management & Computer Security*, 24-41.

Morales, R. (23 de Octubre de 2006). *Isaca.* Obtenido de Isaca: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20061023%20Gobierno%20de%20Seguridad%20de%20Informaci%C3%B3n.pdf

Newhouse, B., Keith, S., Scribner, B., & Witte, G. (2 de Noviembre de 2016). *NIST.* Obtenido de Computer Security Division Computer Security Resource Center: http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf

NIST. (2016, Noviembre 10). *Mobile Threat Catalogue*. Retrieved from Mobile Threat Catalogue: https://pages.nist.gov/mobile-threat-catalogue/application.html#page

NIST. (16 de Abril de 2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Obtenido de Framework for Improving Critical Infrastructure Cybersecurity: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NowSecure. (2016). *NowSecure.* Obtenido de NowSecure: https://info.nowsecure.com/rs/201-XEW-873/images/2016-NowSecure-mobile-security-report.pdf

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2016). *Guide to Bluetooth Security.* Obtenido de http://csrc.nist.gov/publications/drafts/800-121/sp800_121_r2_draft.pdf

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). 'Cyberoperations and international humanitarian law', Information and Computer Security. *Information and Computer Security*, 38 - 52.

Quirolgico, S., Voas, J., Karygiannis, T., Michael, C., & Scarfone, K. (2015). *Vetting the Security of Mobile Applications.*

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cybersecurity. En A. Refsdal, B. Solhaug, & K. Stølen, *Cyber-Risk Management* (págs. 29-32). Oslo, Norway: Springer International Publishing.

Scarfone, K., & Souppaya, M. (2009). *Guide to Enterprise Password Management (Draft).* Obtenido de http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Souppaya, M., & Scarfone, K. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (2007). *Guidelines on Electronic Mail Security.* Obtenido de http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

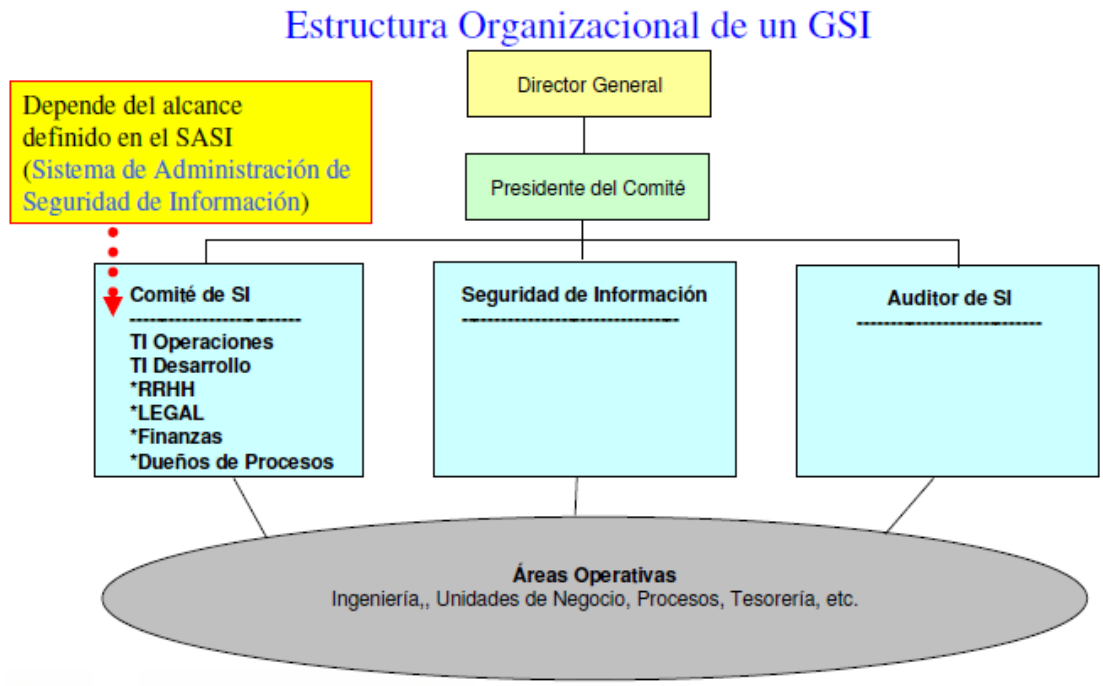
Whyte, C. (2016). Ending cyber coercion: Computer network attack, exploitation and the case of north korea. *Comparative Strategy*, 93-102.

Anexos

Anexo 1 – Estructuras de Gobierno Sugeridas

Aquí se sugerirán dos (2) estructuras de gobierno que se deberían tener para implementar el modelo:

La primera es contar con una estructura de gobierno de seguridad de la información y dentro de esta asignar los roles y responsables a realizar las operaciones del modelo. Esto quiere decir que los aspectos relacionados al gobierno de ciberseguridad estarán dentro del gobierno de seguridad de la información.



Estructura organizacional de un GSI. Tomada de (Morales, 2006)

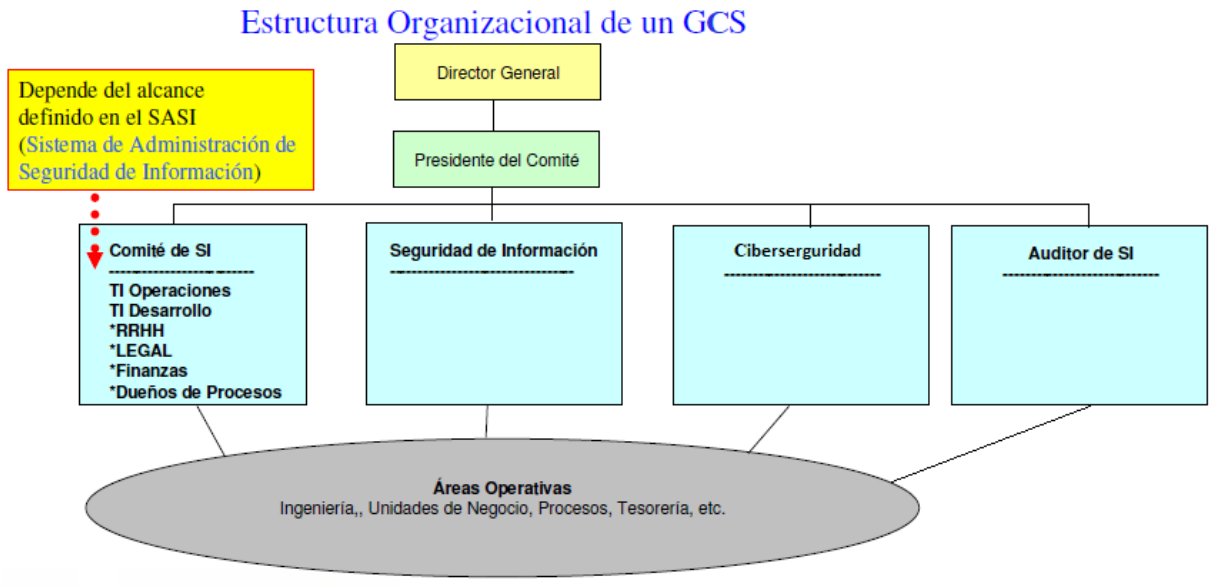
Comité de SI: Se encarga de tomar decisiones tomando en cuenta las áreas críticas de la empresa. Es decir se encargan de aprobar los procedimientos y controles. (Morales, 2006)

Área de Seguridad de la información: Se encarga de elaborar las políticas de seguridad de la información, la metodología de tratamiento de riesgos, elaborar los planes de tratamiento de riesgos, elaborar los procedimientos y controles y las acciones preventivas y correctivas. Tanto en las políticas, planes de tratamiento de riesgos como en los procedimientos y controles se incluyen los temas relacionados a ciberseguridad. (Morales, 2006)

Auditoría de SI: Elaborar los procedimientos de auditoría y revisar los procedimientos, controles, acciones correctivas y preventivas tomadas. Esta auditoría se refiere a auditoría interna de la propia organización. (Morales, 2006)

Se sugiere además de la auditoría interna realizar una auditoría externa para contar con un medio de validación adicional, ya que puede que la auditoría interna no haya tenido el debido rigor y se necesita una externa para validar mejor los procedimientos.

Otra posibilidad es tener un gobierno de seguridad de la información y tener gobierno de ciberseguridad. Es decir en las políticas de seguridad de la información ya no debería incluirse temas de ciberseguridad ya que estas estarían incluidas en el gobierno de ciberseguridad.



Estructura Organizacional de un Gobierno de Ciberseguridad y seguridad de la información. Tomada de (Morales, 2006) y Editada.

Comité de SI: Se encarga de tomar decisiones tomando en cuenta las áreas críticas de la empresa. Es decir se encargan de aprobar los procedimientos y controles. (Morales, 2006)

Área de Seguridad de la información: Se encarga de elaborar las políticas de seguridad de la información, la metodología de tratamiento de riesgos, elaborar los planes de tratamiento de riesgos, elaborar los procedimientos, controles y las acciones preventivas y correctivas. (Morales, 2006) Aquí ya no se incluye lo relacionado a temas de ciberseguridad.

Ciberseguridad: Se encarga de elaborar las políticas de ciberseguridad, la metodología de tratamiento de riesgos, elaborar los planes de tratamiento de riesgos, elaborar los procedimientos, controles y las acciones preventivas y correctivas relacionadas a temas de ciberseguridad.

Auditoría de SI: Elaborar los procedimientos de auditoría y revisar los procedimientos, controles, acciones correctivas y preventivas tomadas. Esta auditoría se refiere a la propia de la organización. (Morales, 2006)

Se sugiere además de la auditoría interna realizar una auditoría externa para contar con un medio de validación adicional, ya que puede que haya existido el debido rigor y se necesita una externa para validar mejor los procedimientos.

Anexo 2 – Lista de verificación para autoevaluación

Observaciones:

Esta autoevaluación requiere previamente que se haya recopilado la información solicitada de los indicadores del modelo.

Los indicadores de cada subcategoría y su valor de referencia se encontraran debajo de cada subcategoría

Instrucciones:

- Comprobar si se cumplen con las precondiciones del modelo
- Marcar cada una de las subcategorías que se tienen implementadas
- Para aquellas subcategorías ya implementadas marcar si los valores recogidos sobre los indicadores están dentro los límites establecidos
- Para las subcategorías implementadas y que están en los límites definidos, se debe revisar el modelo e identificar en función de las subcategorías a las categorías implementadas
- Ir a la guía del implementación del modelo en la parte de niveles de seguridad del modelo y en función de las categorías implementadas identificadas de la parte anterior, identificar en qué nivel de seguridad se encuentra
- Definir el nivel de seguridad que se quiere alcanzar y seleccionar las categorías restantes requeridas para alcanzar ese nivel
- Implementar la lista de actividades de la guía asociadas a las categorías seleccionadas

Conclusión

El resultado de esta autoevaluación es identificar las categorías implementadas, el nivel de seguridad en el que se encuentra, el nivel que se quiere alcanzar, identificar las categorías que se necesitan implementar para alcanzar ese nivel e indicar las actividades necesarias para implementar dichas categorías

[*] Puede usar el macro adjunto para poder realizar la autoevaluación y determinar el nivel de seguridad en el que se encuentra

Subcategoría	
1. Categoría: Gestión de Activos	
Subcategoría: Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas	☐
Indicador: # de roles no asignados	
# de roles no asignados igual a 0	☐

Subcategoría: Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados	☐
Indicador: # de aplicaciones y dispositivos desconocidos	
# de aplicaciones y dispositivos desconocidos menor o igual que 10	☐
Indicador: # de errores en la categorización y clasificación	
# de errores en la categorización y clasificación son menores 5	☐
2. Categoría: Gobierno de ciberseguridad	
Subcategoría: Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	☐
Estado de la política (aprobada, formalizada, difundida, implementada)	
Política ya se encuentra aprobada, formalizada, difundida e implementada	☐
Indicador: # de faltas detectadas a la política	☐
Las políticas no presentan errores	
Indicador: # de violaciones a las políticas	
# de violaciones a las políticas debe ser menor igual que 10	☐

3. Categoría: Gestión de riesgo de TI

Subcategoría: Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados

Indicador: # de incidentes materializados por riesgos aceptados

de incidentes materializados por riesgos aceptados deben ser menores que 8

Indicador: # de incidentes materializados por riesgos no identificados

de incidentes materializados por riesgos no identificados deben ser menores que 4

4. Categoría: Concientización y formación

Subcategoría: Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles

Indicador: # de errores en los procesos de respuesta, recuperación o comunicación de incidentes

de errores en los procesos de respuesta, recuperación o comunicación de incidentes debe ser menor de 15

Indicador: % de aprobados del total de capacitados

% de aprobados del total de capacitados debe ser mayor de 90

Subcategoría: Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones

Indicador: # de incidentes detectados pero no reportados

de incidentes detectados pero no reportados debe ser menor de 10

5. Categoría: Control de acceso

Subcategoría: Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos ☐

Indicador: # de accesos no autorizados

de accesos no autorizados debe ser menor de 2 ☐

6. Categoría: Seguridad de los datos

Subcategoría: Datos almacenados y transmitidos se encuentran protegidos ☐

Indicador: # de filtraciones de información

de filtraciones de información debe ser menor de 2 ☐

Indicador: # de alteraciones detectadas de datos de manera irregular

de alteraciones detectadas de datos de manera irregular debe ser menor de 2 ☐

7. Categoría: Tecnología de protección

Subcategoría: Interfaces de red se encuentran administradas ☐

Indicador: Estado de las interfaces de red (identificada, restringida, monitoreada, gestionada)

Estado de las interfaces de red se encuentran gestionadas (Todas las interfaces de red se encuentran gestionadas) ☐

Indicador: # de dispositivos no autorizados conectados a la red

de dispositivos no autorizados conectados a la red debe ser menor de 2 ☐

Subcategoría: Tecnologías para la administración centralizada de los dispositivos móviles esta implementada ☐

Indicador: # de bloqueos o limpieza remota de los dispositivos fallidas

de bloqueos o limpieza remota de los dispositivos fallidas debe ser menor de 2 ☐

Subcategoría: Dispositivo móviles entregados por la organización están completamente asegurados ☐

Indicador: Estado de dispositivos a entregados (identificados, configurados, protegidos)

Numero de dispositivos móviles no identificados debe ser menor que 3 ☐

Numero de dispositivos móviles no configurados debe ser menor que 5 ☐

Numero de dispositivos móviles no protegidos debe ser menor que 5 ☐

Indicador: # de fallas detectadas en la seguridad

de fallas detectadas en la seguridad debe ser menor de 8 ☐

8. **Categoría: Procesos y procedimientos para la protección de la información**

Subcategoría: Ciclo de vida de las aplicaciones y dispositivos móviles están administrados ☐

Indicador: # de dispositivos no asegurados correctamente

de dispositivos no asegurados correctamente debe ser menor de 2 ☐

9. **Categoría: Anomalías y Eventos**

Subcategoría: Comportamiento del código y anomalías esta administrado ☐

Indicador: # de documentos (manuales de usuarios de las aplicaciones) no actualizados

No debe haber documentos sin actualizar ☐

Indicador: # de anomalías repetidas registradas

de anomalías repetidas registradas debe ser menor de 10 ☐

10. Categoría: Monitoreo continuo de la seguridad

Subcategoría: Seguridad de los dispositivos móviles se encuentra monitoreada ☐

Indicador: # de cambios no autorizados en la configuración no detectados a tiempo

de cambios no autorizados en la configuración no detectados a tiempo debe ser menores a 4 ☐

Subcategoría: Políticas, procesos y procedimientos están monitoreados ☐

Indicador: # de incumplimientos a las políticas, procesos o procedimientos no detectadas a tiempo

de incumplimientos a las políticas, procesos o procedimientos no detectadas a tiempo debe ser menor de 10 ☐

11. Categoría: Planificación de Respuesta

Subcategoría: Plan de respuesta durante incidentes este implementado ☐

Indicador: # de retrasos en la respuesta a incidentes

de retrasos en la respuesta a incidentes debe ser menores de 10 ☐

Indicador: # de incidentes no controlados adecuadamente

de incidentes no controlados adecuadamente debe ser menores de 5 ☐

12. Categoría: Comunicación

Subcategoría: Canales de comunicación para soporte y avisos están habilitados ☐

Indicador: # de veces que se reportan ocupados los canales de comunicación

de veces que se reportan ocupados los canales de comunicación debe ser menores de 10 ☐

13. Categoría: Planificación de Recuperación

Subcategoría: Plan de recuperación después incidentes este implementado ☐

Indicador: # de fallas en la recuperación

de fallas en la recuperación no deben ser mayores a 5 ☐

Indicador: # de recuperaciones retrasadas

de recuperaciones retrasadas no deben ser mayores de 10 ☐

14. Categoría: Mejora

Subcategoría: Lecciones aprendidas de los incidentes están implementadas ☐

Indicador: % de lecciones aprendidas implementadas

% de lecciones aprendidas implementadas debe ser mayor de 50% ☐

Subcategoría: Categorías se encuentren auditadas periódicamente ☐

Indicador: # de auditorías realizadas al modelo

de auditorías realizadas debe ser de al menos 4 ☐

Subcategoría: Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados ☐

Indicador: % de mejoras implementadas

% de mejoras implementadas debe ser mayor de 30% ☐

Anexo 3 – Detalle de Procedimiento de Selección de Subcategorías y Categorías del modelo

En este anexo se presentara el detalle del procedimiento seguido para elaborar la lista de categorías y subcategorías del modelo, el cual estará compuesto de 3 secciones la primera será la presentación de las categorías del marco de NIST, el mapeo de aplicabilidad de subcategorías al modelo y el mapeo de subcategorías identificadas por categorías del marco de NIST.

Primera sección:

Aquí se presentaran todas las categorías del marco de NIST junto con los criterios para identificar si una subcategoría pertenece a dicha categoría.

Categorías del marco de NIST (NIST, 2018) **:**

Categorías	Criterios de Inclusión de subcategorías
Gobierno de ciberseguridad	Estructura, políticas y procedimientos asignados por la alta dirección para establecer buenas prácticas de seguridad sobre dispositivos móviles.
Ambiente del Negocio	La misión de la organización, sus objetivos, interesados y actividades son comprendidos y priorizados
Gestión de Activos	Los datos, dispositivos, aplicaciones y usuarios que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente
Gestión de riesgo de TI	Permite comprender los riesgos de ciberseguridad de los dispositivos móviles y aplicaciones y gestionar los riegos de TI
Estrategia para la gestión de riesgos de TI	Se establecen las prioridades, restricciones, tolerancia al riesgo y supuestos de la organización
Gestión de riesgo de la cadena de suministro	Las prioridades de la organización, las limitaciones, las tolerancias de riesgo se utilizan para apoyar las decisiones de riesgo relacionados con la gestión del riesgo en la

Categorías	Criterios de Inclusión de subcategorías
	cadena de suministro
Concientización y formación	El personal de la organización recibe entrenamiento y concientización sobre ciberseguridad de los dispositivos móviles y/o tecnologías relacionadas.
Seguridad de los datos	La información y datos son protegidos para garantizar la confidencialidad, integridad y disponibilidad de la información
Control de acceso	El acceso a información de la organización por medio de dispositivos móviles se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas
Procesos y procedimientos para la protección de la información	Las políticas de seguridad, procesos y procedimientos se mantienen y son utilizados para garantizar la protección de la información
Mantenimiento	El mantenimiento y las reparaciones de los componentes de los sistemas de información y de control industrial se lleva a cabo en consonancia con las políticas y procedimientos
Tecnología de protección	Las tecnologías para la seguridad se gestionan para garantizar la seguridad y resistencia de los dispositivos móviles y aplicaciones de la organización frente a eventos de seguridad cibernética, en consonancia con las políticas, procedimientos y acuerdos
Monitoreo continuo de la seguridad	Los dispositivos móviles y la seguridad de los mismos son monitoreados a intervalos discretos para identificar eventos de seguridad cibernética
Procesos de detección	Se mantienen procesos y procedimientos de detección y prueban para asegurar el conocimiento oportuno y

Categorías	Criterios de Inclusión de subcategorías
	adecuado de los eventos anómalos
Planificación de Respuesta	Los procesos y procedimientos de respuesta se ejecutan y se mantienen garantizando una respuesta oportuna para durante un evento de ciberseguridad
Análisis	Se efectúa análisis para asegurar una respuesta adecuada y dar soporte a las actividades de recuperación
Mitigación	Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente
Comunicación	Las actividades para coordinar la respuesta y recuperación de incidentes con las partes interesadas internas y externas
Planificación de Recuperación	Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad
Mejora	Las actividades de respuesta de la organización, los planes y procesos de recuperación, los planes de comunicación y los controles establecidos se mejoran incorporando las lecciones aprendidas y los nuevos desarrollos tecnológicos

Segunda Sección:

La segunda sección corresponde a la aplicabilidad de las subcategorías del modelo. Para la cual se han revisado las siguientes fuentes y se han determinado si aplica o no las subcategorías al modelo. Las fuentes son las siguientes:

- NIST SP 800-124 Rev 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise (Souppaya & Scarfone, 2013)
- NIST SP 800-164 : Guidelines on Hardware-Rooted Security in Mobile Devices (Chen, Franklin, & Regenscheid, 2012)

- NIST SP 800-163: Vetting the Security of Mobile Applications (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015)
- NIST SP 800-61 Rev 2 (Draft): Computer Security Incident Handling Guide (Karen, Tom, Grance, & Paul, 2012)
- NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery (Bartock, et al., 2016)
- NIST Special Publication 800-118: Guide to Enterprise Password Management (Draft) (Scarfone & Souppaya, 2009)
- NIST Special Publication 800-1212 Revision 2 (Draft): Guide to Bluetooth Security (Padgette, y otros, 2016)
- NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization (Kissel, Regenscheid, Scholl, & Stine, 2014)
- NIST Special Publication 800-45 Version 2: Guidelines on Electronic Mail Security (Tracy, Jansen, Scarfone, & Butterfield, 2007)
- ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity (ISO, 2012)
- NIST. (10 de Enero de 2017). *Framework for Improving Critical Infrastructure Cybersecurity.* (NIST, 2018)

Mapeo de aplicabilidad de subcategorías del modelo:

Subcategoría	Aplica?	Comentarios
las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas	Si	Aquí se incluirán lo que debe hacer cada empleado según su rol y sus responsabilidades en el manejo de dispositivos móviles
Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados	Si	Esta servirá para llevar un control sobre los dispositivos y aplicaciones que se están usando

Subcategoría	Aplica?	Comentarios
El rol de la organización en la cadena de suministro se encuentra identificado y comunicado	No	No guarda relación con la ciberseguridad de los dispositivos móviles
Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	Si	Aquí se incluyen todas las políticas relacionadas a dispositivos móviles
Política para la gestión de contraseñas establecida	No	En la política de seguridad la información de dispositivos móviles debe estar también las políticas para la gestión de contraseñas de los mismos
Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	Si	Permite conocer los riesgos de los dispositivos y aplicaciones
Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	Si	Permite saber al personal a reaccionar frente a incidentes de seguridad que involucren a los dispositivos móviles
Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	Si	Permite reducir comportamientos del personal que pueden exponer al riesgo los dispositivos
Usuarios conscientes de su responsabilidades en el uso de las tecnologías Bluetooth	No	Este se encuentra incluido dentro de la subcategoría de usuarios concientizados así que ya no se debería incluir
Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran	Si	Esto para limitar el acceso a la información dentro de los dispositivos

Subcategoría	Aplica?	Comentarios
establecidos		
Datos almacenados y transmitidos por los dispositivos móviles se encuentran protegidos	Si	Para garantizar la confidencialidad e integridad de los datos manejados y transmitidos por dispositivos móviles
Las redes a las que se conectan los dispositivos móviles se encuentran administradas	Si	Permite monitorear las conexiones no autorizadas a las redes de la organización a través de dispositivos móviles
Tecnologías para la administración centralizada de los dispositivos móviles esta implementada	No	Ya se encuentra en la parte de administración de dispositivos móviles
Medidas de limpieza remota de los datos para dispositivos móviles establecida	No	Esta está incluida dentro de las tecnologías para la administración centralizada ya que esta permite la limpieza o bloqueo remoto de dispositivos
Mecanismo de seguridad remoto establecidos	No	Está incluida dentro de las tecnologías para la administración centralizada ya que esta permite la limpieza o bloqueo remoto de dispositivos
Dispositivo móviles entregados por la organización están completamente asegurados	No	Ya se encuentra en la subcategoría anterior donde se menciona que los dispositivos se encuentran asegurados
Root of Trust implementados	No	Esta es una forma de configuración de los dispositivos móviles , lo cual estaría incluido dentro de dispositivos

Subcategoría	Aplica?	Comentarios
		móviles asegurados
El desarrollo y mantenimiento de aplicaciones esta administrado	Si	Aquí abarcara el desarrollo y mantenimiento de las aplicaciones, como la documentación del comportamiento de las mismas
La limpieza de información de los dispositivos móviles está administrada	Si	Aquí abarcara los procedimientos de adquisición si hubiese y limpieza o retiro de los dispositivos móviles
Comportamiento del código y anomalías esta administrado	No	Ya está incluido en el desarrollo y mantenimiento de aplicaciones
Seguridad de los dispositivos móviles se encuentra monitoreada	Si	Permite detectar la ocurrencia de incidentes de dispositivos móviles
El cumplimiento de las políticas y procedimientos de seguridad para dispositivos móviles se encuentra monitoreada	Si	Permite comprobar el cumplimiento de los planes y políticas establecidos de seguridad para dispositivos móviles
El procedimiento de respuesta incidentes esta implementado	Si	Permite contar con una serie de procedimientos sobre cómo actuar cuando ocurra un incidente asociado a dispositivos móviles
Plan de comunicación esta implementado	Si	Permite saber a quién comunicar durante la ocurrencia de distintos tipos de incidentes
Mesa de ayuda para el reporte de incidentes esta implementada	Si	Permite notificar la ocurrencia de un incidente o la ocurrencia de una

Subcategoría	Aplica?	Comentarios
		emergencia relacionada a dispositivos móviles
El procedimiento de recuperación de incidentes esta implementado	Si	Permite contar con una serie de procedimientos sobre cómo actuar para recuperarse luego de un incidente
Lecciones aprendidas de los incidentes están implementadas	Si	Permite mejorar los procesos del modelo permitiendo estar mejor preparado en caso de un incidente pueda repetirse de manera similar
Categorías se encuentren auditadas periódicamente	Si	Permite comprobar el cumplimiento de las categorías del modelo
Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas	Si	Permite al modelo mantenerse vigente ante el surgimiento de nuevas tecnologías que puedan presentar vulnerabilidades
Las nuevas vulnerabilidades identificadas se mitigan o documentan como riesgos aceptados	No	Esta subcategoría está incluida dentro de la subcategoría de riesgos tratados ya que para poder identificar los riesgos previamente se necesita identificar las vulnerabilidades
las notificaciones de los sistemas de detección esta investigados	No	Los procedimientos de detección están incluidos en la subcategoría de seguridad se encuentra monitoreada
Las actividades de detección cumplen con todos los requisitos aplicables	No	Esta subcategoría estaría incluida dentro de procedimientos y actividades se encuentran monitoreados

Subcategoría	Aplica?	Comentarios
Se controla la actividad de los proveedores de servicios externos para detectar posibles eventos de ciberseguridad	No	Esto formaría parte que la subcategoría de seguridad se encuentra monitoreada
Se detecta el código móvil no autorizado	No	Esto formaría parte que la subcategoría de seguridad se encuentra monitoreada
Se establecen los umbrales de alerta de incidentes	No	Esta se encuentra dentro de la subcategoría de los planes de respuesta que indica cuando responder a un incidente
Los medios extraíbles se encuentran protegidos y su uso se encuentra restringido de acuerdo con las políticas	No	Esta subcategoría forma parte de la subcategorías de políticas en las políticas debe estar los usos permitidos de los medios extraíbles y de la subcategoría de capacitación apoyar a entender porque se deben cumplir con estas restricciones
Los planes de respuesta y recuperación se testean regularmente	No	Esta subcategoría estaría incluida dentro de procedimientos y actividades se encuentran monitoreados
Los datos son eliminados de acuerdo a las políticas de seguridad	No	Esta se encuentra incluida en la subcategoría de ciclo de vida de aplicaciones y dispositivos administrado
Se gestiona y protege el acceso físico a los activos.	No	No aplica ya que al ser un dispositivo móvil no permanecen en un lugar fijo

Subcategoría	Aplica?	Comentarios
Suministradores y socios son monitoreados para confirmar que ellos satisfacen sus obligaciones como son requeridas	No	Esta no está relacionada con temas de dispositivos móviles
Restricciones a aplicaciones establecidas	No	En la subcategoría de dispositivos asegurados en la configuración de los dispositivos ya se restringe los permisos de las aplicaciones
Conexión de los dispositivos móviles a otros dispositivos restringida	No	Estas restricciones formar parte de la subcategoría de capacitación y concientización la cual busca evitar la conexión a dispositivos infectados
Proceso para evaluar seguridad de las aplicaciones realizado	No	Esto se encuentra en la de riesgos de aplicaciones evaluados y tratados
Tecnologías criptográficas implementadas para proteger la autenticación del usuario y datos de correos	No	Esta forma parte de la subcategoría de mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos
Registro de Anomalías disponible	No	La subcategoría de anomalías cubre esta subcategoría
Comunicación a través de correo protegido	No	Esta se encuentra en datos transmitidos protegidos así que esta no sería necesaria
Acceso a aplicaciones restringido	No	La evaluación de los riesgos de las aplicaciones determinaran que aplicaciones pueden usarse y cuales no

Subcategoría	Aplica?	Comentarios
Requerimientos para expiración de contraseñas establecidos	No	Esta se debe definir por las políticas de gestión de contraseñas que se encuentra en la política de ciberseguridad para dispositivos móviles
Contraseñas transmitidas para la autenticación deben estar cifradas	No	Esta se encuentra en datos transmitidos protegidos así que esta no sería necesaria
Soluciones de dispositivos móviles probadas antes de pasar a producción	No	Esta subcategoría forma parte de la subcategoría de ciclo de vida administrado
Uso de aplicaciones no confiables restringido	No	Estas restricciones formar parte de la subcategoría de capacitación y concientización la cual permitirá reducir los accesos a aplicaciones no confiable por parte personal
Acceso a contenido no confiable con los dispositivos móviles restringido	No	Estas restricciones formar parte de la subcategoría de capacitación y concientización la cual permitirá reducir los accesos a contenido no confiable por parte personal

Tercera Sección:

La última sección corresponde al mapeo de las subcategorías que aplican al modelo con las categorías del marco de NIST para determinar que categorías son las que tienen al menos una subcategoría y por lo cual deben estar incluidas en el modelo y que es el siguiente:

Mapeo de subcategorías que aplican con categorías del marco de NIST

Categoría	Subcategoría	Referencia
Gestión de Activos	Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas	NIST SP 800-124, ISO 27032
	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados	NIST SP 800-124, ISO 27032, NIST SP 800-53
Gobierno de ciberseguridad	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	NIST SP 800-124, NIST SP 800-164, NIST SP 800-118, NIST SP 800-61
Gestión de riesgo de TI	Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	NIST SP 800-163, NIST SP 800-124, ISO 27032
Concientización y formación	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	NIST SP 800-118, NIST SP 800-124, ISO 27032
	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	NIST SP 800-61, NIST SP 800-121, NIST SP 800-124
Control de acceso	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos	NIST SP 800-124
Seguridad de los datos	Datos almacenados y transmitidos se encuentran protegidos	NIST SP 800-124, NIST SP 800-118,NIST

Categoría	Subcategoría	Referencia
		SP 800-45
Tecnología de protección	Interfaces de red se encuentran administradas	NIST SP 800-124, ISO 27032
	Tecnologías para la administración centralizada de los dispositivos móviles esta implementada	NIST SP 800-124
	Dispositivo móviles entregados por la organización están completamente asegurados	NIST SP 800-124, NIST SP 800-45, NIST SP 800-121, NIST SP 800-164, NIST SP 800-118
Procesos y procedimientos para la protección de la información	Ciclo de vida de las aplicaciones y dispositivos móviles están administrados	NIST SP 800-124, NIST SP 800-88
Anomalías y Eventos	Comportamiento del código y anomalías esta administrado	NIST SP 800-124, ISO 27032
Monitoreo continuo de la seguridad	Seguridad de los dispositivos móviles se encuentra monitoreada	NIST SP 800-124, ISO 27032
	Políticas, procesos y procedimientos están monitoreados	NIST SP 800-124, ISO 27032
Planificación de Respuesta	Plan de respuesta durante incidentes este implementado	NIST SP 800-61, ISO 27032

Categoría	Subcategoría	Referencia
Comunicación	Canales de comunicación para soporte y avisos están habilitados	NIST SP 800-184, ISO 27032
Planificación de Recuperación	Plan de recuperación después incidentes este implementado	NIST SP 800-184, ISO 27032
Mejora	Lecciones aprendidas de los incidentes están implementadas	NIST SP 800-61
	Categorías se encuentren auditadas periódicamente	NIST SP 800-163
	Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados	ISO 27032

Anexo 4 – Protocolo para la ejecución del juicio experto

El protocolo para la ejecución del juicio experto será el siguiente:

Se enviara por correo la solicitud para que los expertos ejecuten el juicio experto, enviándoles los documentos necesarios para ejecutar dicha labor. Los documentos que se enviaran son los siguientes:

- Estructuras de Gobierno Sugeridas
- Lista de verificación para autoevaluación
- Macro de la lista de verificación
- Cuestionario 1- Pertinencia de Subcategorías
- Cuestionario 2- Correspondencia entre subcategorías y los indicadores
- Cuestionario 3 - Implementación de la guía
- Detalle de Procedimiento de Selección de Subcategorías y Categorías del modelo
- Guía de Implementación del modelo
- Indicadores del Modelo
- Lista de Componentes del Modelo

En el correo estarán las indicaciones de como usaran estos documentos para poder validar el modelo

Por último, se enviara un documento donde los expertos darán el resultado de su evaluación

A continuación se presentara el correo que se enviara a los expertos:

Carta de Presentación

Saludos Profesor(a),

Me dirijo a usted con la finalidad de pedir su colaboración para la ejecución del juicio experto de mi proyecto de fin de carrera el cual consiste en el diseño de un modelo de ciberseguridad para dispositivos móviles del sector empresarial ya que se requiere su apoyo para poder dar por validado el mismo. Para que puedan ejecutar el juicio experto y validar el modelo se están adjuntado una serie de documentos que son los siguientes:

- Estructuras de Gobierno Sugeridas
- Lista de verificación para autoevaluación
- Macro de la lista de verificación
- Cuestionario 1- Pertinencia de Subcategorías
- Cuestionario 2- Correspondencia entre subcategorías y los indicadores
- Cuestionario 3 - Implementación de la guía
- Detalle de Procedimiento de Selección de Subcategorías y Categorías del modelo
- Guía de Implementación del modelo
- Indicadores del Modelo
- Lista de Componentes del Modelo
- Resultado del juicio experto

Para que puedan ejecutar el juicio experto se les solicita revisar los cuestionarios enviados con los otros documentos de esta forma (Se requiere que imprima los cuestionarios y luego los responda):

1. Responder el Cuestionario 1- Pertinencia de Subcategorías habiendo revisado previamente el documento de la lista de componentes del modelo y el documento del Detalle de Procedimiento de Selección de Subcategorías y Categorías del modelo donde se presentan las categorías y subcategorías del modelo
2. Responder el Cuestionario 2- Correspondencia entre subcategorías y los indicadores habiendo revisado previamente el documento de Indicadores del

Modelo y el documento del Detalle de Procedimiento de Selección de Subcategorías y Categorías del modelo

3. Responder el Cuestionario 3 - Implementación de la guía habiendo revisado previamente el documento de Estructuras de Gobierno Sugeridas, Lista de verificación para autoevaluación junto con la macro de la lista de verificación, Guía de Implementación del modelo y el documento del Detalle de Procedimiento de Selección de Subcategorías y Categorías del modelo

Luego de responder todos los cuestionarios, se solicita completar el documento llamado resultado del juicio experto donde se solicita que determine en función de la evaluación hecha con los cuestionarios si el modelo diseñado es válido o no.

Para esto se requiere que imprima dicho documento y responda. Luego de responder se requiere que escanee este documento junto con los cuestionarios respondidos y me envié dichos documentos a mi correo que se encuentra al final de este correo.

Les agradezco de manera anticipada su atención y participación en esta evaluación.

Atentamente,

Nombre: Ramon Bruderer

Código: 20079007

Estudiante de Ingeniería Informática

Correo: a20079007@pucp.edu.pe

Institución: Pontificia Universidad Católica del Perú

Anexo 5 – Cuestionario 1- Pertinencia de Subcategorías

Objetivo

Validar la pertinencia de las subcategorías definidas

Instrucciones

Marque con una X en los espacios del cuestionario para cada subcategoría si considera que la presencia de dicha subcategoría es pertinente o no para el modelo propuesto

Significado de Respuestas:

No pertinente (1): No debería estar en el modelo

Poco pertinente (2): Su presencia contribuye poco o nada al modelo

Pertinente (3): Debe estar en el modelo

Si las subcategorías tienen un valor asignado de muy pertinente o pertinente no se requerirá hacer ninguna modificación

Si la subcategoría tiene un valor de poco pertinente se revisara

Si la subcategoría tiene un valor de no pertinente se quitara del modelo, En caso la subcategoría fuera la única subcategoría de una categoría también se eliminara dicha categoría

1. **Marque si considera que los componentes del modelo propuesto se ajustan a los componentes del marco de NIST, Los componentes del modelo con respecto a los componentes de NIST son:**

Diferentes	Similares	Iguales

Observaciones:

2. **Marque los espacios en blanco según el nivel de pertinencia que considera que tiene cada subcategoría para el marco:**

Subcategoría	Descripción de Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Roles y Responsabilidades	las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas				
Control de Activos	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados				
Políticas de ciberseguridad para dispositivos móviles	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada				
Riesgos de TI	Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados				

Subcategoría	Descripción de Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Capacitación	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles				
Concientización	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones				
Autenticación	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos				
Protección de la información	Datos almacenados y transmitidos por los dispositivos móviles se encuentran protegidos				
Conectividad	Las redes a las que se conectan los dispositivos móviles se encuentran administradas				

Subcategoría	Descripción de Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Desarrollo y mantenimiento de aplicaciones	El desarrollo y mantenimiento de aplicaciones esta administrado				
Limpieza de información de los dispositivos móviles	La limpieza de información de los dispositivos móviles está administrada				
Monitoreo de anomalías y amenazas	Seguridad de los dispositivos móviles se encuentra monitoreada				
Monitoreo del cumplimiento de las políticas y procedimientos	El cumplimiento de las políticas y procedimientos de seguridad para dispositivos móviles se encuentra monitoreada				
Respuesta a incidentes	El procedimiento de respuesta incidentes esta implementado				
Mesa de Ayuda	Mesa de ayuda para el reporte de incidentes esta implementada				

Subcategoría	Descripción de Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Planificación de comunicación	Plan de comunicación esta implementado				
Recuperación de incidentes	El procedimiento de recuperación de incidentes esta implementado				
Gestión del Conocimiento	Lecciones aprendidas están implementadas				
Evaluación y Auditoría	Categorías se encuentren auditadas periódicamente				
Innovación	Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas				

Nombre del Experto: _____

Fecha de respuesta del cuestionario: _____

Firma del Experto: _____

Anexo 6 – Cuestionario 2- Correspondencia entre subcategorías y los indicadores

Objetivo

Validar que las métricas asignadas miden adecuadamente el cumplimiento de los objetivos de los controles (subcategorías)

Instrucciones

Marque con una X en los espacios del cuestionario para cada indicador si considera que dicho indicador permite medir adecuadamente el cumplimiento de dicho objetivo de control (subcategoría)

Significado de Respuestas:

No Adecuado (1): Se debe cambiar de indicador

Poco Adecuado (2): No está mal pero hay indicadores mejores

Adecuado (3): No necesita ningún cambio

Si el indicador tiene un valor de no adecuado se cambiara por otro indicador

Si el indicador tiene un valor de poco adecuado se revisara si se cambiara o no dicho indicador

Si el indicador tiene un valor de adecuado no se hará ningún cambio del indicador

Marque los espacios en blanco si considera que si corresponde un indicador a la subcategoría asignada:

Subcategoría	Descripción de Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Roles y Responsabilidades	las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas	# de roles no asignados a los usuarios				
		# de incidentes producidos por incumplimiento de las responsabilidades asignadas a los usuarios				
Control de Activos	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados	# de aplicaciones y dispositivos desconocidos				
		# de errores en la clasificación				
		# de fallas detectadas en la seguridad de los dispositivos móviles				
Políticas de ciberseguridad para dispositivos móviles	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	Estado de la política (aprobada, formalizada, difundida, implementada)				
		# de violaciones a las políticas				
Riesgos de TI	Riesgo de aplicaciones y dispositivos se encuentran	# de incidentes materializados por riesgos aceptados				

Subcategoría	Descripción de Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
	identificados, evaluados y tratados	# de incidentes materializados por riesgos cuyo impacto fue mal evaluado				
		# de incidentes materializados por riesgos no identificados				
Capacitación	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	# de errores de los usuarios durante los procesos de respuesta o recuperación de incidentes				
		% de aprobados del total de capacitados				
Concientización	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	# de incidentes producidos no reportados o mal reportados				
Autenticación	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos	# de accesos no autorizados				
Protección de la información	Datos almacenados y transmitidos se encuentran protegidos	# de filtraciones de la información almacenada				
		# de alteraciones en el flujo de información de cada dispositivo móvil				

Subcategoría	Descripción de Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Conectividad	Las redes a las que se conectan los dispositivos móviles se encuentran administradas	# de dispositivos no autorizados conectados a la red				
Desarrollo y mantenimiento de aplicaciones	El desarrollo y mantenimiento de aplicaciones esta administrado	# de aplicaciones que no tienen suficientes medidas de seguridad implementadas				
		# de actualizaciones de seguridad de las aplicaciones desarrolladas realizadas				
Limpieza de información de los dispositivos móviles	La limpieza de información de los dispositivos móviles está administrada	# de fallas en el proceso de limpieza de información de los dispositivos móviles				
Monitoreo de anomalías y amenazas	Seguridad de los dispositivos móviles se encuentra monitoreada	# de cambios no autorizados en la configuración de los dispositivos móviles no detectados a tiempo				
Monitoreo del cumplimiento de las políticas y procedimientos	El cumplimiento de las políticas y procedimientos de seguridad para dispositivos móviles se encuentra monitoreada	# de incumplimientos a las políticas o procedimientos no detectadas a tiempo				
Respuesta a incidentes	El procedimiento de respuesta incidentes esta implementado	# de retrasos en la respuesta a incidentes				
		# de incidentes no controlados adecuadamente				

Subcategoría	Descripción de Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Mesa de Ayuda	Mesa de ayuda para el reporte de incidentes esta implementada	# de veces que se reportan ocupada la mesa de ayuda				
Planificación de comunicación	Plan de comunicación esta implementado	# de filtraciones de información durante la comunicación de la ocurrencia de un incidente				
Recuperación de incidentes	El procedimiento de recuperación de incidentes esta implementado	# de fallas en la recuperación				
		# de recuperaciones retrasadas				
Gestión del Conocimiento	Lecciones aprendidas están implementadas	% de lecciones aprendidas implementadas				
Evaluación y Auditoría	Categorías se encuentren auditadas periódicamente	# de auditorías realizadas				
Innovación	Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas	% de innovaciones para la seguridad de los dispositivos móviles implementadas				

Nombre del Experto: _____

Fecha de respuesta del cuestionario: _____

Firma del Experto: _____

Anexo 7 – Cuestionario 3 - Implementación de la guía

Objetivo

Validar que la información brindada por la guía permita la implementación del modelo propuesto

Instrucciones

Marcar con una X en los espacios del cuestionario si considera que el ítem a evaluar requiere cambios o no

Significado de Respuestas:

No Adecuado (1): Requiere cambiarse todo

Poco Adecuado (2): Requiere algunos cambios

Adecuado (3): No necesita ningún cambio

Para validar la guía primero se validara si las estructuras de gobierno sugeridas y el procedimiento de autoevaluación son los adecuados

Luego se validara si los controles propuestos en la parte de las acciones recomendadas de la guía permiten lograr cumplir los objetivos de los controles (Subcategoría)

1. **¿Considera que las estructuras de gobierno sugeridas son las adecuadas para el modelo propuesto?:**

No Adecuado	Poco Adecuado	Adecuado

Observaciones:

2. **¿Considera que el procedimiento de autoevaluación planteado permite determinar adecuadamente que controles se requieren para alcanzar el nivel de seguridad deseado?:**

No Adecuado	Poco Adecuado	Adecuado

Observaciones:

3. **Marque los espacios en blanco si considera que el control en la guía del modelo asociado a cada subcategorías permite lograr los objetivos de los controles (subcategoría) correspondientes:**

Actividades	Subcategoría	Descripción de Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Definir y comunicar los roles y responsabilidades que tienen a los usuarios de los dispositivos móviles	**Roles y Responsabilidades**	las responsabilidades y roles de seguridad de dispositivos móviles se encuentran establecidas y asignadas				
Realizar el inventario de los dispositivos móviles, las aplicaciones usadas en estos dispositivos y sus usuarios	**Control de Activos**	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados y clasificados, además para los dispositivos móviles estos están asegurados y administrados				
Clasificar y categorizar la información que se manejara por medio de los dispositivos móviles, los dispositivos en sí y las aplicaciones según el tipo de dispositivos , la confidencialidad de la información que se maneje y el software del dispositivo						

Implementar tecnologías para administrar la seguridad de los dispositivos móviles de manera centralizada para poder borrar la información o bloquear un dispositivo móvil de manera remota						
Establecer controles de seguridad en función de la políticas establecidas y configurar los dispositivos que usen Bluetooth con el modo de seguridad de Bluetooth más fuerte con el que disponen						
Establecer controles de seguridad suplementarios como antivirus y tecnologías para la prevención de perdida de datos						
Definir una política de seguridad de la información para dispositivos móviles	**Políticas de ciberseguridad para dispositivos móviles**	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada				

Realizar un inventario de las vulnerabilidades y amenazas de seguridad de los dispositivos móviles y las aplicaciones usadas y evaluar sus riesgos en función del impacto y la frecuencia de la materialización de dichos riesgos	**Riesgos de TI**	Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados				
Establecer controles que permitan mitigar los riesgos y garanticen el cumplimiento de los requerimientos de seguridad definidos en las políticas						
Realizar campañas de capacitación sobre las políticas de seguridad que se usan, sobre la forma que se sigue para detectar, reportar, responder y recuperarse de los incidentes y sobre las acciones recomendadas para controlar los ataques cibernéticos o escenarios de riesgo	**Capacitación**	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles				
Evaluar el resultado de las capacitaciones para comprobar si esta tuvo éxito						

Realizar campañas de concientización sobre las políticas de seguridad que se usan, sobre las responsabilidades de seguridad al momento de usar los dispositivos móviles por parte de los usuarios y sobre las amenazas a los dispositivos móviles y el comportamiento de las mismas	**Concientización**	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones				
Establecer múltiples métodos de autenticación para poder acceder a la información por medio de dispositivos móviles y un proceso para firmar digitalmente un correo para asegurar la integridad del mismo y poder comprobar la identidad del que lo envía	**Autenticación**	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos				
Encriptar los datos almacenados en los dispositivos móviles y los datos transmitidos por estos	**Protección de la información**	Datos almacenados y transmitidos por los dispositivos móviles se encuentran protegidos				

Identificar y segregar las interfaces de red para comunicaciones internas y externas y usar software de administración de redes para monitorear y gestionar las interfaces de red	**Conectividad**	Las redes a las que se conectan los dispositivos móviles se encuentran administradas				
Documentar los pasos a seguir al diseñar y desarrollar aplicaciones de tal forma que estas tengan los niveles de seguridad solicitados y que no permitan el filtrado de información Tener documentado y actualizado un registro sobre el comportamiento de las aplicaciones, sus manuales de usuario	**Desarrollo y mantenimiento de aplicaciones**	El desarrollo y mantenimiento de aplicaciones esta administrado				
Establecer un proceso de saneamiento que permita borrar la información de los dispositivos móviles según el tipo de dispositivo y la información contenida, además establecer un proceso de verificación que permita comprobar el adecuado saneamiento de un dispositivo móvil	**Limpieza de información de los dispositivos móviles**	La limpieza de información de los dispositivos móviles está administrada				

Monitorear la presencia de anomalías en los dispositivos móviles y la ocurrencia de incidentes de seguridad de los dispositivos móviles a través de software de detección de intrusos u otro software de monitoreo, además llevar un registro de las anomalías detectadas	**Monitoreo de anomalías y amenazas**	Seguridad de los dispositivos móviles se encuentra monitoreada				
Monitorear y reportar cuando una violación de las políticas, procedimientos establecidos de respuesta, recuperación y comunicación de incidentes ocurre	**Monitoreo del cumplimiento de las políticas y procedimientos**	El cumplimiento de las políticas y procedimientos de seguridad para dispositivos móviles se encuentra monitoreada				
Definir una estrategia y elaborar un plan para la respuesta a los incidentes y una guía para priorizar la respuesta a incidentes, además definir procedimientos para responder cuando se materialice un incidente	**Respuesta a incidentes**	El procedimiento de respuesta incidentes esta implementado				
Hacer un plan de comunicación y realizar simulacros de prueba del plan de comunicación para comprobar el correcto funcionamiento de plan	**Planificación de comunicación**	Plan de comunicación esta implementado				

Implementar un mesa de ayuda para responder consultas y que permita comunicar adecuadamente la ocurrencia de incidentes	**Mesa de Ayuda**	Mesa de ayuda para el reporte de incidentes esta implementada				
Definir una estrategia y elaborar un plan para la recuperación de los incidentes y una guía para priorizar la recuperación de incidentes, además definir procedimientos a seguir cuando se deba recuperar de un incidente	**Recuperación de incidentes**	El procedimiento de recuperación de incidentes esta implementado				
Realizar reuniones sobre las lecciones aprendidas y usar la información de las reuniones de lecciones aprendidas para identificar y corregir las deficiencias y debilidades en las políticas, controles y procedimientos de respuesta, comunicación y recuperación de incidentes	**Gestión del Conocimiento**	Lecciones aprendidas están implementadas				

Realizar auditorías periódicamente para evaluar el funcionamiento de las categorías del modelo y proponer mejoras en función de los resultados de las auditorias que permitan mejorar la seguridad de los dispositivos, los procedimientos de respuesta, comunicación y recuperación de incidentes	**Evaluación y Auditoría**	Categorías se encuentren auditadas periódicamente				
Participar en comunidades o foros de la industria relevantes para mantenerse al día con las mejores prácticas y últimas vulnerabilidades y por medio de la implementación de dichas prácticas o controles cubrir las nuevas vulnerabilidades que se detecten	**Innovación**	Las últimas innovaciones de seguridad para dispositivos móviles están revisadas e implementadas				

Nombre del Experto: _____

Fecha de respuesta del cuestionario: _____

Firma del Experto: _____

Anexo 8 – Resultados del Juicio Experto

Plantilla de Resultado de Juicio Experto

Saludos Profesor(a),

En función de la evaluación hecha con los cuestionarios se solicita que llene los espacios en blanco y de su resultado si el modelo de ciberseguridad para dispositivos móviles del sector empresarial propuesto es válido o no.

Resultado de los cuestionarios:

En función de los resultados del Cuestionario 1 si considera que los componentes y procesos de modelo son:

Valido ( ) Inválido ( )

En función de los resultados del Cuestionario 2 si considera que los indicadores del modelo son:

Valido ( ) Inválido ( )

En función de los resultados del Cuestionario 3 si considera que la guía del modelo es:

Valido ( ) Inválido ( )

Resultado del Juicio Experto:

Marque si considera que el modelo diseñado es

Valido ( ) Inválido ( )

Comentarios:

_____

_____

_____

Nombre y apellidos del Experto: _____-

Correo: _____-

DNI: _____

Especialidad: _____

Institución: _____

Firma: _____

Cuestionario para juicio experto sobre un modelo de ciberseguridad para dispositivos móviles del sector empresarial – Pertinencia de subcategorías

Objetivo

Validar la pertinencia de las subcategorías definidas

Instrucciones

Marque con una X en los espacios del cuestionario para cada subcategoría si considera que la presencia de dicha subcategoría es pertinente o no para el modelo propuesto

Significado de Respuestas:

No pertinente (1): No debería estar en el modelo

Poco pertinente (2): Su presencia contribuye poco o nada al modelo

Pertinente (3): Debe estar en el modelo

Si las subcategorías tienen un valor asignado de muy pertinente o pertinente no se requerirá hacer ninguna modificación

Si la subcategoría tiene un valor de poco pertinente se revisara

Si la subcategoría tiene un valor de no pertinente se quitara del modelo, En caso la subcategoría fuera la única subcategoría de una categoría también se eliminara dicha categoría

1. **Marque si considera que los componentes del modelo propuesto se ajustan a los componentes del marco de NIST, Los componentes del modelo con respecto a los componentes de NIST son:**

Diferentes	Similares	Iguales
	X	

Observaciones:

Los componentes son similares y adecuados para un modelo de marco de Ciberseguridad para dispositivos móviles.

2. **Marque los espacios en blanco según el nivel de pertinencia que considera que tiene cada subcategoría para el marco:**

Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas			X	
Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados			X	
Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada			X	
Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados			X	
Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles			X	
Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones			X	

Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos			X	
Datos almacenados y transmitidos se encuentran protegidos			X	
Interfaces de red se encuentran administradas			X	
Tecnologías para la administración centralizada de los dispositivos móviles esta implementada			X	
Dispositivo móviles entregados por la organización están completamente asegurados			X	
Ciclo de vida de las aplicaciones y dispositivos móviles están administrados			X	
Comportamiento del código y anomalías esta administrado			X	Se debe precisar a qué se refiere con código.
Seguridad de los dispositivos móviles se encuentra monitoreada			X	
Políticas, procesos y procedimientos están monitoreados			X	Precisar si se refiere a todas las políticas y procedimientos o sólo a las políticas y procedimientos referentes a dispositivos móviles.

Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Plan de respuesta durante incidentes este implementado			X	
Canales de comunicación para soporte y avisos están habilitados			X	
Plan de recuperación después incidentes este implementado			X	
Lecciones aprendidas de los incidentes están implementadas			X	
Categorías se encuentren auditadas periódicamente			X	
Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados			X	

Nombre del Experto: Diana Lepage Hoces

Fecha de respuesta del cuestionario: 18/11/2017

Firma del Experto: 

Cuestionario para juicio experto sobre un modelo de ciberseguridad para dispositivos móviles del sector empresarial – Correspondencia entre subcategorías y los indicadores

Objetivo

Validar que las métricas asignadas miden adecuadamente el cumplimiento de los objetivos de los controles (subcategorías)

Instrucciones

Marque con una X en los espacios del cuestionario para cada indicador si considera que dicho indicador permite medir adecuadamente el cumplimiento de dicho objetivo de control (subcategoría)

Significado de Respuestas:

No Adecuado (1): Se debe cambiar de indicador

Poco Adecuado (2): No está mal pero hay indicadores mejores

Adecuado (3): No necesita ningún cambio

Si el indicador tiene un valor de no adecuado se cambiara por otro indicador

Si el indicador tiene un valor de poco adecuado se revisara si se cambiara o no dicho indicador

Si el indicador tiene un valor de adecuado no se hará ningún cambio del indicador

Marque los espacios en blanco si considera que si corresponde un indicador a la subcategoría asignada:

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas	# de roles no asignados		X		Se refiere a roles (estructura de gobierno) o los roles de seguridad que se asignarán sobre el dispositivo móvil.
Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados	# de aplicaciones y dispositivos desconocidos			X	
	# de errores en la categorización y clasificación			X	
Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	Estado de la política (aprobada, formalizada, difundida, implementada)			X	
	# de faltas detectadas a la política		X		Ya se cuenta con un indicador asociado a violaciones de la política, pero no está mal según el contexto en el cual aplica.
	# de violaciones a las políticas			X	
Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	# de incidentes materializados por riesgos aceptados			X	
	# de incidentes materializados por riesgos no identificados			X	

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	# de errores en los procesos de respuesta, recuperación o comunicación de incidentes			X	La métrica es correcta, pero se podría precisar que los errores en el proceso de respuesta, recuperación o comunicación de incidentes no dependerán necesariamente de los usuarios.
	% de aprobados del total de capacitados			X	
Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	# de incidentes detectados pero no reportados			X	
Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos	# de accesos no autorizados			X	
Datos almacenados y transmitidos se encuentran protegidos	# de filtraciones de información			X	
	# de alteraciones detectadas de datos de manera irregular		X		Se podría refrasear por #alteraciones en el flujo de información de cada dispositivo móvil.
Interfaces de red se encuentran administradas	Estado de la interfaces de red (identificada, restringida, monitoreada, gestionada)			X	
	# de dispositivos no autorizados conectados a la red			X	
Tecnologías para la administración centralizada de los dispositivos móviles esta implementada	# de bloqueos o limpieza remota de los dispositivos fallidas			X	

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Dispositivo móviles entregados por la organización están completamente asegurados	Estado de dispositivos a entregados (identificados, configurados, protegidos)		X		Revisar esta métrica, pues es un poco confusa, ya hay una métrica de inventario de equipos.
	# de fallas detectadas en la seguridad			X	Considerar complementar por # de fallas detectadas en la seguridad de dispositivos móviles.
Ciclo de vida de las aplicaciones y dispositivos móviles están administrados	# de dispositivos no asegurados correctamente			X	
Comportamiento del código y anomalías esta administrado	# de documentos (manuales de usuarios de las aplicaciones) no actualizados			X	
	# de anomalías repetidas registradas			X	
Seguridad de los dispositivos móviles se encuentra monitoreada	# de cambios no autorizados en la configuración no detectados a tiempo			X	
Políticas, procesos y procedimientos están monitoreados	# de incumplimientos a las políticas, procesos o procedimientos no detectadas a tiempo		X		Revisar esta métrica, me parece que está repetida.
Plan de respuesta durante incidentes este implementado	# de retrasos en la respuesta a incidentes			X	
	# de incidentes no controlados adecuadamente			X	

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Canales de comunicación para soporte y avisos están habilitados	# de veces que se reportan ocupados los canales de comunicación			X	La métrica es correcta, pero pueden haber algunas un poco más sólidas.
Plan de recuperación después incidentes este implementado	# de fallas en la recuperación			X	
	# de recuperaciones retrasadas			X	
Lecciones aprendidas de los incidentes están implementadas	% de lecciones aprendidas implementadas			X	
Categorías se encuentren auditadas periódicamente	# de auditorías realizadas			X	
Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados	% de mejoras implementadas			X	

Nombre del Experto: Diana Lepage Hoces.

Fecha de respuesta del cuestionario: 18/11/2017.

Firma del Experto: 

Cuestionario para juicio experto sobre un modelo de ciberseguridad para dispositivos móviles del sector empresarial – Implementación de la guía

Objetivo

Validar que la información brindada por la guía permita la implementación del modelo propuesto

Instrucciones

Marcar con una X en los espacios del cuestionario si considera que el ítem a evaluar requiere cambios o no

Significado de Respuestas:

No Adecuado (1): Requiere cambiarse todo

Poco Adecuado (2): Requiere algunos cambios

Adecuado (3): No necesita ningún cambio

Para validar la guía primero se validara si las estructuras de gobierno sugeridas y el procedimiento de autoevaluación son los adecuados

Luego se validara si los controles propuestos en la parte de las acciones recomendadas de la guía permiten lograr cumplir los objetivos de los controles (Subcategoría)

1. **¿Considera que las estructuras de gobierno sugeridas son las adecuadas para el modelo propuesto?:**

No Adecuado	Poco Adecuado	Adecuado
		X

Observaciones:

Ninguna.

2. **¿Considera que el procedimiento de autoevaluación planteado permite determinar adecuadamente que controles se requieren para alcanzar el nivel de seguridad deseado?:**

No Adecuado	Poco Adecuado	Adecuado
	X	

Observaciones:

Me parece que la lista de verificación podría ser más sencilla, no obstante se han implementado mejoras respecto a la versión inicial.

3. **Marque los espacios en blanco si considera que el control en la guía del modelo asociado a cada subcategorías permite lograr los objetivos de los controles (subcategoría) correspondientes:**

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Definir y comunicar los roles y responsabilidades que tienen a los usuarios de los dispositivos móviles	Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas			X	
Realizar el inventario de los dispositivos móviles, las aplicaciones usadas en estos dispositivos y sus usuarios	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados			X	
Clasificar y categorizar la información que se manejara por medio de los dispositivos móviles, los dispositivos en sí y las aplicaciones según el tipo de dispositivos , la confidencialidad de la información que se maneje y el software del dispositivo					
Definir una política de seguridad de la información para dispositivos móviles	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada			X	
Realizar un inventario de las vulnerabilidades y amenazas de seguridad de los dispositivos móviles y las aplicaciones usadas y evaluar sus riesgos en función del impacto y la frecuencia de la materialización de dichos riesgos	Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados			X	
Establecer controles que permitan mitigar los riesgos y garanticen el cumplimiento de los requerimientos de seguridad definidos en las políticas					

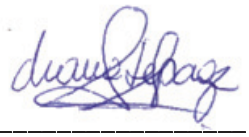
Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Realizar campañas de capacitación sobre las políticas de seguridad que se usan, sobre la forma que se sigue para detectar, reportar, responder y recuperarse de los incidentes y sobre las acciones recomendadas para controlar los ataques cibernéticos o escenarios de riesgo	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles			X	
Evaluar el resultado de las capacitaciones para comprobar si esta tuvo éxito					
Realizar campañas de concientización sobre las políticas de seguridad que se usan, sobre las responsabilidades de seguridad al momento de usar los dispositivos móviles por parte de los usuarios y sobre las amenazas a los dispositivos móviles y el comportamiento de las mismas	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones			X	
Establecer múltiples métodos de autenticación para poder acceder a la información por medio de dispositivos móviles y un proceso para firmar digitalmente un correo para asegurar la integridad del mismo y poder comprobar la identidad del que lo envía	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos			X	
Encriptar los datos almacenados en los dispositivos móviles y los datos transmitidos por estos	Datos almacenados y transmitidos se encuentran protegidos			X	
Identificar y segregar las interfaces de red para comunicaciones internas y externas y usar software de administración de redes para monitorear y gestionar las interfaces de red	Interfaces de red se encuentran administradas			X	
Implementar tecnologías para administrar la seguridad de los dispositivos móviles de manera centralizada para poder borrar la información o bloquear un dispositivo móvil de manera remota	Tecnologías para la administración centralizada de los dispositivos móviles esta implementada			X	

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Establecer controles de seguridad en función de la políticas establecidas y configurar los dispositivos que usen Bluetooth con el modo de seguridad de Bluetooth más fuerte con el que disponen Establecer controles de seguridad suplementarios como antivirus y tecnologías para la prevención de perdida de datos	Dispositivo móviles entregados por la organización están completamente asegurados			X	
Establecer un proceso de saneamiento que permita borrar la información de los dispositivos móviles según el tipo de dispositivo y la información contenida, además establecer un proceso de verificación que permita comprobar el adecuado saneamiento de un dispositivo móvil	Ciclo de vida de las aplicaciones y dispositivos móviles están administrados		X		La actividad está bien pero no corresponde con esta sub-categoría, la subcategoría corresponde más a actividades asociadas a cambios y desarrollos.
Tener documentado y actualizado un registro sobre el comportamiento de las aplicaciones, sus manuales de usuario y de las anomalías detectadas	Comportamiento del código y anomalías esta administrado			X	
Monitorear la presencia de anomalías en los dispositivos móviles y la ocurrencia de incidentes de seguridad de los dispositivos móviles a través de software de detección de intrusos u otro software de monitoreo	Seguridad de los dispositivos móviles se encuentra monitoreada			X	
Monitorear y reportar cuando una violación de las políticas, procedimientos establecidos de respuesta, recuperación y comunicación de incidentes ocurre	Políticas, procesos y procedimientos están monitoreados			X	
Definir una estrategia y elaborar un plan para la respuesta a los incidentes y una guía para priorizar la respuesta a incidentes, además definir procedimientos para responder cuando se materialice un incidente	Plan de respuesta durante incidentes este implementado			X	

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Hacer un plan de comunicación y realizar simulacros de prueba del plan de comunicación para comprobar el correcto funcionamiento de plan	Canales de comunicación para soporte y avisos están habilitados		X		Me parece que no está alineado con la métrica que corresponde a esta sub-categoría.
Definir una estrategia y elaborar un plan para la recuperación de los incidentes y una guía para priorizar la recuperación de incidentes, además definir procedimientos a seguir cuando se deba recuperar de un incidente	Plan de recuperación después incidentes este implementado			X	
Realizar reuniones sobre las lecciones aprendidas y usar la información de las reuniones de lecciones aprendidas para identificar y corregir las deficiencias y debilidades en las políticas, controles y procedimientos de respuesta, comunicación y recuperación de incidentes	Lecciones aprendidas de los incidentes están implementadas			X	
Realizar auditorías periódicamente para evaluar el funcionamiento de las categorías del modelo y proponer mejoras en función de los resultados de las auditorias que permitan mejorar la seguridad de los dispositivos, los procedimientos de respuesta, comunicación y recuperación de incidentes	Categorías se encuentren auditadas periódicamente			X	
Participar en comunidades o foros de la industria relevantes para mantenerse al día con las mejores prácticas y últimas vulnerabilidades y por medio de la implementación de dichas prácticas o controles cubrir las nuevas vulnerabilidades que se detecten	Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados		X		Reforzar la parte de la implementación de las actualizaciones.

Nombre del Experto: Diana Lepage.

Fecha de respuesta del cuestionario: 18/11/2017.

Firma del Experto: 

Resultado del juicio experto

Sr Evaluador(a),

En función de la evaluación hecha con los cuestionarios se solicita que llene los espacios en blanco y de su resultado si el modelo de ciberseguridad para dispositivos móviles del sector empresarial propuesto es válido o no.

Resultado de los cuestionarios:

En función de los resultados del Cuestionario 1 si considera que los componentes y procesos de modelo son:

Valido (X) Inválido ( )

En función de los resultados del Cuestionario 2 si considera que los indicadores del modelo son:

Valido (X) Inválido ( )

En función de los resultados del Cuestionario 3 si considera que la guía del modelo es:

Valido (X) Inválido ( )

Resultado del Juicio Experto:

Marque si considera que el modelo diseñado es

Valido (X) Inválido ( )

Comentarios:

Según la evaluación realizada, a mi parecer el modelo requiere algunos ajustes adicionales que puedan complementarlo a fin de asegurar su practicidad y que pueda ser empleado en todo tipo de organización que maneje dispositivos móviles.

Estos ajustes adicionales, no obstante no restan validez al modelo presentado, pero será importante considerarlos con el fin de garantizar la continuidad del modelo y una futura implementación del mismo.

Nombre y apellidos del Evaluador: Diana Estefanía Lepage Hoces.

Correo: dlepage@pucp.pe

DNI: 44978344

Especialidad: Ingeniería Informática

Institución: Pontificia Universidad Católica del Perú.

Firma: 

Cuestionario para juicio experto sobre un modelo de ciberseguridad para dispositivos móviles del sector empresarial – Pertinencia de subcategorías

Objetivo

Validar la pertinencia de las subcategorías definidas

Instrucciones

Marque con una X en los espacios del cuestionario para cada subcategoría si considera que la presencia de dicha subcategoría es pertinente o no para el modelo propuesto

Significado de Respuestas:

No pertinente (1): No debería estar en el modelo

Poco pertinente (2): Su presencia contribuye poco o nada al modelo

Pertinente (3): Debe estar en el modelo

Si las subcategorías tienen un valor asignado de muy pertinente o pertinente no se requerirá hacer ninguna modificación

Si la subcategoría tiene un valor de poco pertinente se revisara

Si la subcategoría tiene un valor de no pertinente se quitara del modelo, En caso la subcategoría fuera la única subcategoría de una categoría también se eliminara dicha categoría

1. **Marque si considera que los componentes del modelo propuesto se ajustan a los componentes del marco de NIST, Los componentes del modelo con respecto a los componentes de NIST son:**

Diferentes	Similares	Iguales
	X	

Observaciones:

Tener en consideración que si fuesen “iguales” sería una copia del marco y el grado de innovación de la investigación sería nulo.

2. **Marque los espacios en blanco según el nivel de pertinencia que considera que tiene cada subcategoría para el marco:**

Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas			X	Podría mejorarse la redacción de tal manera que las categorías sean solamente una frase con descripción: 1. Roles y responsabilidades 2. Control de activos 3. Políticas y procedimientos 4. Gestión de riesgos 5. Capacitación 6. Autenticación 7. …
Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados			X	
Política de seguridad de información de dispositivos móviles aprobada, formalizada, difundida e implementada			X	
Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados			X	
Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles			X	
Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones			X	

Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos			X	
Datos almacenados y transmitidos se encuentran protegidos			X	¿A qué datos se refiere: a los manejados en los dispositivos móviles?
Interfaces de red se encuentran administradas		X		No se entiende qué son estas interfases de red y su relación con los dispositivos móviles.
Tecnologías para la administración centralizada de los dispositivos móviles esta implementada		X		¿A qué se refiere con administrar de manera centralizada los dispositivos electrónicos, si precisamente su movilidad hace que no sea un TIC centralizada sino ubiquitous?
Dispositivo móviles entregados por la organización están completamente asegurados			X	Esto es control de activos en todo caso.
Ciclo de vida de las aplicaciones y dispositivos móviles están administrados		X		¿Se refiere al desarrollo de aplicaciones móviles para los dispositivos para fines empresariales? Se entiende esto.
Comportamiento del código y anomalías esta administrado		X		¿Código fuente de las aplicaciones? ¿No estaría incluido en el caso anterior?
Seguridad de los dispositivos móviles se encuentra monitoreada			X	
Políticas, procesos y procedimientos están monitoreados			X	¿No está incluido antes? Al redactar la política y el procedimiento de monitoreo.

Subcategoría	No Pertinente	Poco Pertinente	Pertinente	Observaciones
Plan de respuesta durante incidentes este implementado			X	
Canales de comunicación para soporte y avisos están habilitados		X		No se entiende
Plan de recuperación después incidentes este implementado		X		Podría estar incluido en gestión de incidentes o plan de respuetas.
Lecciones aprendidas de los incidentes están implementadas		X		
Categorías se encuentren auditadas periódicamente			X	La categoría puede llamarse Evaluación y Auditoría o Revisión y Evaluación
Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados		X		Si no se especifica su relación con los dispositivos móviles, se encuentra formado.

Nombre del Experto: MANUEL TUPIA ANTICONA

Fecha de respuesta del cuestionario: **Sábado, 18 de Noviembre de 2017**

Firma del Experto: _____

Cuestionario para juicio experto sobre un modelo de ciberseguridad para dispositivos móviles del sector empresarial – Correspondencia entre subcategorías y los indicadores

Objetivo

Validar que las métricas asignadas miden adecuadamente el cumplimiento de los objetivos de los controles (subcategorías)

Instrucciones

Marque con una X en los espacios del cuestionario para cada indicador si considera que dicho indicador permite medir adecuadamente el cumplimiento de dicho objetivo de control (subcategoría)

Significado de Respuestas:

No Adecuado (1): Se debe cambiar de indicador

Poco Adecuado (2): No está mal pero hay indicadores mejores

Adecuado (3): No necesita ningún cambio

Si el indicador tiene un valor de no adecuado se cambiara por otro indicador

Si el indicador tiene un valor de poco adecuado se revisara si se cambiara o no dicho indicador

Si el indicador tiene un valor de adecuado no se hará ningún cambio del indicador

Marque los espacios en blanco si considera que si corresponde un indicador a la subcategoría asignada:

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas	# de roles no asignados			X	Adecuado pero no sería lo único. Que hayan 100 roles no significa que la empresa sea más segura
Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados	# de aplicaciones y dispositivos desconocidos			X	
	# de errores en la categorización y clasificación			X	Explicar qué son errores de categorización
Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada	Estado de la política (aprobada, formalizada, difundida, implementada)			X	
	# de faltas detectadas a la política	X			Basta con la siguiente
	# de violaciones a las políticas			X	
Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados	# de incidentes materializados por riesgos aceptados		X		¿Por qué por riesgos aceptados nada más? Justificar
	# de incidentes materializados por riesgos no identificados			X	¿Solo aquellos cuya fuente son los riesgos no identificados? ¿Y el resto?

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles	# de errores en los procesos de respuesta, recuperación o comunicación de incidentes			X	
	% de aprobados del total de capacitados			X	
Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones	# de incidentes detectados pero no reportados		X		Hay que ser conscientes que si no se reporta no necesariamente es porque ha fallado la concientización
Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos	# de accesos no autorizados			X	
Datos almacenados y transmitidos se encuentran protegidos	# de filtraciones de información			X	
	# de alteraciones detectadas de datos de manera irregular			X	
Interfaces de red se encuentran administradas	Estado de la interfaces de red (identificada, restringida, monitoreada, gestionada)	X			No se entiende la métrica porque no se entiende la categoría
	# de dispositivos no autorizados conectados a la red			X	
Tecnologías para la administración centralizada de los dispositivos móviles esta implementada	# de bloqueos o limpieza remota de los dispositivos fallidas	X			Revisar comentarios en el cuestionario anterior.

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Dispositivo móviles entregados por la organización están completamente asegurados	Estado de dispositivos a entregados (identificados, configurados, protegidos)			x	
	# de fallas detectadas en la seguridad			x	¿Fallas o incidentes? Aclarar
Ciclo de vida de las aplicaciones y dispositivos móviles están administrados	# de dispositivos no asegurados correctamente	X			
Comportamiento del código y anomalías esta administrado	# de documentos (manuales de usuarios de las aplicaciones) no actualizados	X			
	# de anomalías repetidas registradas	X			
Seguridad de los dispositivos móviles se encuentra monitoreada	# de cambios no autorizados en la configuración no detectados a tiempo			X	
Políticas, procesos y procedimientos están monitoreados	# de incumplimientos a las políticas, procesos o procedimientos no detectadas a tiempo			X	
Plan de respuesta durante incidentes este implementado	# de retrasos en la respuesta a incidentes			X	
	# de incidentes no controlados adecuadamente			X	

Subcategoría	Indicadores	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Canales de comunicación para soporte y avisos están habilitados	# de veces que se reportan ocupados los canales de comunicación			X	Considerar las observaciones hechas en el cuestionario 1
Plan de recuperación después incidentes este implementado	# de fallas en la recuperación			X	
	# de recuperaciones retrasadas			X	
Lecciones aprendidas de los incidentes están implementadas	% de lecciones aprendidas implementadas			X	
Categorías se encuentren auditadas periódicamente	# de auditorías realizadas			X	
Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados	% de mejoras implementadas			X	

Nombre del Experto: MANUEL TUPIA ANTICONA

Fecha de respuesta del cuestionario: **Sábado, 18 de Noviembre de 2017**

Firma del Experto: _____

Cuestionario para juicio experto sobre un modelo de ciberseguridad para dispositivos móviles del sector empresarial – Implementación de la guía

Objetivo

Validar que la información brindada por la guía permita la implementación del modelo propuesto

Instrucciones

Marcar con una X en los espacios del cuestionario si considera que el ítem a evaluar requiere cambios o no

Significado de Respuestas:

No Adecuado (1): Requiere cambiarse todo

Poco Adecuado (2): Requiere algunos cambios

Adecuado (3): No necesita ningún cambio

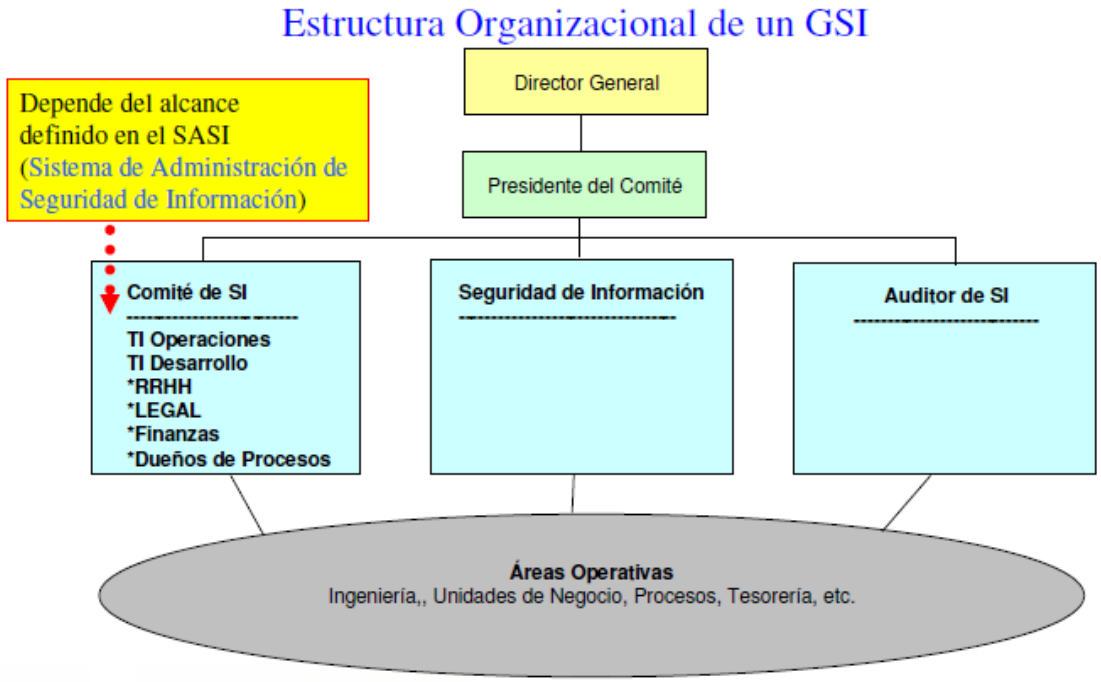
Para validar la guía primero se validara si las estructuras de gobierno sugeridas y el procedimiento de autoevaluación son los adecuados

Luego se validara si los controles propuestos en la parte de las acciones recomendadas de la guía permiten lograr cumplir los objetivos de los controles (Subcategoría)

1. **¿Considera que las estructuras de gobierno sugeridas son las adecuadas para el modelo propuesto?:**

No Adecuado	Poco Adecuado	Adecuado
		X

Observaciones:



Según este diagrama es necesario indicar el rol de la máxima autoridad en materia de seguridad de la información.

2. **¿Considera que el procedimiento de autoevaluación planteado permite determinar adecuadamente que controles se requieren para alcanzar el nivel de seguridad deseado?:**

No Adecuado	Poco Adecuado	Adecuado
		X

Observaciones:

3. **Marque los espacios en blanco si considera que el control en la guía del modelo asociado a cada subcategorías permite lograr los objetivos de los controles (subcategoría) correspondientes:**

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Definir y comunicar los roles y responsabilidades que tienen a los usuarios de los dispositivos móviles	Responsabilidades y roles de seguridad de dispositivos móviles establecidas y asignadas			X	
Realizar el inventario de los dispositivos móviles, las aplicaciones usadas en estos dispositivos y sus usuarios	Dispositivos móviles, las aplicaciones instaladas y sus usuarios se encuentran inventariados, categorizados y clasificados			X	
Clasificar y categorizar la información que se manejara por medio de los dispositivos móviles, los dispositivos en sí y las aplicaciones según el tipo de dispositivos , la confidencialidad de la información que se maneje y el software del dispositivo					
Definir una política de seguridad de la información para dispositivos móviles	Política de seguridad la información de dispositivos móviles aprobada, formalizada, difundida e implementada			X	
Realizar un inventario de las vulnerabilidades y amenazas de seguridad de los dispositivos móviles y las aplicaciones usadas y evaluar sus riesgos en función del impacto y la frecuencia de la materialización de dichos riesgos	Riesgo de aplicaciones y dispositivos se encuentran identificados, evaluados y tratados			X	
Establecer controles que permitan mitigar los riesgos y garanticen el cumplimiento de los requerimientos de seguridad definidos en las políticas					

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Realizar campañas de capacitación sobre las políticas de seguridad que se usan, sobre la forma que se sigue para detectar, reportar, responder y recuperarse de los incidentes y sobre las acciones recomendadas para controlar los ataques cibernéticos o escenarios de riesgo	Usuarios se encuentran capacitados en las amenazas a dispositivos móviles y los procedimientos de seguridad para dispositivos móviles			X	
Evaluar el resultado de las capacitaciones para comprobar si esta tuvo éxito					
Realizar campañas de concientización sobre las políticas de seguridad que se usan, sobre las responsabilidades de seguridad al momento de usar los dispositivos móviles por parte de los usuarios y sobre las amenazas a los dispositivos móviles y el comportamiento de las mismas	Usuarios son conscientes de las políticas y responsabilidades en el manejo de los dispositivos móviles y aplicaciones			X	
Establecer múltiples métodos de autenticación para poder acceder a la información por medio de dispositivos móviles y un proceso para firmar digitalmente un correo para asegurar la integridad del mismo y poder comprobar la identidad del que lo envía	Mecanismos de autenticación y seguridad para dispositivos móviles se encuentran establecidos			X	
Encriptar los datos almacenados en los dispositivos móviles y los datos transmitidos por estos	Datos almacenados y transmitidos se encuentran protegidos			X	
Identificar y segregar las interfaces de red para comunicaciones internas y externas y usar software de administración de redes para monitorear y gestionar las interfaces de red	Interfaces de red se encuentran administradas			X	
Implementar tecnologías para administrar la seguridad de los dispositivos móviles de manera centralizada para poder borrar la información o bloquear un dispositivo móvil de manera remota	Tecnologías para la administración centralizada de los dispositivos móviles esta implementada			X	

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Establecer controles de seguridad en función de la políticas establecidas y configurar los dispositivos que usen Bluetooth con el modo de seguridad de Bluetooth más fuerte con el que disponen	Dispositivo móviles entregados por la organización están completamente asegurados			X	
Establecer controles de seguridad suplementarios como antivirus y tecnologías para la prevención de perdida de datos					
Establecer un proceso de saneamiento que permita borrar la información de los dispositivos móviles según el tipo de dispositivo y la información contenida, además establecer un proceso de verificación que permita comprobar el adecuado saneamiento de un dispositivo móvil	Ciclo de vida de las aplicaciones y dispositivos móviles están administrados			X	
Tener documentado y actualizado un registro sobre el comportamiento de las aplicaciones, sus manuales de usuario y de las anomalías detectadas	Comportamiento del código y anomalías esta administrado			X	
Monitorear la presencia de anomalías en los dispositivos móviles y la ocurrencia de incidentes de seguridad de los dispositivos móviles a través de software de detección de intrusos u otro software de monitoreo	Seguridad de los dispositivos móviles se encuentra monitoreada			X	
Monitorear y reportar cuando una violación de las políticas, procedimientos establecidos de respuesta, recuperación y comunicación de incidentes ocurre	Políticas, procesos y procedimientos están monitoreados			X	
Definir una estrategia y elaborar un plan para la respuesta a los incidentes y una guía para priorizar la respuesta a incidentes, además definir procedimientos para responder cuando se materialice un incidente	Plan de respuesta durante incidentes este implementado			X	

Actividades	Subcategoría	No Adecuado	Poco Adecuado	Adecuado	Observaciones
Hacer un plan de comunicación y realizar simulacros de prueba del plan de comunicación para comprobar el correcto funcionamiento de plan	Canales de comunicación para soporte y avisos están habilitados			X	
Definir una estrategia y elaborar un plan para la recuperación de los incidentes y una guía para priorizar la recuperación de incidentes, además definir procedimientos a seguir cuando se deba recuperar de un incidente	Plan de recuperación después incidentes este implementado			X	
Realizar reuniones sobre las lecciones aprendidas y usar la información de las reuniones de lecciones aprendidas para identificar y corregir las deficiencias y debilidades en las políticas, controles y procedimientos de respuesta, comunicación y recuperación de incidentes	Lecciones aprendidas de los incidentes están implementadas			X	
Realizar auditorías periódicamente para evaluar el funcionamiento de las categorías del modelo y proponer mejoras en función de los resultados de las auditorias que permitan mejorar la seguridad de los dispositivos, los procedimientos de respuesta, comunicación y recuperación de incidentes	Categorías se encuentren auditadas periódicamente			X	
Participar en comunidades o foros de la industria relevantes para mantenerse al día con las mejores prácticas y últimas vulnerabilidades y por medio de la implementación de dichas prácticas o controles cubrir las nuevas vulnerabilidades que se detecten	Las últimas actualizaciones y desarrollos tecnológicos están revisados e implementados			X	

Nombre del Experto: MANUEL TUPIA ANTICONA

Fecha de respuesta del cuestionario: **Sábado, 18 de Noviembre de 2017**

Firma del Experto: _____

Resultado del juicio experto

Sr Evaluador(a),

En función de la evaluación hecha con los cuestionarios se solicita que llene los espacios en blanco y de su resultado si el modelo de ciberseguridad para dispositivos móviles del sector empresarial propuesto es válido o no.

Resultado de los cuestionarios:

En función de los resultados del Cuestionario 1 si considera que los componentes y procesos de modelo son:

Válido (X) Inválido ( )

En función de los resultados del Cuestionario 2 si considera que los indicadores del modelo son:

Válido (X) Inválido ( )

En función de los resultados del Cuestionario 3 si considera que la guía del modelo es:

Válido (X) Inválido ( )

Resultado del Juicio Experto:

Marque si considera que el modelo diseñado es

Válido (X) Inválido ( )

Comentarios:

El modelo se encuentra correcto, se han hecho algunas observaciones a las categorías más de forma que de contenido por lo que levantadas, convierten al modelo en un instrumento válido para los fines en los que fue creado.

Nombre del Experto: MANUEL TUPIA ANTICONA

Correo: tupia.mf@pucp.edu.pe

DNI: 10279924

Especialidad: INGENIERO INFORMÁTICO

Institución: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Firma: _____

Anexo 9 – Certificado de participación en Conferencia Internacional

Datos de la Conferencia:

Lugar: Lisboa, Portugal.

Fecha: 14-16 de abril de 2018

Nombre: 11th IADIS International Conference on Information System 2018

Organización: International Asociation for Development of the Information Society

(Bruderer, Villena, Tupia, & Bruzza, 2018)

Certificado:

CERTIFICATE

Ramon Bruderer

has participated and presented the paper
"A CYBERSECURITY MODEL FOR MOBILE DEVICES AIMED AT SMES THAT USE FREELANCERS AND BYOD SCHEMES"
at the
11th IADIS International Conference on Information Systems 2018,
held in Lisbon, Portugal, 14 – 16 April, 2018

organized by
International Association for Development of the Information Society

Ana Rodrigues
Organizing Committee

Ilustración 14 – Certificado de Participación en Conferencia Internacional