

Universidad Cenfotec

Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

Creación de Modelo de Madurez en Ciberseguridad

Rodríguez Bravo, Cesar Augusto

Enero 2017

Declaratoria de Derechos de autor

©2016, Modelo de Madurez en Ciberseguridad, César Augusto Rodríguez Bravo

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento.

Dedicatoria

Esta tesis, esta meta, este sueño hecho realidad, se lo dedico a mi familia, la cual ha sido la fuerza que siempre me ha motivado a salir adelante.

En especial a mis primos Michael y Minor por ser mi ejemplo a seguir y marcarme el camino hacia el éxito.

A mi madre, por ser mi mayor inspiración, y por todos los esfuerzos y sacrificios que ha hecho por darme todo lo que soy.

A mis hermanos por todos los momentos compartidos, los consejos y sus enseñanzas.

A mi abuelo, por sus buenos consejos e historias, pero sobre todo por enseñarme a buscar soluciones creativas a los problemas y ver siempre el lado bueno de las cosas.

A mi tío Dany y Minor por compartir toda su sabiduría conmigo, porque cada conversación es un aprendizaje, pero sobre todo por ser un modelo a seguir.

A todos mis primos, primas, tíos, tías, por estar siempre ahí cuando más los necesito, y porque sus palabras de aliento y gestos de cariño han sido el soporte para seguir adelante.

Pero en especial a mi abuela “Ita” quien siempre me motivó a dar lo mejor de mí, a superarme día con día y cuyas palabras de aliento son uno de mis mayores tesoros. Este sueño, este logro es por y para ti.

Agradecimientos

En primer lugar, quiero agradecer a todos mis profesores que durante esta carrera me compartieron su valioso conocimiento y experiencia. De este grupo de profesionales, quiero resaltar mi profundo agradecimiento a mis tutores Juan Ignacio Zamora y Carlos Calvo, quienes siempre confiaron en mi trabajo y de quienes siempre tuve todo el apoyo para lograr mis objetivos… de verdad que son los mejores profesores, profesionales, tutores y amigos.

También quiero agradecer a la universidad por poner a nuestra disposición esta carrera tan emocionante y de gran relevancia a nivel mundial. En especial quiero agradecerle a María Eugenia Ucros e Ignacio Trejos por todo su apoyo e incansable trabajo durante esta carrera.

A mi amigo y colega, Carlos Arce también con quien estoy profundamente agradecido por su apoyo durante esta tesis, no solo como lector, sino también como amigo y consejero durante todo este tiempo.

A John Feezell, por ser un mentor excepcional y apoyarme durante todo este proceso.

No puedo dejar de mencionar a mis compañeros de clases, los cuales se convirtieron en mis amigos y a quienes aprecio y admiro por todo el esfuerzo durante esta maestría. De verdad que tuve la suerte de ser parte de un grupo excepcional y con quien espero seguir compartiendo en el futuro.

Y en general a todos mis amigos, compañeros, jefes, estudiantes y familiares quienes siempre me apoyaron con sus consejos y motivaciones, de verdad que ese apoyo fue vital para cumplir este sueño…..Gracias!

TABLA DE CONTENIDO

INTRODUCCIÓN 12

Reputación e imagen 13

Costos por la pérdida de datos 13

Demandas 13

Robo de información confidencial 14

Costos de investigación y remediación 14

OBJETIVOS 17

Objetivo General 17

Objetivos Específicos 17

ALCANCES Y LIMITACIONES 18

Alcances 18

Nicho de negocio: Servicios, manufactura, transportes, comercio, etc. 18

Tamaños: Grande, mediana, pequeña 18

Presupuesto: $10.000/año, $100.000/año, $1.000.000/año, etc. 18

Geografía: Global 18

Limitaciones 18

MARCO TEÓRICO 19

¿Qué es Ciberseguridad? 19

¿Qué es un Modelo de Madurez? 19

ESTADO DE LA CUESTIÓN 21

Estados de los sistemas de madurez 21

Análisis de los principales Modelos de Madurez en Ciberseguridad 21

Valoración de madurez en Ciberseguridad de Rapid 7 21

Modelo de Madurez en Seguridad de The Forrester 22
Cybersecurity Capability Maturity Model (C2M2) 22
ITScore for Security and Risk Management 23
Open information security Management Maturity Model (O-ISM3) 23
Cybersecurity Capability Maturity Model (White paper) 24
Cybersecurity Capability Maturity Model (CMM) v1.2 24
NIST Security Maturity Levels 25
DESCRIPCIÓN DEL PROBLEMA 26
Problemas Económicos 26
Problemas Gerenciales 27
Problemas Funcionales 27
Problemas de Seguridad 27
Problemas de Riesgos 27
JUSTIFICACIÓN 29
Completo 29
Fácil de implementar 29
Fácil de comprender 29
Actualizado 30
Ventajas desde el punto de vista gerencial 30
Ventajas desde el punto de vista económico 30
Ventajas desde el punto de vista técnico/operativo 31

PROPUESTA DE SOLUCIÓN 32
Áreas de evaluación del Modelo de Madurez en Ciberseguridad 32
Escala de Evaluación del Modelo (Niveles de Madurez) 37
Nivel 0 37
Nivel 1 37
Nivel 2 38
Nivel 3 38
Nivel 4 38
Modelo de Madurez en Ciberseguridad 40
D01-Políticas de Ciberseguridad 40
D01-C01– Existencia 40
D01-C02 – Diseño 41
D01-C03 – Aprobación 42
D01-C04 – Actualización 43
D01-C05 – Difusión 44
D02- Organización Interna relacionada con la Ciberseguridad 45
D02-C01 – Roles y Responsabilidades 45
D02-C02 – Segregación de Funciones 46
D02-C03 – Comunicaciones externas 47
D02-C04 – Ciberseguridad en la gestión de proyectos 48
D02-C05 – Política sobre el uso de dispositivos móviles 49
D02-C06 – Política sobre el Teletrabajo 50
D03 – Ciberseguridad y el recurso humano 51
D03-C01 – Términos y condiciones 51
D03-C02 – Procesos Disciplinarios 52
D03-C03 – Campañas de concientización en Ciberseguridad 53
D04 – Manejo de Activos 54

D04-C01 – Inventarios de TI 54
D04-C02 – Política sobre uso y devolución de activos 55
D04-C03 – Política de reutilización de activos 56
D04-C04 – Clasificación, Etiquetado y Manejo de la información 57
D04-C05 – Política de almacenamiento seguro de los datos 58
D04-C06 – Controles para el almacenamiento seguro de los datos 59
D04-C07 – Política de destrucción de información 60
D05 – Control de Accesos 61
D05-C01 – Política de control de accesos 61
D05-C02 – Registros de control de acceso físico y lógico 62
D05-C03 – Procesos de control de acceso a usuarios 63
D05-C04 – Sistemas y procedimientos para la administración de identidades de usuario (IAM) 64
D05-C05 – Política sobre contraseñas 65
D05-C06 – Sistemas de gestión y comprobación de contraseñas 66
D06 - Criptografía 67
D06-C01 – Política sobre criptografía 67
D07 – Seguridad Física y Ambiental 68
D07-C01 – Controles de acceso físico 68
D07-C02 – Evaluación de Amenazas físicas y ambientales a los equipos de TI 69
D08 – Ciberseguridad en las operaciones de la empresa 70
D08-C01 – Gestión de Cambios en TI 70
D08-C02 – Gestión de Riesgos en TI 71
D08-C03 – Segregación de Ambientes de TI 72
D08-C04 – Controles contra Ciber-Amenazas activas (virus, malware, SPAM, etc.) 73
D08-C05 – Controles contra Ciber Ataques (DDOS, intrusiones, hackeos, ingeniería social, phishing, etc) 74
D08-C06 – Política de Respaldo de Información 75
D08-C07 – Disponibilidad de los Sistemas 76
D08-C08 – Integridad de la información 77
D08-C09 – Política de Registro de Eventos de los sistemas de TI 78

D08-C10 – Política de instalación de software en los equipos 79
D08-C11 – Política de instalación de hardware en los equipos 80
D08-C12 – Política de auditoría de Ciberseguridad 81
D09 – Seguridad en las comunicaciones 82
D09-C01 – Política de seguridad de las redes de comunicación 82
D09-C02 – Política de confidencialidad y no divulgación 83
D09-C03 – Controles de seguridad de las redes de comunicación 84
D09-C04 –Controles para la transmisión segura de los datos 85
D09-C05 – Política sobre el uso del correo y los sistemas de mensajería y colaboración 86
D10 – Sistemas de información 87
D10-C01 – Adquisición de los Sistemas de TI 87
D10-C02 – Desarrollo de los Sistemas de TI 88
D10-C03 – Mantenimiento de los Sistemas de TI 89
D11 – Relación con Proveedores: 90
D11-C01 – Controles de seguridad de la información con proveedores 90
D12 – Gestión de incidentes de Ciberseguridad 91
D12-C01 – Política de manejo de incidentes de Ciberseguridad 91
D12-C02 – Controles para el manejo de incidentes de Ciberseguridad 92
D12-C03 – Análisis de las causas de los incidentes de Ciberseguridad 93
D12-C04 – Proceso de mejora continua en Ciberseguridad 94
D12-C05 – Proceso de recolección de evidencia en incidentes de Ciberseguridad 95
D13 – Continuidad del Negocio 96
D13-C01 – Proceso de contingencia en Ciberseguridad en caso de desastres 96
D13-C02 – Redundancia en Ciberseguridad 97
D13-C03 – BCP y Ciberseguridad 98
D14 – Requerimientos Legales 99
D14-C01 – Alineamiento con Leyes locales 99
D14-C02 – Cumplimiento de regulaciones 100
D14-C03 – Política para la protección y manejo de la propiedad intelectual 101

D14-C04 – Política para la protección y manejo de los datos personales.....102
GUIA DE IMPLEMENTACION DEL MODELO.....103
Alcance.....103
Periodicidad.....103
Interpretación de resultados.....103
Por control.....103
Por Dominio.....104
Por empresa.....104
RECOMENDACIONES PARA LA IMPLEMENTACION.....105
CONCLUSIONES.....106
RECOMENDACIÓNES.....108
TRABAJOS FUTUROS.....110
BIBLIOGRAFÍA.....111
GLOSARIO.....116

Tabla de Figuras

Figura 1: Modelo Plan-DO-Check-Act (PDCA)..... 1
Figura 2: Ejemplo de presentación de datos del modelo de madurez 4

INTRODUCCIÓN

En el ámbito de la informática, a pesar de que su creación y desarrollo están dirigidos para facilitar y agilizar un gran número de operaciones, tanto empresariales como individuales; siempre existe quien o quienes distorsionen subjetivamente los propósitos originales, y encuentren la manera de sacar provecho en perjuicio de los otros. Sucede que al día de hoy, es común, encontrar dentro de las noticias, titulares sobre "Ciberataques" que afectan, tanto a empresas como a gobiernos, cuyo impacto puede llegar a ser catastrófico, al grado de que se puede llevar a una empresa a la banca rota, como le sucedió a la empresa DigiNotar (autoridad certificadora en Internet), la cual se declaró en quiebra luego de que sus certificados fueran comprometidos, lo que provocó que la compañía perdiera credibilidad y por ende a sus clientes. (Castro, R. 2011)

De igual modo, a nivel de gobierno, es de absoluto rigor que se cuenten con controles, políticas y mecanismos para evitar los Ciberataques, puesto que, la tecnología es una pieza clave para su funcionamiento. Esta por esta dependencia tecnológica de los gobiernos que un Ciberataque puede incluso provocar un conflicto armado.

Incluso, existen muchas fuentes que califican los Ciberataques como el nuevo terrorismo del siglo XXI. De esta manera ha sido expuesto en la presentación del tercer seminario sobre la lucha contra el terrorismo organizado por la UNED en España. En este seminario se señala a los Ciberataques como "una de las mayores amenazas terroristas del siglo XXI". (Europapress, 2016)

Los Estados Unidos califican a los "Ciberataques" como la amenaza más grande para su gobierno; lo anterior, según un informe del senado que indica que los "Ciberataques y el Ciberespionaje" han sustituido al terrorismo tradicional como la principal amenaza actual. (Gobierno de Brasil, 2013).

Por lo tanto surge la pregunta: ¿Cómo es posible que un ataque de este tipo cause tanto daño?. Para responder a esta pregunta, vamos a analizar algunas de

las aristas que pueden verse afectadas por un “Ciberataque” como lo son las siguientes:

Reputación e imagen

Uno de los recursos más valiosos de una empresa es sin duda su imagen y reputación. Y son precisamente estas las más vulnerables en caso de un Ciberataque. Y aunque a veces es difícil cuantificar este impacto, existen algunos reportes que dan una idea de lo costoso que puede ser el efecto de un Ciberataque para una organización, el cual podría variar desde los $184 millones hasta $332 millones, dependiendo del tipo de información comprometida. (Excelsior College, 2016).

Costos por la pérdida de datos

Líderes en el área de Ciberseguridad estiman que, en promedio, las grandes empresas atacadas han reflejado costos de hasta 4 millones de dólares por recuperación de los datos (IBM, 2016). No obstante, en esta cifra no se incluye el *Ransomware,* el cual les pone un precio a los datos secuestrados, y los daños del uso de este *Malware* se estiman en 1 billón de dólares al año (Palmer, D. 2016).

Demandas

En algunos casos, las empresas han sido condenadas a pagar montos millonarios para indemnizar a sus clientes, producto de un Ciberataque, como es el caso de la empresa Target, para la cual se estima que el costo por acciones legales debido al robo de información de más de 40 millones de tarjetas de crédito de sus clientes puede llegar a $1 Billón de dólares (Warwick, A., 2015). Asimismo, la empresa Adobe, tiene que pagar $1 millón de dólares en compensación por un caso similar al sufrido por Target. (Dark Reading, 2016).

Robo de información confidencial

Sin duda alguna, uno de los recursos más valiosos de una empresa son sus secretos comerciales y su propiedad intelectual. Por ejemplo, se dice que la receta de la coca cola es uno de los secretos de negocios mejor guardados de la historia con un costo de millones de dólares, información que muchos hackers desearían poder obtener. Dicha receta aparentemente fue puesta a la venta en internet por 15 millones de dólares de acuerdo a una publicación del periódico británico Daily Mail. (RT New, 2013).

De igual manera existe el peligro del robo de propiedad intelectual, el cual permite a terceros fabricar imitaciones de productos (posiblemente más baratas), para lograr que las ventas del producto original sufran un descenso y por ende los ingresos de las compañías productoras también.

Costos de investigación y remediación

Las empresas se ven en la necesidad de invertir en costos asociados a la investigación y remediación (post mortem) y la calidad de estos dependerá mucho del monto con el que se cuente. Por ejemplo, en el ciberataque en contra de la empresa Sony del año 2014, se estima que alcanzó un costo por encima de los 35 millones de dólares en investigación y remediación (Hornyak, T., 2015).

No es de extrañar que, ante estas amenazas, algunas empresas líderes de diferentes industrias e incluso gobiernos, hayan decidido incrementar su presupuesto para reducir el riesgo ante estos “Ciberataques”. Es así como el presupuesto en Ciberseguridad del Gobierno de Estados Unidos para el 2017 creció a 19 mil millones de dólares (Netmedia. 2016).

Una de las mayores dificultades que enfrenta el jefe de seguridad de la información (CISO por sus siglas en ingles), es lograr justificar el presupuesto, ya que normalmente TI interno se ve como un gasto (no genera ingresos) y por lo tanto, tiene presupuestos muy bajos, lo que provoca que los recursos para Ciberseguridad sean aún más limitados.

Ante estas limitantes, es imperativo que el presupuesto sea ejecutado de la mejor manera para maximizar su retorno de la inversión (ROI) y tratar de reducir los riesgos al máximo. Para esto el CISO necesita tener un modelo que permita esta maximización de recursos, donde el modelo Plan-DO-Check-Act (PDCA) puede ser de gran utilidad como lo menciona el gobierno de los Estados Unidos (Us-cert.gov. 2013). De hecho, este modelo es ampliamente utilizado en la implementación del ISO 27001 y 27002 (Fedco, 2015).



Figura 1 - Modelo Plan-DO-Check-Act (PDCA)

Fuente:
https://en.wikipedia.org/wiki/Information_security_management_system#/media/File:Risk_Management_Elements.jpg

Con base en este modelo, lo primero a realizar es “Estructurar” un plan; en el que se han de crean todas las políticas, objetivos, procesos, procedimientos y controles de Ciberseguridad. El segundo paso es “Hacer”, sin embargo, el concepto correcto podría ser más bien “Implementar” los controles, políticas, procesos y procedimientos que se habrían definido en el paso anterior. Y el tercer paso es “Revisar” que los procesos, políticas, controles y procedimientos se hayan

implementado de la mejor manera y que se les siga utilizando o que se les dé el seguimiento correspondiente. Por último, es necesario el “Actuar”, el cual, se puede definir como un paso hacia la mejora continua, que incluye revisar la efectividad y la toma de medidas para garantizar la mejora continua del modelo.

Un factor vital para una eficaz implementación de este modelo de Ciberseguridad es contar con una herramienta de medición que permita responder a las siguientes interrogantes:

¿Cómo está la empresa a nivel de Ciberseguridad?

¿A qué nivel de Ciberseguridad quiere llegar la empresa?

¿Cuáles son los requisitos para medir la posibilidad de avanzar entre el estado actual y el estado futuro deseado?

En busca de responder las anteriores interrogantes se propone la creación de un modelo de “Madurez en Ciberseguridad” que le permita a toda empresa y /o institución contar con las posibilidades de:

- Determinar el estado actual real en materia de “Ciberseguridad”, basado en estándares internacionales.
- Identificar los diferentes niveles de “Madurez en Ciberseguridad” que sirvan como instrumento de medición.
- Conocer los controles, políticas, procesos y procedimientos globales aplicables en Ciberseguridad.
- Definir los controles, políticas, procesos y procedimientos requeridos para mejorar el nivel de Ciberseguridad de la empresa.
- Visualizar el esfuerzo requerido para mejorar la Ciberseguridad.
- Identificar las fortalezas y debilidades en Ciberseguridad.
- Crear conciencia sobre el nivel de exposición de riesgo actual en Ciberseguridad.

OBJETIVOS

Objetivo General

Diseñar un Modelo de Madurez en Ciberseguridad aplicable para todo tipo de organización o empresas sin importar el tamaño o sector.

Objetivos Específicos

1. Analizar los principales Modelos de Madurez en Ciberseguridad.
2. Seleccionar las áreas de evaluación del Modelo de madurez.
3. Definir la escala de resultados del Modelo de madurez.
4. Desarrollar un Modelo de madurez en Ciberseguridad para empresas de cualquier tamaño y sector.
5. Crear una guía de implementación del Modelo de madurez en Ciberseguridad.

ALCANCES Y LIMITACIONES

Alcances

Este modelo está diseñado para ser utilizado por cualquier organización o empresa, indiferentemente de cuales sean sus características; entre ellas podemos citar:

Nicho de negocio: Servicios, manufactura, transportes, comercio, etc.

Tamaños: Grande, mediana, pequeña

Presupuesto: $10.000/año, $100.000/año, $1.000.000/año, etc.

Geografía*:* Global

Limitaciones

Toda investigación o propuesta en algún aspecto presenta limitantes, las que pueden presentarse precisamente por la naturaleza de la misma o por el contexto en el que se aplica. En este caso en particular, este modelo toma en cuenta los aspectos generales a evaluar en el área de Ciberseguridad, no obstante, a las empresas que brindan servicios de TI y en especial en el área de Ciberseguridad, se les recomienda utilizar controles más extensos y desarrollados a la medida con base a las necesidades y requisitos de sus clientes, así como al tipo de información que manejan.

MARCO TEÓRICO

¿Qué es Ciberseguridad?

Existen diferentes definiciones de lo que se entiende por Ciberseguridad, pero, la más acertada para fines de esta tesis es la que la define como: "*Una Parte de la seguridad de la información que se encarga de la protección de la infraestructura computacional, su entorno y todos los datos que circulen o sean procesados por la misma" (CertSuperior, 2016).*

De esta definición se infiere que la seguridad de la información engloba un dominio más amplio que la Ciberseguridad, y esto es correcto, ya que la seguridad de la información, aparte de la Ciberseguridad, también toma en cuenta otros aspectos como lo son la información escrita, verbal y todos los posibles estados y/o formas que estas puedan tener.

¿Qué es un Modelo de Madurez?

También se le conoce como "Modelo de Madurez de Capacidades", y se puede definir como un modelo de evaluación de procesos de una organización *(Carnegie Mellon University. 1993).* Inicialmente fue desarrollado para los procesos relativos al desarrollo e implementación de software, no obstante, su popularidad ha crecido debido a su importantísimo valor para la alta gerencia, al punto de que se ha empezado a utilizar como un "benchmark" para medir otros procesos críticos de la empresa.

Empresas líderes en consultoría a nivel mundial como Deloitte han creado sus propios modelos de madurez en diferentes áreas como lo son:

1. Modelo de madurez en sostenibilidad (Deloitte. 2016).
2. Modelo de madurez de talento (Recursos Humanos) (Deloitte. 2016).

3. Modelo de madurez en procesos financieros (Deloitte. 2016).

Otros líderes de la industria como Microsoft, también soportan el desarrollo de dichos modelos de madurez, como por ejemplo el “Modelo de Madurez en Administración de Proyectos” (Microsoft. 2016). Incluso existe un modelo de “Inmadurez” creado por Anthony Finkelstein que se refiere a las organizaciones que ni siquiera tienen el nivel cero de madurez y más bien tienden a presentar notas negativas (Finkelstein. A. 2016).

ESTADO DE LA CUESTIÓN

Estados de los sistemas de madurez

A pesar de que el primer Modelo de Madurez (CMM por sus siglas en inglés) salió hace más de 20 años, ha sido hasta hace unos años que estos han crecido en popularidad y cada vez son más aceptados por diferentes industrias.

Este apogeo puede ser en gran medida a la gran cantidad de ventajas que la empresa u organización puede obtener basado en sus resultados. Sin embargo, frecuentemente se critica a los modelos de madurez por su nivel de complejidad y el esfuerzo requerido para su correcta implementación.

Por otra parte, los técnicos se quejan a menudo de la enorme carga de "papeleo" que impone el modelo, lo cual consideran más como un mecanismo de control por parte de la dirección, que una herramienta que les ayude en su trabajo.

A continuación, se analizan algunos de los modelos de madurez de Ciberseguridad más conocidos:

Análisis de los principales Modelos de Madurez en Ciberseguridad

Valoración de madurez en Ciberseguridad de Rapid 7

La compañía Rapid7 ofrece un servicio de evaluación de la situación actual de la empresa, en cuanto a Ciberseguridad, junto con un análisis de las vulnerabilidades y recomendaciones (Rapid 7, 2016). Este es un servicio a la medida para cada empresa en particular, por lo que no se puede considerar como un Modelo de Madurez en Ciberseguridad.

Entre las desventajas de este modelo se pueden mencionar las siguientes:

- No es considerado un modelo, ya que es un servicio pago y cerrado.

- No puede ser implementado por la propia empresa, ya que solo Rapid7 lo puede implementar.
- El modelo no está disponible para descargar, por lo que no se pueden conocer las áreas que evalúa ni el nivel de profundidad.
- Al no ser un modelo abierto, se pierde de valiosos aportes potenciales de expertos en el área de Ciberseguridad.
- Al ser un modelo cerrado y exclusivo para clientes, no es posible obtener información sobre implementaciones previas y criticas de expertos.
- Según la información disponible en la página web, su enfoque es principalmente en la evaluación de los programas de seguridad de la empresa y no en un modelo que abarque de manera integral todos los aspectos relacionados a la Ciberseguridad de la empresa.

Modelo de Madurez en Seguridad de The Forrester

La empresa The Forrester ofrece un modelo de madurez a sus clientes, el cual tiene un costo de $499. (Forrester, 2014). Entre las desventajas de este modelo se anotan las siguientes:

- El modelo no está disponible para descargar, por lo que no se puede conocer las áreas que evalúa ni el nivel de profundidad.
- Al no ser un modelo abierto, se pierde de valiosos aportes potenciales de expertos en el área de Ciberseguridad.
- Al ser un modelo cerrado y exclusivo para clientes, no es posible obtener información sobre implementaciones previas y criticas de expertos.

Cybersecurity Capability Maturity Model (C2M2)

Este modelo fue diseñado por el gobierno de los Estados Unidos con el fin de que pueda ser usado por cualquier compañía para conocer sus capacidades en el área de Ciberseguridad (Energy.gov. 2014). Entre las desventajas de este modelo se encuentran:

- Solamente define 3 niveles, lo cual hace el ámbito de cada nivel muy amplio, lo cual puede llevar a una empresa a crear falsos supuestos.
- No contempla temas claves como las políticas de la empresa.
- Es muy enfocado en el tema de riesgos.
- Los criterios usados en cada nivel son muy genéricos y carecen de detalles técnicos vitales durante su implementación.
- El modelo no presenta actualizaciones desde el 2014, lo cual en un ambiente tan variable como lo es la Ciberseguridad es suficiente para ser considerado como desactualizado.

ITScore for Security and Risk Management

El modelo ITScore, busca conocer el estado de madurez de los proyectos y programas de IT. Sin embargo, este no es un modelo definido, ya que no identifica claramente las diferencias entre niveles, ni como subir/bajar entre ellos (Gartner, 2014).

Open information security Management Maturity Model (O-ISM3)

La página lo define como un Framework para el manejo de la seguridad de la información que busca asegurar que los procesos de seguridad estén alineados con los requerimientos del negocio (Open Group, 2011). Entre las desventajas de este modelo se encuentran:

- El modelo no presenta actualizaciones desde el 2011, lo cual en un ambiente tan variable como lo es la Ciberseguridad es suficiente para ser considerado como desactualizado.
- Solo está disponible para miembros de The Open Group o comprando la publicación escrita.
- El documento es sumamente complejo y difícil de implementar aun para una persona con experiencia en Ciberseguridad.
- No cuenta con una guía clara de implementación.

- El documento se parece más a una guía de buenas prácticas que a un modelo de medición de madurez en Ciberseguridad.

Cybersecurity Capability Maturity Model (White paper)

Más que un modelo, es un artículo creado con el fin de crear conciencia sobre la necesidad de que las empresas evalúen su estado actual en Ciberseguridad. Si bien el documento menciona algunas propuestas, este deja abierto el tema para una discusión entre gobierno y empresa para fortalecer el tema de Ciberseguridad, lo que implica en primera instancian el conocimiento del estado actual de Ciberseguridad de la empresa. Vale destacar que este artículo fue publicado por el departamento de Home Land Security del gobierno de los Estados Unidos (US Gob., 2014).

Cybersecurity Capability Maturity Model (CMM) v1.2

Este modelo de madurez es bastante amplio y detallado, lo cual puede hacer difícil su implementación (Oxford, 2014). Entre las desventajas de este modelo se mencionan las siguientes:

- El modelo completo es muy extenso y puede complicar/encarecer su implementación.
- No cuenta con guías claras para determinar cuáles dimensiones (así es como ellos llaman a sus grupos de procesos) son obligatorias y cuales opcionales.
- Tampoco cuenta con reglas claras de implementación ni cómo interpretar resultados.
- No cuenta con un “score” global para conocer el estado global de la empresa en materia de Ciberseguridad.
- El modelo no presenta actualizaciones desde el 2014, lo cual en un ambiente tan variable como lo es la Ciberseguridad es suficiente para ser considerado como desactualizado.

NIST Security Maturity Levels

El NIST define 5 niveles de madurez, sin embargo, estos niveles son más una especie de secciones a evaluar. Además, esto no es un modelo de madurez y solamente constituye una guía de posibles niveles a revisar en cuanto a la madurez en seguridad (NIST. 2014). Entre las desventajas de este modelo se encuentran:

- El documento solo menciona los elementos de evaluación de la medición.
- El documento es apenas una página.
- No cuenta con las secciones ni detalles de lo que se va a evaluar.

DESCRIPCIÓN DEL PROBLEMA

Los “Modelos de Madurez” son una herramienta fundamental para que las empresas reconozcan su realidad actual, identifiquen sus fortalezas y áreas de oportunidad para así centrar sus esfuerzos estratégicamente en las áreas que más lo necesitan (alineadas con la estrategia del negocio). Originalmente fueron creados para evaluar los procesos relativos al desarrollo e implementación de software, sin embargo, la evolución tecnológica y la necesidad intrínseca de asegurar los sistemas de información, han hecho que sea necesario contar con un modelo de madurez orientado hacia la seguridad de la información.

Actualmente este es un tema bastante nuevo y si bien es cierto que ya existen algunos modelos de madurez en Ciberseguridad, todos han tenido problemas de implementación, lo que no ha permitido que ninguno haya despegado como el estándar en el tema. Esta falta de un estándar global de fácil implementación ha provocado que la mayoría de las empresas no conozcan su estado de madurez en Ciberseguridad, lo que provoca un desconocimiento del estado actual, real y global de la empresa, desde un punto de vista integral, o sea, tomando en cuentas todas las aristas involucradas. Esta falta de conocimiento puede generar muchos problemas tanto económicos, gerenciales, funcionales y de seguridad, así como también una alta exposición a riesgos.

Problemas Económicos

- Perdida de reputación en caso de un ataque o filtración de información.
- Perdida de información confidencial.
- Robo de información confidencial.
- Ataques a la disponibilidad de equipos o información crítica.
- Caída de equipos o información crítica de la empresa.
- Costos de recuperación ante un ataque o incidente.
- Costos asociados con la gestión de riesgos de IT.
- Costos asociados a la Ciberseguridad de la empresa.

- Costos asociados a pruebas de penetración.
- Costos asociados a la mala planeación de presupuestos en Ciberseguridad.

Problemas Gerenciales

- Falta de información para la toma de decisiones en cuanto Ciberseguridad.
- Falta de información para respaldar las inversiones en Ciberseguridad.
- Falta de información para crear presupuestos relacionados a Ciberseguridad.
- Falta de información para la gerencia de riesgos en Ciberseguridad

Problemas Funcionales

- Desconocimiento de las políticas sobre Ciberseguridad.
- Desconocimiento de los controles sobre Ciberseguridad.
- Desconocimiento de los métodos y alcances de divulgación de las políticas y controles sobre Ciberseguridad.
- Descoordinación de los esfuerzos de entrenamiento en Ciberseguridad.
- Desconocimiento de los roles y responsabilidades asociadas a la Ciberseguridad.

Problemas de Seguridad

- Falta de controles.
- Duplicación de controles.
- Falta de políticas.
- Falta de apoyo de la alta gerencia.
- Duplicación de esfuerzos.
- Falta de entrenamiento.

Problemas de Riesgos

- Desconocimiento de riesgos en el área de Ciberseguridad.
- Falta de planes de mitigación.

- Duplicación de planes de mitigación.
- Aumento en la exposición de riesgos.
- Aumento de la probabilidad del riesgo.
- Aumento del impacto del riesgo.

JUSTIFICACIÓN

Está propuesta pretende responder a la urgencia de contrarrestar los riesgos en Ciberseguridad que se ha venido presentando y que afecta a la todas las empresas, industrias y organizaciones. Por tal razón se propone el diseño y creación del Modelo de Madurez en Ciberseguridad, el cual estará estructurado para que cumpla con las siguientes características:

Completo

El modelo debe de contar con un esquema definido. Áreas de estudio definidas, así como también con sus escalas definidas y explicadas.

Fácil de implementar

El modelo debe de ser sencillo para que una persona con experiencia en TI de la empresa sea capaz de implementar el modelo y hacer la evaluación de la empresa.

Fácil de comprender

Un modelo de madurez, no se hace para cumplir, se hace para conocer a fondo a la empresa y por eso es vital que las personas encargadas de implementarlo, lo comprendan a cabalidad.

Además, debe de ser una herramienta de comunicación para usar con la alta gerencia y que permita ver de forma clara la situación real de la empresa, en cuanto a Ciberseguridad en un lenguaje claro, y sin tener que entrar en tecnicismos que pueden complicar la comunicación.

Actualizado

En un ambiente tan cambiante como lo es el mundo de IT, es imperativo que el modelo sea actualizado para que contemple todos los nuevos factores que puedan afectar el modelo.

Otro de los graves problemas es que las implementaciones de modelos propietarios son muy costosas, lo que provoca que algunas empresas medianas no puedan acceder a ellos y estas quedan vulnerables ante los crecientes riesgos en materia de Ciberseguridad.

Además, el modelo de Ciberseguridad presenta una serie de ventajas que proyectan resultados muy positivos para la empresa u organización que los implemente. A continuación, se enumeran algunas de esas ventajas:

Ventajas desde el punto de vista gerencial

- Permite un mejor conocimiento del estado real de la empresa en materia de Ciberseguridad.
- Permite conocer las mejores prácticas en materia de Ciberseguridad.
- Permite hacer un “benchmark” con otras empresas.
- Ayuda a identificar riesgos asociados con la Ciberseguridad de la empresa.
- Ayuda a dar visibilidad a los riesgos a los que está expuesta la empresa en Ciberseguridad.
- Ayuda a soportar la inversión en temas de Ciberseguridad.

Ventajas desde el punto de vista económico

- Ayuda en la elaboración de presupuestos en Ciberseguridad
- Ayuda a identificar las áreas prioritarias en Ciberseguridad
- Ayuda en la reducción de costos asociados con riesgos en Ciberseguridad.
- Permite identificar las áreas prioritarias para inversión en Ciberseguridad
- Ayuda en la creación de un ROI de las iniciativas en Ciberseguridad.

Ventajas desde el punto de vista técnico/operativo

- Permite enfocar los recursos de TI más eficientemente
- Ayuda como una guía para conocer las áreas prioritarias a trabajar en temas de Ciberseguridad.
- Ayuda a evitar el “desperdicio de recursos de TI” en tareas con menos impacto.
- Ayuda a crear una visión más clara sobre el enfoque en Ciberseguridad.
- Ayuda a promover una cultura basada en Ciberseguridad

PROPUESTA DE SOLUCIÓN

Áreas de evaluación del Modelo de Madurez en Ciberseguridad

En este apartado se enumeran las áreas de evaluación que se van a utilizar en esta propuesta de modelo de madurez. Estas áreas de evaluación están basadas en los 14 dominios, 35 Objetivos y 114 controles del Sistema de Gestión de la Seguridad de la Información (SGSI) la ISO 27002, el cual es un estándar bastante robusto y aceptado en la industria. Sobre esa base se han creado 63 controles a evaluar los cuales están organizados en 14 dominios. Cada control constituye un área en particular a evaluar en el tema de Ciberseguridad, mientras que los dominios pretenden organizar estos controles de manera que la implementación del modelo sea más ordenada. Adicionalmente, los dominios permiten visualizar los resultados de una forma más estructurada. A continuación el detalle:

Dominio 01 - Políticas de Ciberseguridad
Control 01 – Existencia
Control 02 – Diseño
Control 03 – Aprobación
Control 04 – Actualización
Control 05 – Difusión

Dominio 02 - Organización Interna relacionada con la Ciberseguridad
Control 01 - Roles y Responsabilidades
Control 02 - Segregación de Funciones
Control 03 - Comunicaciones externas
Control 04 - Ciberseguridad en la gestión de proyectos
Control 05 - Política sobre el uso de dispositivos móviles
Control 06 - Política sobre el Teletrabajo

Dominio 03 - Ciberseguridad y el recurso humano
Control 01 - Términos y condiciones
Control 02 - Procesos Disciplinarios
Control 03 - Campañas de concientización en Ciberseguridad

Dominio 04 - Manejo de Activos
Control 01 - Inventarios de TI
Control 02 - Política sobre uso y devolución de activos
Control 03 - Política de reutilización de activos
Control 04 - Clasificación, Etiquetado y Manejo de la información
Control 05 - Política de almacenamiento seguro de los datos
Control 06 - Controles para el almacenamiento seguro de los datos
Control 07 - Política de destrucción de información

Dominio 05 - Control de Accesos
Control 01 - Política de control de accesos
Control 02 - Registros de control de acceso físico y lógico
Control 03 - Procesos de control de acceso a usuarios
Control 04 - Sistemas y procedimientos para la administración de identidades de usuario (IAM)
Control 05 - Política sobre contraseñas
Control 06 - Sistemas de gestión y comprobación de contraseñas

Dominio 06 - Criptografía
Control 01 - Política sobre criptografía

Dominio 07 - Seguridad Física y Ambiental
Control 01 - Controles de acceso físico
Control 02 - Evaluación de Amenazas físicas y ambientales a los equipos de TI

Dominio 08 - Ciberseguridad en las operaciones de la empresa
Control 01 - Gestión de Cambios en TI
Control 02 - Gestión de Riesgos en TI
Control 03 - Segregación de Ambientes de TI
Control 04 - Controles contra Ciber-Amenazas activas (virus, malware, SPAM, etc.)
Control 05 - Controles contra Ciber Ataques (DDOS, intrusiones, hackeos, ingeniería social, phishing, etc.)
Control 06 - Política de Respaldo de Información
Control 07 - Disponibilidad de los Sistemas
Control 08 - Integridad de la información
Control 09 - Política de Registro de Eventos de los sistemas de TI
Control 10 - Política de instalación de software en los equipos
Control 11 - Política de instalación de hardware en los equipos
Control 11 - Política de auditoría de Ciberseguridad

Dominio 09 - Seguridad en las comunicaciones
Control 01 - Política de seguridad de las redes de comunicación
Control 02 - Política de confidencialidad y no divulgación
Control 03 - Controles de seguridad de las redes de comunicación
Control 04 - Controles para la transmisión segura de los datos
Control 05 - Política sobre el uso del correo y los sistemas de mensajería y colaboración

Dominio 10 - Sistemas de información
Control 01 - Adquisición de los Sistemas de TI
Control 02 - Desarrollo de los Sistemas de TI
Control 03 - Mantenimiento de los Sistemas de TI

Dominio 11 - Relación con Proveedores
Control 01 - Controles de seguridad de la información con proveedores

Dominio 12 - Gestión de incidentes de Ciberseguridad
Control 01 - Política de manejo de incidentes de Ciberseguridad
Control 02 - Controles para el manejo de incidentes de Ciberseguridad
Control 03 - Análisis de las causas de los incidentes de Ciberseguridad
Control 04 - Proceso de mejora continua en Ciberseguridad
Control 05 - Proceso de recolección de evidencia en incidentes de Ciberseguridad

Dominio 13 - Continuidad del Negocio
Control 01 - Proceso de contingencia en Ciberseguridad en caso de desastres
Control 02 - Redundancia en Ciberseguridad
Control 03 - BCP y Ciberseguridad

Dominio 14 - Requerimientos Legales
Control 01 - Alineamiento con Leyes locales
Control 02 - Cumplimiento de regulaciones
Control 03 - Política para la protección y manejo de la propiedad intelectual
Control 04 - Política para la protección y manejo de los datos personales

Escala de Evaluación del Modelo (Niveles de Madurez)

Para evaluar cada una de las secciones del modelo, se utilizan 5 niveles que van del 0 al 4. La siguiente es la definición de cada nivel:

Nivel 0

- Este es el nivel de madurez más bajo y se utiliza cuando la evidencia sobre el control, la política o el proceso es inexistente.
- Se utiliza también en casos donde la empresa tiene desconocimiento del tema y por lo tanto, no aplica ningún control, política o proceso.
- El factor de riesgo en las secciones con este nivel de madurez es **Muy Alto,** ya que la empresa es altamente vulnerable.
- Se recomienda que la empresa le asigne la mayor prioridad al proyecto requerido para implementar dichos controles y reducir la exposición a los riesgos

Nivel 1

- En este nivel hay evidencia de que se están creando los controles, políticas o procesos necesarios, pero aún no han sido completados.
- El factor de riesgo en las secciones con este nivel de madurez es **Alto,** ya que mientras estos controles no se completen, la empresa sigue siendo vulnerable.
- Se recomienda que la empresa le dé prioridad al proyecto requerido para terminar la implementación dichos controles y reducir la exposición a los riesgos.

Nivel 2

- En este nivel la empresa cuenta con los controles, políticas y/o procesos requeridos. Sin embargo, no hay evidencia de que estos se estén aplicando correctamente.
- El factor de riesgo en las secciones con este nivel de madurez es **Medio,** ya que mientras estos controles no se apliquen eficientemente, la empresa sigue siendo vulnerable.
- Se recomienda que la empresa trabaje en proyectos para fomentar la aplicación e implementación eficiente de dichos controles.

Nivel 3

- En este nivel, la empresa no solo cuenta con los controles, políticas y/o procesos requeridos, sino que también existe evidencia de su correcta y continua implementación.
- El factor de riesgo en las secciones con este nivel de madurez es **Bajo,** puesto que, la implementación eficiente de los controles ayuda a reducir los factores de riesgo a los que está expuesta la empresa.
- Se recomienda que la empresa continúe fomentando la aplicación y actualización de dichos controles para mantener una probabilidad de riesgos baja.

Nivel 4

- Los esfuerzos realizados por la empresa para crear, implementar y actualizar los controles, procesos y políticas, son reconocidos y/o aceptados por otras empresas (o industria) como buenas prácticas en Ciberseguridad.
- Este es el máximo nivel en el modelo y el factor de riesgo asociado es **Muy Bajo**.

- La mayor parte de los ataques son oportunistas (los hackers buscan los objetivos más fáciles), por lo tanto, empresas con este nivel son menos probables que sean atacadas.
- Se recomienda que la empresa continúe manteniendo dichas prácticas que sirva como un punto de comparación (benchmark) aceptado por la industria.



Modelo de Madurez en Ciberseguridad

D01-Políticas de Ciberseguridad

Niveles					
D01-C01– Existencia	No existen políticas sobre Ciberseguridad	Existen algunas políticas definidas en el área de Ciberseguridad	Existe una cantidad importante de políticas en el área de Ciberseguridad	Se cuenta con todas las políticas relacionadas a Ciberseguridad basado en un standard internacional.	Estas políticas son reconocidas por terceros como un estándar o “Best Practice” en la industria.

Notas:

_____

_____

_____

_____

_____

_____

_____

_____

D01-Políticas de Ciberseguridad

Niveles					
D01-C02 – Diseño	Inexistente	Una única persona es la encargada del diseño de las políticas de Ciberseguridad	Las políticas de Ciberseguridad son creadas por un grupo de expertos (internos)	Las políticas de Ciberseguridad son diseñadas por expertos, con retroalimentación de las principales organizaciones de la empresa	Las políticas de Ciberseguridad son diseñadas por expertos líderes en la industria (internos o externos), con retroalimentación de las principales organizaciones de la empresa

Notas:

_____

_____

_____

_____

_____

_____

_____

D01-Políticas de Ciberseguridad

Niveles					
D01-C03 – Aprobación	Las políticas sobre Ciberseguridad no han sido aprobadas por la alta gerencia	Hay evidencia de un proyecto para obtener aprobación de la alta gerencia de las políticas en Ciberseguridad	La mayoría de las políticas en Ciberseguridad han sido aprobadas por la alta gerencia	Todas las políticas sobre Ciberseguridad han sido aprobadas por la alta gerencia.	El modelo de aprobación de las políticas de Ciberseguridad es reconocido por terceros como un estándar o “Best Practice” en la industria.

Notas:

D01-Políticas de Ciberseguridad

Niveles					
D01-C04 – Actualización	No existe un proceso de actualización de las políticas de Ciberseguridad	Hay evidencia de que se está trabajando en un proceso de actualización de políticas de Ciberseguridad.	Existe un proceso definido para la actualización de las políticas de Ciberseguridad	El proceso de actualización de las políticas de Ciberseguridad es conocido y seguido por los principales actores	El proceso de actualización de las políticas de Ciberseguridad es reconocido por terceros como un estándar o “Best Practice” en la industria.

Notas:

_____

_____

_____

_____

_____

_____

_____

D01-Políticas de Ciberseguridad

Niveles					
D01-C05 – Difusión	La mayoría desconoce las políticas sobre Ciberseguridad	Solo el departamento de TI conoce las políticas de Ciberseguridad	Existe un conocimiento generalizado sobre las políticas de Ciberseguridad.	Toda la empresa conoce las políticas de Ciberseguridad	Toda la empresa conoce a profundidad las políticas de Ciberseguridad, sus alcances e importancia

Notas:

_____

_____

_____

_____

_____

_____

_____

D02- Organización Interna relacionada con la Ciberseguridad

Niveles					
D02-C01 – Roles y Responsabilidades	No existen Roles y responsabilidades definidas sobre Ciberseguridad	Hay evidencia sobre la creación de Roles y Responsabilidades sobre Ciberseguridad.	Existen algunos roles y/o responsabilidades definidas sobre Ciberseguridad	Los Roles y responsabilidades sobre Ciberseguridad están claramente definidos	Los roles y responsabilidades sobre Ciberseguridad están claramente definidos y basados en un estándar internacional.

Notas:

_____

_____

_____

_____

_____

_____

_____

D02- Organización Interna relacionada con la Ciberseguridad

Niveles					
D02-C02 – Segregación de Funciones	No existe segregación de funciones	Hay evidencia de un proyecto para la segregación de funciones relacionadas con Ciberseguridad	Existe segregación de funciones en los principales roles relacionados con Ciberseguridad	La segregación de funciones se aplica en todos los roles relacionados a Ciberseguridad	La segregación de funciones se aplica en todos los roles relacionados a Ciberseguridad basado en un estándar internacional.

Notas:

_____

_____

_____

_____

_____

_____

_____

D02- Organización Interna relacionada con la Ciberseguridad

Niveles					
D02-C03 – Comunicaciones externas	No existe un proceso establecido para el manejo y difusión de comunicaciones externas sobre Ciberseguridad	Existen algunos procedimientos establecidos y aprobados para las comunicaciones externas sobre Ciberseguridad	Existe un proceso claro, definido y aprobado sobre el manejo de las comunicaciones externas sobre Ciberseguridad	Todas las personas involucradas conocen el proceso sobre el manejo de comunicaciones externas sobre Ciberseguridad.	El proceso establecido para el manejo de comunicaciones externas es reconocido por terceros como un estándar o “Best Practice” en la industria.

Notas:

_____

_____

_____

_____

_____

_____

_____

D02- Organización Interna relacionada con la Ciberseguridad

Niveles					
D02-C04 – Ciberseguridad en la gestión de proyectos	No existe evidencia de que se utilice ningún enfoque sobre Ciberseguridad en la administración de los proyectos.	La Ciberseguridad solo se analiza en algunos proyectos	Ciberseguridad es una parte opcional en la metodología de manejo de proyectos usada por la empresa.	Ciberseguridad es una parte integral y obligatoria en la metodología de manejo de proyectos usada por la empresa.	Los lineamientos en Ciberseguridad usados en la administración de proyectos son reconocidos por terceros como un “Best Practice” de la industria.

Notas:

_____

_____

_____

_____

_____

_____

_____

D02- Organización Interna relacionada con la Ciberseguridad

Niveles					
D02-C05 – Política sobre el uso de dispositivos móviles	No existe una política sobre el uso de dispositivos móviles.	La política sobre dispositivos móviles está incompleta o en proceso	Existe una política definida sobre dispositivos móviles	Existe evidencia del cumplimiento y actualización de la política sobre dispositivos móviles	La política sobre dispositivos móviles es reconocida por terceros como un estándar o “Best Practice”

Notas:

_____

_____

_____

_____

_____

_____

_____

D02- Organización Interna relacionada con la Ciberseguridad

Niveles					
D02-C06 – Política sobre el Teletrabajo	No existe una política sobre el teletrabajo	La política sobre teletrabajo está incompleta o en proceso	Existe una política definida sobre teletrabajo	Existe evidencia del cumplimiento y actualización de la política sobre teletrabajo	La política sobre teletrabajo es reconocida por terceros como un estándar o “Best Practice”

Notas:

_____

_____

_____

_____

_____

_____

_____

D03 – Ciberseguridad y el recurso humano

Niveles					
D03-C01 – Términos y condiciones	Los empleados no firman ningún addendum del contrato relacionado con la seguridad de la información.	Algunos empleados firman un addendum del contrato relacionado con la seguridad de la información	Existe un procedimiento definido en cuanto a los documentos legales que los empleados deben firmar en relación con la seguridad de la información.	Los (addendum) que firman los empleados relacionados con la seguridad de la información, están alineados con las leyes y regulaciones del país y estos son revisados y autenticados por abogados.	Los (addendum) que firman los empleados relacionados con la seguridad de la información, son reconocidos por terceros como un estándar o “Best Practice”

Notas:

_____

_____

_____

_____

_____

_____

_____

D03 – Ciberseguridad y el recurso humano

Niveles					
D03-C02 – Procesos Disciplinarios	No existen procesos disciplinarios relacionados con la Seguridad de la información.	Existen algunos procesos disciplinarios (o están en proceso) relacionados con la seguridad de la información	Existe un procedimiento definido en relacionado a los procesos disciplinarios sobre la seguridad de la información.	Existe evidencia del cumplimiento y actualización de los procedimientos disciplinarios en relaciona con la seguridad de la información	Los procesos y acciones disciplinarias relacionados con la seguridad de la información, son reconocidos por terceros como un estándar o “Best Practice”

Notas:

_____

_____

_____

_____

_____

_____

_____

D03 – Ciberseguridad y el recurso humano

Niveles					
D03-C03 – Campañas de concientización en Ciberseguridad	No se realizan campañas de concientización en Ciberseguridad	Existe evidencia de campañas de concientización asiladas en Ciberseguridad	Existe un programa dedicado a la concientización sobre Ciberseguridad	Existe un programa dedicado a la concientización sobre Ciberseguridad que cubre a toda la compañía y se actualiza constantemente	Las campañas y programas de concientización en Ciberseguridad son reconocidas por terceros como “Best Practices” en la industria.

Notas:

_____

_____

_____

_____

_____

_____

_____

D04 – Manejo de Activos

Niveles					
D04-C01 – Inventarios de TI	No se tienen inventarios de los equipos de TI	Los inventarios de equipos de TI se encuentran incompletos o desactualizados	Existe un inventario detallado de todos los equipos (HW, SW, etc.) de TI	El inventario se encuentra actualizado y los empleados son responsables de la actualización de los activos asignados.	Los sistemas y procesos de manejo de inventario de TI son reconocidos por terceros como estándares o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D04 – Manejo de Activos

Niveles					
D04-C02 – Política sobre uso y devolución de activos	No se cuenta con una política sobre el uso y devolución de activos	La política sobre el uso y devolución de activos está incompleta o en proceso de creación.	Existe una política definida sobre el uso y devolución de activos.	Existe evidencia del cumplimiento y actualización de la política de uso y devolución de activos	La política de uso y devolución de activos es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D04 – Manejo de Activos

Niveles					
D04-C03 – Política de reutilización de activos	No existe una política de reutilización de activos	La política sobre la reutilización de activos está incompleta o en proceso de creación.	Existe una política definida sobre la reutilización de activos	Existe evidencia del cumplimiento y actualización de la política de reutilización de activos	La política de uso reutilización de activos es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D04 – Manejo de Activos

Niveles					
D04-C04 – Clasificación, Etiquetado y Manejo de la información	No existe una política sobre la clasificación, manejo y etiquetado de la información de la empresa	La política sobre la clasificación, manejo y etiquetado de la información de la empresa está incompleta o en proceso de creación.	Existe una política definida sobre la clasificación, manejo y etiquetado de la información de la empresa	Existe evidencia de cumplimiento y actualización de las políticas sobre la clasificación, manejo y etiquetado de la información de la empresa	La política sobre la clasificación, manejo y etiquetado de la información de la empresa es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

D04 – Manejo de Activos

Niveles					
D04-C05 – Política de almacenamiento seguro de los datos	No existe una política sobre el almacenamiento seguro de los datos	La política de almacenamiento seguro de los datos está incompleta o en proceso de creación.	Existe una política definida sobre el almacenamiento seguro de los datos	Existe evidencia de cumplimiento y actualización de la política sobre el almacenamiento seguro de los datos	La política sobre el almacenamiento seguro de los datos es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D04 – Manejo de Activos

Niveles					
D04-C06 – Controles para el almacenamiento seguro de los datos	No existen controles (herramientas) para garantizar el almacenamiento seguro de los datos	Existen algunos controles (herramientas) para garantizar el almacenamiento seguro de los datos	La empresa cuenta con controles (herramientas) efectivas para garantizar el almacenamiento seguro de los datos	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para garantizar el almacenamiento seguro de los datos	Los controles (herramientas) utilizados para garantizar el almacenamiento seguro de los datos, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

D04 – Manejo de Activos

Niveles					
D04-C07 – Política de destrucción de información	No existe una política sobre la destrucción de información de la empresa	La política de destrucción de información de la empresa está incompleta o en proceso de creación.	Existe una política definida sobre la destrucción de información de la empresa	Existe evidencia de cumplimiento y actualización de las políticas sobre la destrucción de información de la empresa	La política sobre la destrucción de información de la empresa es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D05 – Control de Accesos

Niveles					
D05-C01 – Política de control de accesos	No existe una política de control de accesos físicos y lógicos	La política de control de accesos físicos y lógicos está incompleta o en proceso de creación.	Existe una política definida sobre el control de acceso físico y lógico	Existe evidencia de cumplimiento y actualización de las políticas sobre el control de accesos físicos y lógicos	La política sobre el control de accesos físicos y lógicos es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D05 – Control de Accesos

Niveles					
D05-C02 – Registros de control de acceso físico y lógico	No se guardan registros sobre los accesos físicos y lógicos a los sistemas de TI	Solo se guardan algunos registros de accesos físicos y/o lógicos a los sistemas de TI	Se cuenta con registros de control de accesos lógicos y físicos a todos los sistemas de TI	Se cuenta con respaldos de los registros de control de accesos lógicos y físicos de todos los sistemas de TI	Los sistemas y procedimientos de registro de control de acceso físico y lógico son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D05 – Control de Accesos

Niveles					
D05-C03 – Procesos de control de acceso a usuarios	No existen procesos establecidos para el control de acceso a usuarios.	Existen algunos procedimientos de control de acceso a usuarios.	La empresa cuenta con todos los procesos de control de accesos a usuarios definidos	Existe evidencia del cumplimiento y actualización de los procesos de control de acceso a usuarios	Los sistemas y procesos de control de accesos a usuarios son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D05 – Control de Accesos

Niveles					
D05-C04 – Sistemas y procedimientos para la administración de identidades de usuario (IAM)	No existen sistemas y/o procedimientos para la administración de identidades de usuarios	Existen algunos sistemas y/o procedimientos para la administración de identidades de usuarios	La empresa cuenta con todos los procedimientos y sistemas para la administración de identidades de usuarios	Existe evidencia del cumplimiento y actualización de los procedimientos y sistemas para la administración de identidades de usuarios	Los sistemas y procedimientos para la administración de identidades de usuarios son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D05 – Control de Accesos

Niveles					
D05-C05 – Política sobre contraseñas	No existen políticas sobre contraseñas	La política sobre contraseñas está incompleta o en proceso de creación.	Existe una política definida sobre contraseñas	Existe evidencia del cumplimiento y actualización de las políticas de contraseñas	La política de contraseña de la empresa es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

D05 – Control de Accesos

Niveles					
D05-C06 – Sistemas de gestión y comprobación de contraseñas	No existen sistemas para la gestión y/o comprobación de contraseñas	Existen algunos sistemas para la gestión y/o comprobación de contraseñas	La empresa cuenta con todos los sistemas necesarios para una adecuada gestión y comprobación de contraseñas	Existe evidencia de la utilización y actualización continua de los sistemas de gestión y comprobación de contraseñas	Los sistemas de gestión y comprobación de contraseñas de la empresa son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D06 - Criptografía

Niveles					
D06-C01 – Política sobre criptografía	No existe una política sobre criptografía	La política sobre criptografía está incompleta o en proceso de creación.	Existe una política definida sobre criptografía	Existe evidencia del cumplimiento y actualización continua de la política de criptografía	La política de criptografía de la empresa es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D07 – Seguridad Física y Ambiental

Niveles					
D07-C01 – Controles de acceso físico	No existen controles de acceso físico a la empresa	Existen algunos controles de acceso físico a la empresa	La empresa cuenta con todos los controles de acceso físico necesarios para evitar accesos no autorizados	Existe evidencia del cumplimiento y monitoreo de los controles de acceso físico a la empresa	Los controles de acceso físico a la empresa son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D07 – Seguridad Física y Ambiental

Niveles					
D07-C02 – Evaluación de Amenazas físicas y ambientales a los equipos de TI	No existe un proceso para la evaluación de las amenazas físicas y ambientales a los equipos de TI	Existen algunos procesos para la evaluación de las amenazas físicas y ambientales a los equipos de TI	La empresa cuenta con un proceso definido para evaluar las amenazas físicas y ambientales a los equipos de TI	Existe evidencia de la evaluación periódica de las amenazas físicas y ambientales a los equipos de IT	El proceso para la evaluación de las amenazas físicas y ambientales a los equipos de TI, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C01 – Gestión de Cambios en TI	No existe un proceso de gestión de cambios en TI	Existen algunos procesos de gestión de cambios de TI, pero estos están incompletos o en proceso de creación.	La empresa cuenta con un proceso documentado para la gestión de cambios de TI	Existe evidencia del cumplimiento y actualización continua del proceso de gestión de cambios en TI.	Los procesos de gestión de cambios de TI son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C02 – Gestión de Riesgos en TI	No existe un proceso de gestión de riesgos en TI	Existen algunos procesos de gestión de riesgos de TI, pero estos están incompletos o en proceso de creación.	La empresa cuenta con un proceso documentado para la gestión de riesgos de TI	Existe evidencia del cumplimiento y actualización continua del proceso de gestión de riesgos en TI.	Los procesos de gestión de riesgos de TI son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C03 – Segregación de Ambientes de TI	No existe segregación de ambientes de TI	Existe segregación en algunos ambientes de TI	Existe segregación en todos los ambientes de TI de la empresa (desarrollo, pruebas, producción, etc.)	Existe un proceso definido para revisar periódicamente que la segregación de ambientes de TI se está cumpliendo.	La segregación de ambientes de TI es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C04 – Controles contra Ciber-Amenazas activas (virus, malware, SPAM, etc.)	No existen controles (herramientas) para evitar las Ciber-Amenazas	Existen algunos controles (herramientas) para evitar las Ciber-Amenazas	La empresa cuenta con controles efectivos para evitar las Ciber-Amenazas	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para evitar las Ciber-Amenazas	Los controles (herramientas) utilizados para evitar las Ciber-Amenazas, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C05 – Controles contra Ciber Ataques (DDOS, intrusiones, hackeos, ingeniería social, phishing, etc)	No existen controles (herramientas) para evitar Ciberataques efectivamente	Existen algunos controles (herramientas) para evitar Ciberataques	La empresa cuenta con controles (herramientas) efectivas para evitar Ciberataques	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para evitar Ciberataques	Los controles (herramientas) utilizados para evitar Ciberataques, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C06 – Política de Respaldo de Información	No existe una política sobre los respaldos de información.	La política sobre respaldos de información está incompleta o en proceso de creación.	Existe una política definida sobre los respaldos de información	Existe evidencia de la implementación y actualización continua de la política sobre los respaldos de información	La política sobre respaldos de información, es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C07 – Disponibilidad de los Sistemas	No existen controles (herramientas) para garantizar la disponibilidad de los sistemas	Existen algunos controles (herramientas) para garantizar la disponibilidad de los sistemas	La empresa cuenta con controles (herramientas) efectivas para garantizar la disponibilidad de los sistemas	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para garantizar la disponibilidad de los sistemas	Los controles (herramientas) utilizados para garantizar la disponibilidad de los sistemas, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C08 – Integridad de la información	No existen controles (herramientas) para garantizar la integridad de la información	Existen algunos controles (herramientas) para garantizar la integridad de la información	La empresa cuenta con controles (herramientas) efectivas para garantizar la integridad de la información	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para garantizar la integridad de la información	Los controles (herramientas) utilizados para garantizar la integridad de los sistemas son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C09 – Política de Registro de Eventos de los sistemas de TI	No existe una política sobre los registros de eventos de los sistemas de TI.	La política sobre los registros de eventos de los sistemas de TI está incompleta o en proceso de creación.	Existe una política definida sobre los registros de eventos de los sistemas de TI.	Existe evidencia de la implementación y actualización continua de la política sobre los registros de eventos de los sistemas de TI	La política sobre los registros de eventos de los sistemas de TI, es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C10 – Política de instalación de software en los equipos	No existe una política sobre la instalación de software en los equipos.	La política sobre la instalación de software en los equipos está incompleta o en proceso de creación.	Existe una política definida sobre la instalación de software en los equipos	Existe evidencia de la implementación y actualización continua de la política sobre la instalación de software en los equipos	La política sobre la instalación de software en los equipos, es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C11 – Política de instalación de hardware en los equipos	No existe una política sobre la instalación de hardware en los equipos.	La política sobre la instalación de hardware en los equipos está incompleta o en proceso de creación.	Existe una política definida sobre la instalación de hardware en los equipos	Existe evidencia de la implementación y actualización continua de la política sobre la instalación de hardware en los equipos	La política sobre la instalación de hardware en los equipos, es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

D08 – Ciberseguridad en las operaciones de la empresa

Niveles					
D08-C12 – Política de auditoría de Ciberseguridad	No existe una política de auditoria en Ciberseguridad.	La política de auditoria en Ciberseguridad está incompleta o en proceso de creación.	Existe una política definida de auditoria en Ciberseguridad.	Existe evidencia de la implementación y actualización continua de la política de auditoria en Ciberseguridad.	La política de auditoria en Ciberseguridad es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D09 – Seguridad en las comunicaciones

Niveles					
D09-C01 – Política de seguridad de las redes de comunicación	No existe una política de seguridad de las redes de comunicación.	La política de seguridad de las redes de comunicación está incompleta o en proceso de creación.	Existe una política definida de seguridad de las redes de comunicación	Existe evidencia de la implementación y actualización continua de la política de seguridad de las redes de comunicación.	La política de seguridad de las redes de comunicación es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D09 – Seguridad en las comunicaciones

Niveles					
D09-C02 – Política de confidencialidad y no divulgación	No existe una política sobre confidencialidad y no divulgación	La política sobre confidencialidad y no divulgación está incompleta o en proceso de creación.	Existe una política definida sobre confidencialidad y no divulgación y está alineada con las leyes aplicables	Existe evidencia de la implementación y actualización continua de la política sobre confidencialidad y no divulgación.	La política sobre confidencialidad y no divulgación es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D09 – Seguridad en las comunicaciones

Niveles					
D09-C03 – Controles de seguridad de las redes de comunicación	No existen controles (herramientas) para garantizar la seguridad de las redes de comunicación	Existen algunos controles (herramientas) para garantizar la seguridad de las redes de comunicación	La empresa cuenta con controles (herramientas) efectivas para garantizar la seguridad de las redes de comunicación	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para garantizar la seguridad de las redes de comunicación	Los controles (herramientas) utilizados para garantizar la seguridad de las redes de comunicación, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

D09 – Seguridad en las comunicaciones

Niveles					
D09-C04 – Controles para la transmisión segura de los datos	No existen controles (herramientas) para garantizar la transmisión segura de los datos	Existen algunos controles (herramientas) para garantizar la transmisión segura de los datos	La empresa cuenta con controles (herramientas) efectivas para garantizar la transmisión segura de los datos	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para garantizar la transmisión segura de los datos	Los controles (herramientas) utilizados para garantizar la seguridad de las redes de comunicación, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D09 – Seguridad en las comunicaciones

Niveles					
D09-C05 – Política sobre el uso del correo y los sistemas de mensajería y colaboración	No existe una política sobre el uso del correo y los sistemas de mensajería y colaboración	La política sobre el uso del correo y los sistemas de mensajería y colaboración está incompleta o en proceso de creación.	Existe una política definida sobre el uso del correo y los sistemas de mensajería y colaboración	Existe evidencia de la implementación y actualización de la política sobre el uso del correo y los sistemas de mensajería y colaboración.	La política sobre el uso del correo y los sistemas de mensajería y colaboración son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D10 – Sistemas de información

Niveles					
D10-C01 – Adquisición de los Sistemas de TI	No existe un proceso definido para la adquisición de los sistemas de TI	Existen algunos procedimientos para la adquisición de los sistemas de TI.	La empresa cuenta con todos los procesos de adquisición de los sistemas de TI.	Existe evidencia del cumplimiento y actualización de los procesos de adquisición de los sistemas de TI.	Los procesos de adquisición de los sistemas de TI son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D10 – Sistemas de información

Niveles					
D10-C02 – Desarrollo de los Sistemas de TI	No existe un proceso definido para el desarrollo de los sistemas de TI	Existen algunos procedimientos para el desarrollo de los sistemas de TI	La empresa cuenta con todos los procesos para el desarrollo de los sistemas de TI	Existe evidencia del cumplimiento y actualización de los procesos de desarrollo de los sistemas de TI	Los sistemas y procesos del desarrollo de los sistemas de TI son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D10 – Sistemas de información

Niveles					
D10-C03 – Mantenimiento de los Sistemas de TI	No existe un proceso definido para el mantenimiento de los sistemas de TI	Existen algunos procedimientos para el mantenimiento de los sistemas de TI	La empresa cuenta con todos los procesos para el mantenimiento de los sistemas de TI	Existe evidencia del cumplimiento y actualización de los procesos para el mantenimiento de los sistemas de TI	Los sistemas y procesos del mantenimiento de los sistemas de TI son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D11 – Relación con Proveedores:

Niveles					
D11-C01 – Controles de seguridad de la información con proveedores	No existen controles de seguridad de la información con proveedores	Existen algunos controles de seguridad de la información con proveedores	La empresa cuenta con todos los controles de seguridad de la información con proveedores	Existe evidencia del cumplimiento y actualización de los controles de seguridad de la información con proveedores	Los controles de seguridad de la información con proveedores son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D12 – Gestión de incidentes de Ciberseguridad

Niveles					
D12-C01 – Política de manejo de incidentes de Ciberseguridad	No existe una política sobre el manejo de incidentes de Ciberseguridad	La política sobre el manejo de incidentes de Ciberseguridad está incompleta o en proceso de creación.	Existe una política definida sobre el manejo de incidentes de Ciberseguridad	Existe evidencia de la implementación y actualización continua de la política sobre el manejo de incidentes de Ciberseguridad.	La política sobre el manejo de incidentes de Ciberseguridad es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D12 – Gestión de incidentes de Ciberseguridad

Niveles					
D12-C02 – Controles para el manejo de incidentes de Ciberseguridad	No existen controles (herramientas) para el manejo de los incidentes de Ciberseguridad	Existen algunos controles (herramientas) para el manejo de los incidentes de Ciberseguridad	La empresa cuenta con controles (herramientas) efectivas para el manejo de los incidentes de Ciberseguridad	Existe evidencia de la implementación y actualización continua de los controles (herramientas) para el manejo de los incidentes de Ciberseguridad	Los controles (herramientas) para el manejo de los incidentes de Ciberseguridad, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D12 – Gestión de incidentes de Ciberseguridad

Niveles					
D12-C03 – Análisis de las causas de los incidentes de Ciberseguridad	No existe un proceso definido para el análisis de las causas de los incidentes de Ciberseguridad	Existen algunos procedimientos para el análisis de las causas de los incidentes de Ciberseguridad	La empresa cuenta con todos los procesos para el análisis de las causas de los incidentes de Ciberseguridad	Existe evidencia del cumplimiento y actualización de los procesos de análisis de las causas de los incidentes de Ciberseguridad	Los procesos de análisis de las causas de los incidentes de Ciberseguridad son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D12 – Gestión de incidentes de Ciberseguridad

Niveles					
D12-C04 – Proceso de mejora continua en Ciberseguridad	No existe un proceso definido para la mejora continua en Ciberseguridad	Existen algunos procedimientos para la mejora continua en Ciberseguridad	La empresa cuenta con todos los procesos para la mejora continua en Ciberseguridad	Existe evidencia del cumplimiento y actualización de los procesos de mejora continua en Ciberseguridad	Los procesos de mejora continua en Ciberseguridad son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D12 – Gestión de incidentes de Ciberseguridad

Niveles					
D12-C05 – Proceso de recolección de evidencia en incidentes de Ciberseguridad	No existe un proceso definido para la recolección de evidencia en incidentes de Ciberseguridad	Existen algunos procedimientos para la recolección de evidencia en incidentes de Ciberseguridad	La empresa cuenta con todos los procesos para la recolección de evidencia en incidentes de Ciberseguridad	Existe evidencia del cumplimiento y actualización de los procesos de recolección de evidencia en incidentes de Ciberseguridad	Los sistemas y procesos de recolección de evidencia en incidentes de Ciberseguridad son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D13 – Continuidad del Negocio

Niveles					
D13-C01 – Proceso de contingencia en Ciberseguridad en caso de desastres	No existe un proceso definido de contingencia en Ciberseguridad en caso de desastres	Existen algunos procedimientos de contingencia en Ciberseguridad en caso de desastres	La empresa cuenta con todos los procesos de contingencia en Ciberseguridad en caso de desastres	Existe evidencia del cumplimiento y actualización de los procesos de contingencia en Ciberseguridad en caso de desastres	Los sistemas y procesos de contingencia en Ciberseguridad en caso de desastres son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D13 – Continuidad del Negocio

Niveles					
D13-C02 – Redundancia en Ciberseguridad	No existe redundancia en los sistemas de Ciberseguridad	Existe redundancia en algunos sistemas de Ciberseguridad	Existe redundancia en todos los sistemas de Ciberseguridad	Existe un proceso definido para revisar periódicamente que la redundancia en Ciberseguridad se está cumpliendo	La redundancia en Ciberseguridad de la empresa, es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D13 – Continuidad del Negocio

Niveles					
D13-C03 – BCP y Ciberseguridad	En el BCP no se menciona la Ciberseguridad	Existen algunas menciones sobre Ciberseguridad en el BCP	El BCP contempla de manera íntegra el tema de la Ciberseguridad	Existe evidencia del cumplimiento, prueba y actualización de los procesos de Ciberseguridad en el BCP	La integración de la Ciberseguridad en el BCP, es reconocido por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

D14 – Requerimientos Legales

Niveles					
D14-C01 – Alineamiento con Leyes locales	Las políticas y sanciones sobre Ciberseguridad no están alineadas con las leyes locales	Algunas políticas y sanciones sobre Ciberseguridad están alineadas con las leyes locales	Todas las políticas y sanciones sobre Ciberseguridad están alineadas con las leyes locales	Existe un proceso definido para la revisión y actualización de los lineamientos entre las leyes locales y las políticas y sanciones sobre Ciberseguridad en la empresa	El proceso sobre la revisión y actualización de los lineamientos entre las leyes locales y las políticas y sanciones sobre Ciberseguridad en la empresa, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

D14 – Requerimientos Legales

Niveles					
D14-C02 – Cumplimiento de regulaciones	Las políticas de Ciberseguridad no están alineadas con las regulaciones externas aplicables	Algunas políticas de Ciberseguridad están alineadas con las regulaciones externas aplicables	Todas las políticas de Ciberseguridad están alineadas con las regulaciones externas aplicables	Existe un proceso definido para la revisión y actualización de los lineamientos entre las regulaciones externas aplicables y las políticas y de Ciberseguridad en la empresa	El proceso sobre la revisión y actualización de los lineamientos entre las regulaciones externas y las políticas de Ciberseguridad en la empresa, son reconocidos por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

D14 – Requerimientos Legales

Niveles					
D14-C03 – Política para la protección y manejo de la propiedad intelectual	No existe una política para la protección y manejo de la propiedad intelectual	La política sobre la protección y manejo de la propiedad intelectual está incompleta o en proceso de creación.	Existe una política definida sobre la protección y manejo de la propiedad intelectual	Existe evidencia de la implementación y actualización continua de la política sobre la protección y manejo de la propiedad intelectual.	La política sobre la protección y manejo de la propiedad intelectual es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

D14 – Requerimientos Legales

Niveles					
D14-C04 – Política para la protección y manejo de los datos personales	No existe una política para la protección y manejo de los datos personales	La política sobre la protección y manejo de los datos personales está incompleta o en proceso de creación.	Existe una política definida sobre la protección y manejo de los datos personales	Existe evidencia de la implementación y actualización continua de la política sobre la protección y manejo de los datos personales	La política sobre la protección y manejo de los datos personales es reconocida por terceros como un estándar o “Best Practice” de la industria

Notas:

_____

_____

_____

_____

_____

_____

_____

GUIA DE IMPLEMENTACION DEL MODELO

Alcance

Se recomienda que este modelo se implemente a nivel de toda la empresa, y que se procure la participación activa de la mayor cantidad de empleados colaboradores posibles. Y con el fin de fomentar una cultura de Ciberseguridad, se recomienda compartir los resultados con toda la empresa.

Periodicidad

La alta gerencia debe definir en base a sus metas y objetivos, la periodicidad con la que se debe revisar y actualizar los resultados de la implementación del modelo.

Interpretación de resultados

El modelo es abierto y adaptable, por lo tanto, la empresa debe identificar los controles que no sean aplicables para excluirlos de la evaluación. Sin embargo, estos controles excluidos se deben presentar a la alta gerencia con una justificación de su exclusión para así procurar mantener el principio de transparencia.

Este modelo es modular, por lo tanto, la lectura de los resultados se puede definir en 3 áreas:

Por control

El modelo permite que se puedan calificar las áreas por separado. Esto es muy útil cuando se quiere presentar uno/unos controles a la alta gerencia para darle visibilidad al nivel de riesgo al que está expuesta la empresa en un área en particular de Ciberseguridad.

Por Dominio

El modelo también permite que se pueda hacer una calificación ponderada por dominio. Para lograrlo se parte de la ideología que dice: “la fortaleza de una cadena es equivalente al más débil de sus eslabones”. Por ende, la fórmula es muy sencilla, el resultado o calificación del dominio equivale al nivel más bajo obtenido en dicho nivel. *Por ejemplo*: Los resultados de los controles de un dominio son: 4-3-4-2-5

En este caso la evaluación del dominio seria un 2.

Por empresa

El Modelo de Madurez en Ciberseguridad, también permite que se pueda hacer una calificación final completa. Para lograr esto se toma en cuenta la ideología que dice: “la fortaleza de una cadena es equivalente al más débil de sus eslabones”. Por ende, la fórmula es muy sencilla, el resultado o calificación del nivel de madurez equivale al nivel más bajo obtenido. Por ejemplo: Los resultados de los controles de un dominio son: 4-3-4-2-5

En este caso la evaluación del dominio seria un 2.

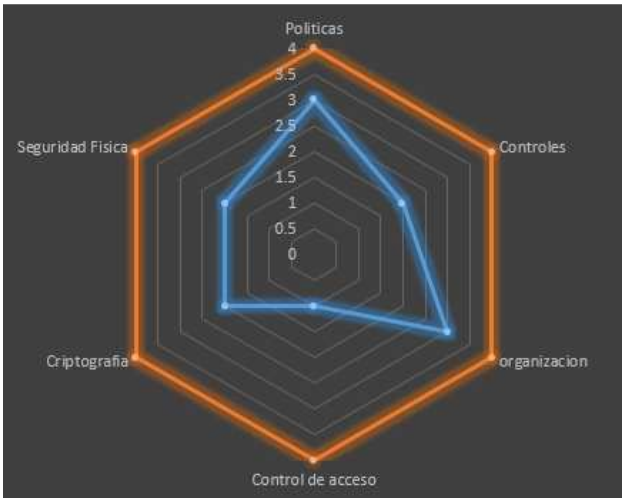


Figura 2 – Ejemplo de presentación de datos del modelo de madurez

RECOMENDACIONES PARA LA IMPLEMENTACION

Para procurar una implementación exitosa se recomienda lo siguiente:

- Apoyo total de parte de la alta gerencia, para esto se recomienda que el responsable del modelo sea parte de la alta gerencia (CISO, CIO, etc.).
- La implementación de este modelo debe de ser manejada como un proyecto, esto para ayudar a que la implementación sea exitosa.
- Asignar los recursos necesarios para la culminación del proyecto
- Asignar un responsable principal de la implementación del modelo, así como dueños para cada una de las áreas a evaluar

CONCLUSIONES

1. Basado en el análisis de los principales modelos de madurez en Ciberseguridad, se confirmó la falta de un modelo de madurez en Ciberseguridad que les permita a las empresas identificar de manera fácil, clara, rápida y efectiva su estado actual en Ciberseguridad, así como su nivel de riesgo asociado.

2. Se evidenció los diferentes tipos de impacto asociados que puede tener una empresa como consecuencia de un Ciberataque.

3. Se conocieron los múltiples beneficios que puede tener una empresa al implementar este Modelo de Madurez en Ciberseguridad.

4. Se definieron las principales políticas, controles, procesos y procedimientos que una empresa debe aplicar en materia de Ciberseguridad, basados en estándares internacionales.

5. Se confirmó que una escala de 5 niveles de madurez, era el ideal para este modelo, ya que es un punto intermedio que permitió efectivamente evaluar cada uno de los controles diseñados.

6. Se creó el Modelo de Madurez en Ciberseguridad completo, sencillo y que puede ser implementado por la misma empresa, lo cual reduce significativamente los costos de implementación.

7. El diseño del modelo permite que el mismo pueda ser implementado por cualquier tipo de empresa, industria u organización.

8. Se definió una guía de implementación que ayude a la empresa a aplicar e implementar este Modelo de Madurez en Ciberseguridad de una forma clara,

simple y efectiva. Sin necesidad de invertir recursos adicionales en la contratación de consultores externos.

9. La aplicación de este modelo, permitirá también visualizar de manera sencilla las fortalezas y debilidades de la empresa en términos de Ciberseguridad.

10. El diseño modular del modelo, permite que el mismo modelo pueda ser usado por diferentes empresas u organizaciones y que sean estas las que con conocimiento del negocio, decidan los controles aplicables, así como también su prioridad.

RECOMENDACIÓNES

1. Se recomienda realizar una evaluación de la madurez en Ciberseguridad de la empresa utilizando esta modelo, antes de la preparación del presupuesto en TI. Esto le permitiría a la empresa conocer las áreas prioritarias en donde se deben enfocar los recursos para reducir los principales riesgos en Ciberseguridad. Así también como servir de base para identificar la cantidad de recursos requeridos.

2. Se recomienda presentar los resultados reales a la alta gerencia. Se debe destacar que el hecho de que una empresa está en nivel 0, no es malo. Por el contrario, para la empresa es de un gran valor conocer este resultado para así poder enfocar sus recursos para mejorar el nivel de Ciberseguridad en dicha área. Es por eso que los resultados deben de ser presentados de la manera más fidedigna posible.

3. Se recomienda realizar esta evaluación de madurez en Ciberseguridad de forma periódica para que le permita a la empresa conocer el avance obtenido a partir de los últimos resultados, así como también evaluar la efectividad de los recursos invertidos para mejorar el nivel de Ciberseguridad de la empresa.

4. Se recomienda alinear los objetivos y estrategias de TI con los resultados de la evaluación de la madurez en Ciberseguridad de la empresa. Esto con el fin de:
    a. Reducir los riesgos asociados con “Ciberseguridad”.
    b. Alinear los objetivos y recursos, con el fin de fortalecer las áreas más vulnerables a ciberataques.
    c. Evitar el desperdicio de recursos en áreas menos críticas.
    d. Promover la maximización de recursos, los cuales deben ser asignados en las áreas que más lo necesitan.

5. Asignar roles y responsabilidades a cargo de cada uno de los controles mencionados en el Modelo de Madurez en Ciberseguridad. Esto con el fin de darle un seguimiento y control más efectivo y eficiente de los esfuerzos para mejorar o mantener el nivel de dicho control.

TRABAJOS FUTUROS

Este Modelo de Madurez en Ciberseguridad debe de mantenerse actualizado con información relevante, en busca de la mejora continua del modelo y que permita a las empresas evaluarse contra un modelo actualizado con base en la realidad internacional y las últimas tendencias, buenas prácticas y estándares en Ciberseguridad.

También, se espera que este modelo sea implementado en diferentes empresas y organizaciones, de modo que se confirme su aplicabilidad universal a cualquier tipo de empresa u organización.

Una acción interesante de alto valor sería lograr aplicar el modelo a nivel Gubernamental, esto para conocer el estado actual de un gobierno o institución autónoma, en cuanto a Ciberseguridad. Adicionalmente, el análisis de los resultados de la aplicación de este modelo, permitiría al gobierno, crear una estrategia más eficiente y con objetivos más claros para fortalecer el área de Ciberseguridad.

BIBLIOGRAFÍA

Carnegie Mellon University. (2016). *Capability Maturity Model*. Recuperado el 18 de octubre 2016, de https://www.sei.cmu.edu/reports/93tr024.pdf

Castro, R. (2011). *Ataque informático lleva DigiNotar a la quiebra*. *WeLiveSecurity*. Recuperado el 10 de Octubre 2016, de http://www.welivesecurity.com/la-es/2011/10/07/ataque-informatico-lleva-diginotar-quiebra/

CertSuperior. (2016). *Seguridad informática*. Recuperado el 18 de octubre 2016, de https://www.certsuperior.com/seguridadinformatica.aspx

Dark Reading. (2016). Adobe To Pay $1 Million Compensation In Data Breach Case. Recuperado el 12 de octubre 2016, de http://www.darkreading.com/operations/adobe-to-pay-$1-million-compensation-in-data-breach-case/d/d-id/1327513

Deloitte. (2016). *Diagnóstico de madurez* | *Deloitte México*. Recuperado el 18 de octubre 2016, de https://www2.deloitte.com/co/es/pages/human-capital/articles/nuestros-servicios.html

Deloitte. (2016). Madurez en los procesos financieros| *Deloitte México*. Recuperado el 18 de octubre 2016, de https://www2.deloitte.com/mx/es/pages/audit/articles/madurez-procesos-financieros.html

Deloitte. (2016). *Modelo de madurez* | *Deloitte México*. Recuperado el 18 de octubre 2016, de https://www2.deloitte.com/mx/es/pages/risk/articles/modelo-de-madurez.html

Energy.gov. (2014). *Cybersecurity Capability Maturity Model (C2M2)* | *Department*

of Energy. Recuperado el 22 de octubre 2016, de http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

Europapress. (2016). *El terrorismo del Siglo XXI: Los ciberataques y la amenaza nuclear*. *europapress.es*. Recuperado el 11 Octubre 2016, de http://www.europapress.es/nacional/noticia-terrorismo-siglo-xxi-ciberataques-amenaza-nuclear-20160419180142.html

Excelsior College. (2016). *How does a data breach affect your business' reputation? National Cybersecurity Institute*. Recuperado el 12 De Octubre 2016, de http://www.nationalcybersecurityinstitute.org/general-public-interests/how-does-a-data-breach-affect-your-business-reputation/

Fedco. (2015). *Continual Improvement in ISO 27001 PDCA Life Cycle | IT and ICS Security - Consultant, Training, Solutions*. Recuperado el 12 de octubre 2016, de http://fedco.co.id/continual-improvement-in-iso-27001-pdca-life-cycle/

Finkelstein. A, (1992). *A Software Process Immaturity Model*. Recuperado el 19 de octubre 2016, de http://www0.cs.ucl.ac.uk/staff/A.Finkelstein/papers/immaturity.pdf

Forrester. (2014). *The Forrester Information Security Maturity Model*. Recuperado el 18 de octubre 2016, de https://www.forrester.com/report/The+Forrester+Information+Security+Maturity+Model/-/E-RES57372

Gartner. (*2014). ITScore Overview for Security and Risk Management. Recuperado el 20 de octubre 2016*, de http://cdn.ttgtmedia.com/searchSecurity/downloads/Gartner%20Security%20Research_ITScore%20Overview.pdf

Gobierno de Brasil. (2013). *Ciberataques y ciberespionaje, sustitutos del terrorismo como primera amenaza en EEUU — Secretaria de Cooperação Jurídica Internacional*. *Internacional.mpf.mp.br*. Recuperado el 11 De Octubre 2016, de http://www.internacional.mpf.mp.br/informes-internacionais/ciberataques-y-ciberespionaje-sustitutos-del-terrorismo-como-primera-amenaza-en-eeuu

Hornyak,T. (2015). *2014 cyberattack to cost Sony $35M in IT repairs*. *Computerworld*. Recuperado el 14 de octubre 2016, de http://www.computerworld.com/article/2879480/2014-cyberattack-to-cost-sony-35m-in-it-repairs.html

IBM. (2016). *IBM 2016 Cost of Data Breach Study - United States*. *IBM Security*. Recuperado el 12 de octubre 2016, de http://www-03.ibm.com/security/data-breach/

Microsoft. (2016). El modelo de madurez del sistema de gestión de proyectos: notas del producto. Recuperado el 19 de octubre 2016, de https://support.office.com/es-es/article/El-modelo-de-madurez-del-sistema-de-gesti%C3%B3n-de-proyectos-notas-del-producto-77b7634e-97cc-4436-b1dd-1b8028f7c2eb

Netmedia. (2016)*. Obama presenta presupuesto para 2017: 19 mil millones para Ciberseguridad*. Recuperado el 14 de octubre 2016, de http://www.netmedia.mx/analisis/obama-presenta-presupuesto-para-2017-19-mil-millones-para-Ciberseguridad/

NIST. (2014). Security Maturity Levels. Recuperado el 20 de octubre 2016, de: http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html

OpenGroup. (2011). Open Information Security Management Maturity Model (O-

SM3). Recuperado el 20 de octubre 2016, de: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12238

Oxford University. (2014). Cyber Security Capability Maturity Model (CMM). *Recuperado el 20 de octubre 2016*, de: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

Palmer, D. (2016). *The cost of ransomware attacks: $1 billion this year | ZDNet*. *ZDNet*. Recuperado el 14 de octubre 2016, de http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/

Rapid7. (2016). *Security Program Assessment* Recuperado el 20 de octubre 2016, de https://www.rapid7.com/services/security-advisory-services/security-program-assessment/

RT News. (2013). Internauta pone en venta la "receta secreta" de Coca-Cola por 15 millones de dólares. Recuperado el 12 de octubre 2016, de https://actualidad.rt.com/sociedad/view/94407-coca-cola-receta-subasta-ebay

US Gov. (2014). Cybersecurity Capability Maturity Model White Paper. *Recuperado el 20 de octubre 2016*, de: https://niccs.us-cert.gov/sites/default/files/Capability%20Maturity%20Model%20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf

Us-cert.gov. (2013). *"Plan, Do, Check, Act" | US-CERT*. Recuperado el 18 de octubre 2016, de https://www.us-cert.gov/bsi/articles/best-practices/deployment-and-operations/plan-do-check-act

Warwick, A. (2015). *Target breach could cost $1bn or more, say security experts*. *ComputerWeekly*. Recuperado el 12 de octubre 2016, de http://www.computerweekly.com/news/2240241419/Target-breach-could-cost-1bn-or-more-say-security-experts

Wikipedia.org. (2016). *Seguridad informática*. Recuperado el 19 de octubre 2016, de https://en.wikipedia.org/wiki/Capability_Immaturity_Model

Wikipedia.org. (2016). *Seguridad informática*. Recuperado el 19 de octubre 2016, de https://es.wikipedia.org/wiki/Modelo_de_Capacidad_y_Madurez

GLOSARIO

Infraestructura de TI

Conjunto de equipos (PC, servidores, dispositivos de red, dispositivos de almacenamiento, etc.) encargados de procesar, almacenar, transmitir, la información digital de la empresa.

CISO

Chief information Security Officer, es la persona o rol encargado de la seguridad de la información en la empresa.

Ciberataques

Ataques realizados desde y/o hacia un entorno de TI o/y su información.

Ransomware

Es un tipo de virus diseñado para “secuestrar” la información contenida en un equipo de cómputo. Este funcionado encriptando su contenido sin el consentimiento del dueño de la información, para luego extorsionarlo a cambio de obtener la llave privada que des encripta los datos.

Hacker

Persona que utiliza sus conocimientos en informática para ganar acceso o datos de un sistema informático.

TI

Más conocida como Tecnologías de la información, es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

ISO 27001

Es parte de la familia de estándares en seguridad de la información (ISO27000) y contiene los requisitos del Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO 27002

Es parte de la familia de estándares en seguridad de la información (ISO27000) y consiste en una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Pruebas de penetración

Es una serie de pruebas realizadas con el fin de evaluar las debilidades en seguridad de un sistema informático.

Benchmark

Es una medida de comparación o estándar que puede ser usado como punto de referencia para comparar o evaluar.