Ventajas de un Modelo de Madurez en Ciberseguridad

César Rodríguez Bravo, MSc

Cybersecurity Program Manager - IBM

Profesor/Tutor Maestría en Ciberseguridad – Cenfotec

IBM Certified Expert Project Manager - PMP® - ITILv3 - SMC™ - SDC™ - SPOC™
Certified Agile Expert - Certified Scrum Trainer

¿Por qué es importante la Ciberseguridad?

- BANCARROTA
- REPUTACIÓN
- PÉRDIDA DE INFORMACIÓN
- DEMANDAS
- COSTOS DE INVESTIGACIÓN
- CIBER TERRORISMO

DigiNotar
Internet Trust Services

Adobe

TARGET

¿CÓMO EMPEZAR CON CIBERSEGURIDAD?

- ¿CÓMO ESTA LA EMPRESA A NIVEL DE CIBERSEGURIDAD?
- ¿A QUÉ NIVEL QUIERE LLEGAR LA EMPRESA?
- ¿CÓMO HACER PARA LLEGAR AL NIVEL DESEADO?

¿QUÉ ES UN MODELO DE MADUREZ?

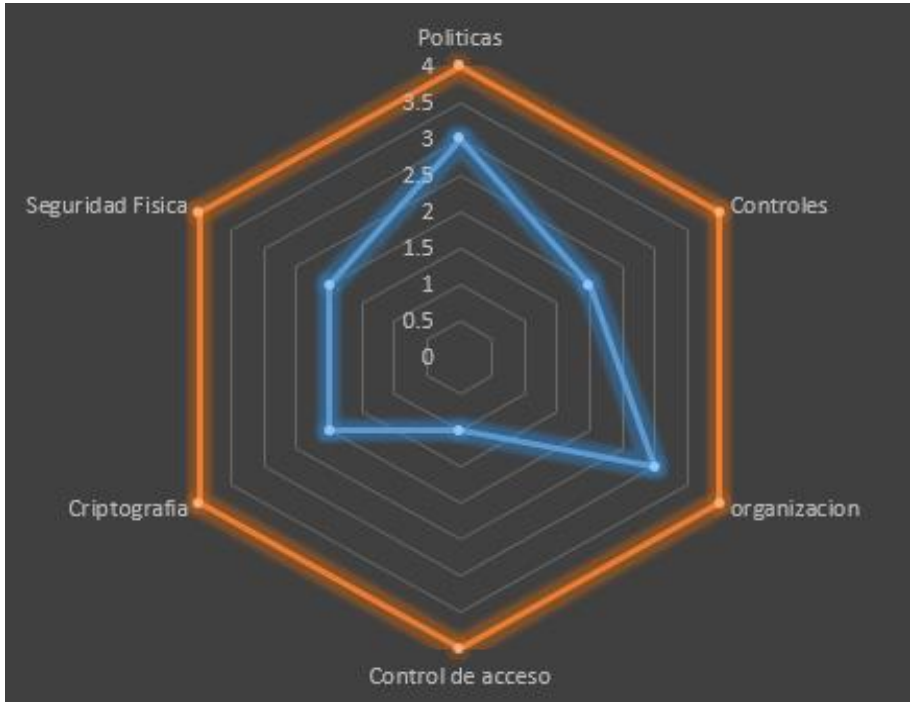
- También se le conoce como “Modelo de Madurez de Capacidades”, y se puede definir como un modelo de evaluación de procesos de una organización *(Carnegie Mellon University. 1987).*

- Unos ejemplos:
  - Modelo de Madurez en sostenibilidad. (Deloitte. 2016).
  - Modelo de Madurez en procesos financieros. (Deloitte. 2016).
  - Modelo de Madurez en Administración de Proyectos”. (Microsoft. 2016)
  - Modelo de “Inmadurez”. (Finkelstein. A. 2016).

¿EXISTEN MODELOS DE MADUREZ EN CIBERSEGURIDAD?

Características deseables de un Modelo de Madurez en Ciberseguridad

- Universal (cualquier nicho, tamaño, ubicación)
- Fácil de implementar
- Fácil de comprender
- Completo
- Actualizado
- Abierto



VENTAJAS

- GERENCIAL

ECONÓMICO

TÉCNICO/OPERATIVO

PROPUESTA DE SOLUCIÓN

- Diseñado con base en estándares internacionales como lo son:
  - COBIT
  - ITIL
  - ISO27001/27002.
- El modelo está formado por 63 Controles, los cuales están divididos en 14 Dominios.

universidad cenfotec_
tecnologías digitales

ESCALAS DE EVALUACION DEL MODELO

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM²)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM²)

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.

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM²)

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.

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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.)

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

Dominio 08 - Ciberseguridad en las operaciones de la empresa
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 12 - Política de auditoría de Ciberseguridad

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

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

MODELO DE MADUREZ EN CIBERSEGURIDAD (ECM^2)

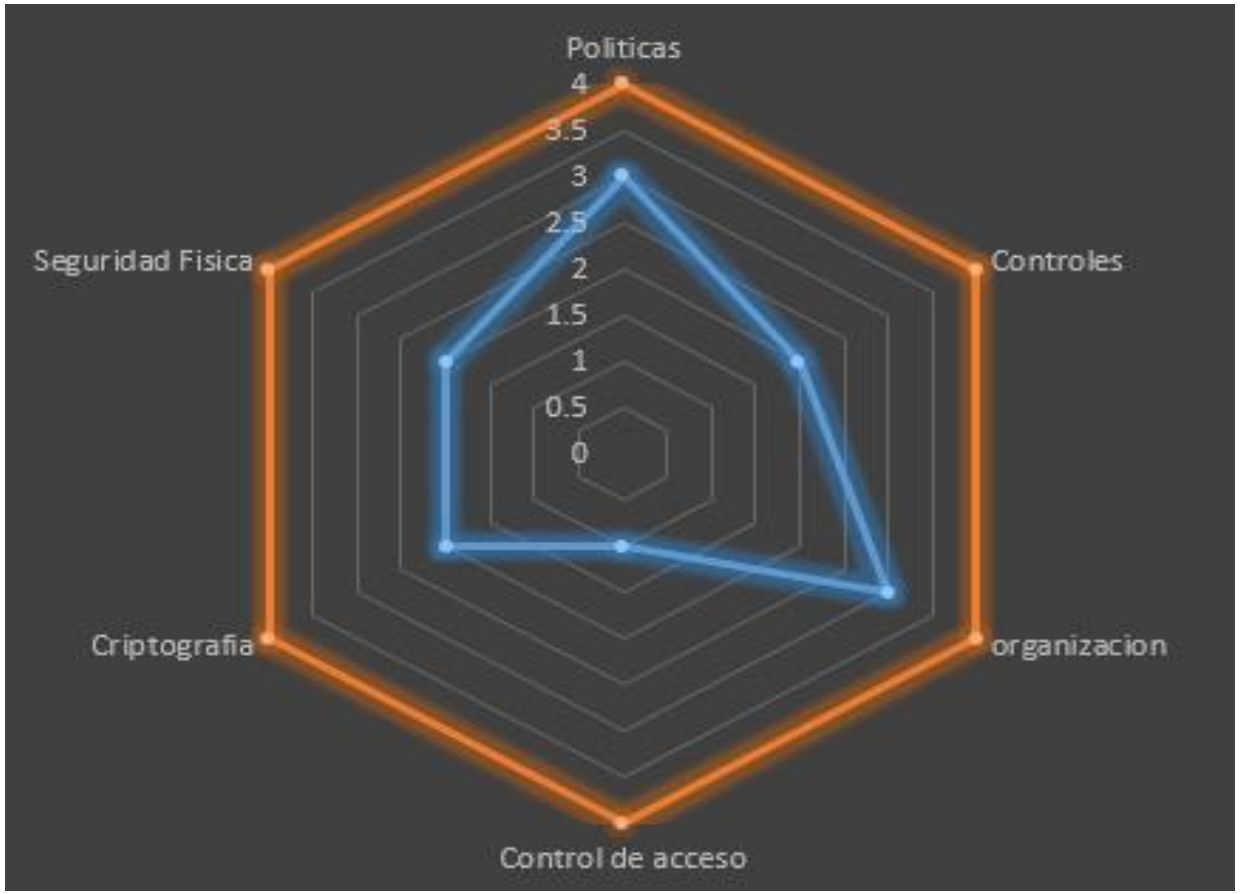
Dominio 14 - Requerimientos Legales
Control 01 - Alineamiento con Leyes locales
Control 02 - Cumplimiento de regulaciones
Control 03 - Política para la protección y manejo de la propiedad intelectual
Control 04 - Política para la protección y manejo de los datos personales

IMPLEMENTACIÓN DEL MODELO

Control **Dominio** **Empresa**

RESULTADOS	NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4
Políticas de Ciberseguridad					
Manejo de Activos					
Control de Accesos					
Seguridad en las comunicaciones					

IMPLEMENTACIÓN DEL MODELO



COMENTARIOS

MUCHAS GRACIAS

universidad cenfotec_
tecnologías digitales

COMENTARIOS

Backup Slides

universidad cenfotec
tecnologías digitales

PROPUESTA DE SOLUCIÓN

Dominio 01 - Políticas de Ciberseguridad
Dominio 02 - Organización Interna relacionada con la Ciberseguridad
Dominio 03 - Ciberseguridad y el recurso humano
Dominio 04 - Manejo de Activos
Dominio 05 - Control de Accesos
Dominio 06 - Criptografía
Dominio 07 - Seguridad Física y Ambiental

PROPUESTA DE SOLUCIÓN

Dominio 08 - Ciberseguridad en las operaciones de la empresa
Dominio 09 - Seguridad en las comunicaciones
Dominio 10 - Sistemas de información
Dominio 11 - Relación con Proveedores
Dominio 12 - Gestión de incidentes de Ciberseguridad
Dominio 13 - Continuidad del Negocio
Dominio 14 - Requerimientos Legales