CIBERDEFENSA

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

Mayor MARIANO OSCAR GÓMEZ (EJÉRCITO ARGENTINO)
PROFESOR ECEME - BRASIL

VISIÓN MILITAR Y EMPRESARIAL DE LA CIBERDEFENSA EN LOS NIVELES TÁCTICO/TÉCNICO, OPERACIONAL/GERENCIAL Y ESTRATÉGICO/DIRECTIVO

CIBERDEFENSA

Modelo de Resiliencia Cibernética de Nivel Estratégico

CIBERDEFENSA

Resiliencia:

“Energía de deformación que puede recuperarse del cuerpo deformado cuando cesa el estrés causado por la misma" (p. 30).

“Límite elástico: una vez que se supera este límite, el material ya no puede recuperarse y se deforma" (p. 31).

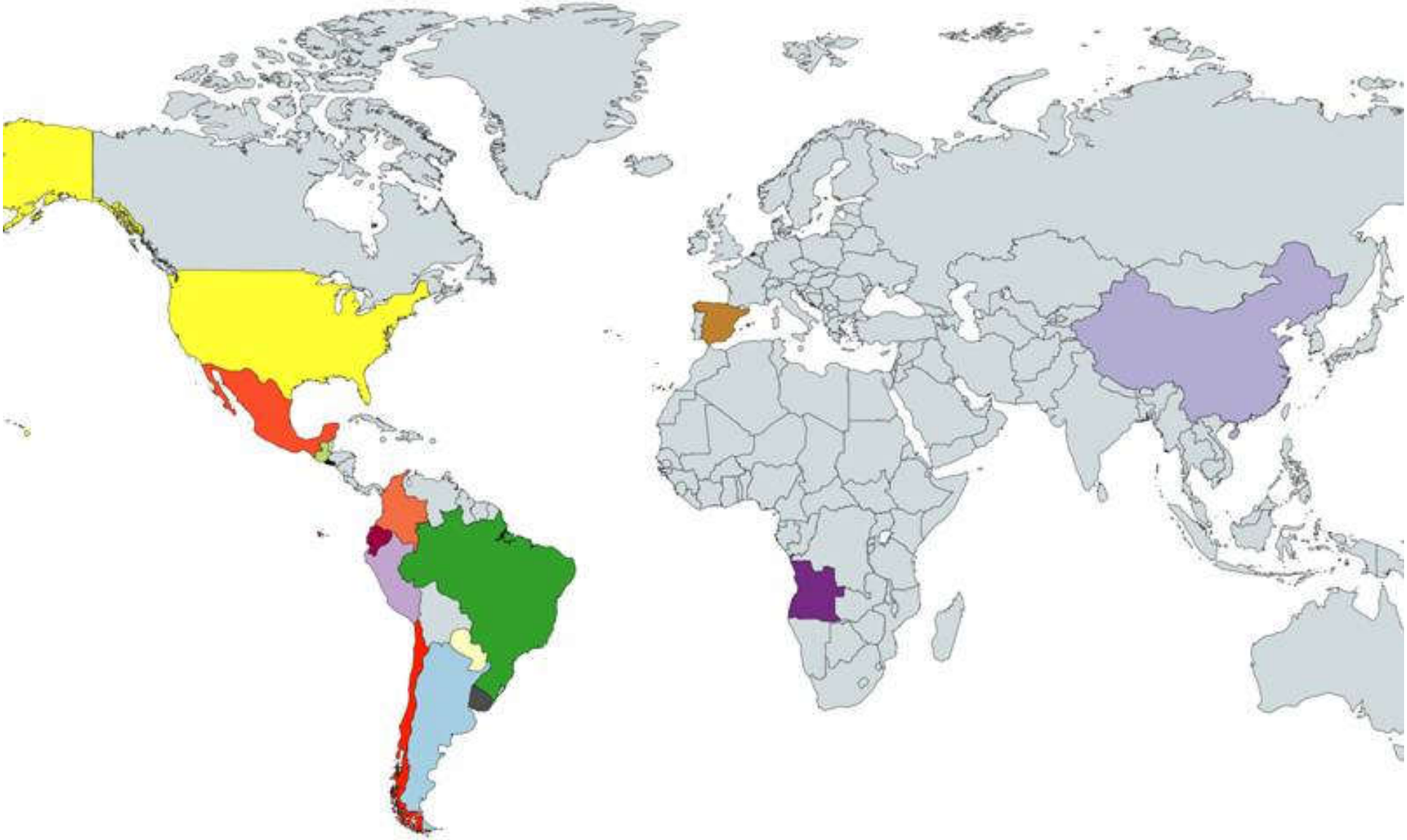
Corletti Estrada, 2017

Ciberseguridad, uma estratégia informático-militar

CIBERDEFENSA

Condición / Asunto		
Condición 1	Gestión de riesgo y de cambio	Corletti y Ardita
Condición 2	Profundo conocimiento de la organización (interno y externo)	Ardita
Condición 3	Capacidad y participación en el nivel gerencial y de toma de decisiones de la organización	Ardita
Condición 4	Capacidad para anticiparse a la crisis (CERT)	Cicerchia
Condición 5	Simplificación de los sistemas de información para reducir los procesos e interfaces	Vazquez
Condición 6	Procesos continuos y operativos en todas las circunstancias	Vazquez
Condición 7	Garantizar las regulaciones sobre las infraestructuras críticas	Malagutti
Condición 8	Estructura del sistema de información (hardware y software)	Regueira y Malvacio
Condición 9	Desarrollo de ejercicios y modelos de simulación	Regueira y Malvacio
Condición 10	Actualización del marco legal	Moresi
Condición 11	Cooperación estatal, nacional, regional y privada	de Vergara y Carneiro
Condición 12	Herramientas de desarrollo y mejora continua de la seguridad cibernética	Casi todos
Condición 13	Protección física del patrimonio tecnológico	Malagutti
Condición 14	Formación de capital humano y especialización	Todos
Condición 15	Aplicación y actualización de estrategias de resiliencia cibernética (ciclo de vida)	Corletti
Condición 16	Asignación presupuestaria suficiente	Casi todos

CIBERDEFENSA



CIBERDEFENSA

Condición	Porcentajes y Ponderaciones														TOTAL
	Imprescindible(%)	Coef 7	Muy Relevante (%)	Coef 6	Relevan-te (%)	Coef 5	Mediana-mente Relevante (%)	Coef 4	Poco Relevante (%)	Coef 3	Irrele-vante (%)	Coef 2	No aplica (%)	Coef 1	
Nº 1	48,3	338,1	34,5	207	13,8	69	1,7	6,8	0	0	1,7	3,4	0	0	624,3
Nº 2	55,2	386,4	27,6	165,6	13,8	69	3,4	13,6	0	0	0	0	0	0	634,6
Nº 3	15,5	108,5	62,1	372,6	15,5	77,5	6,9	27,6	0	0	0	0	0	0	586,2
Nº 4	32,8	229,6	46,6	279,6	12,1	60,5	5,2	20,8	3,4	10,2	0	0	0	0	600,7
Nº 5	5,2	36,4	13,8	82,8	63,8	319	15,5	62	1,7	5,1	0	0	0	0	505,3
Nº 6	46,6	326,2	41,4	248,4	8,6	43	3,4	13,6	0	0	0	0	0	0	631,2
Nº 7	41,4	289,8	48,3	289,8	8,6	43	1,7	6,8	0	0	0	0	0	0	629,4
Nº 8	6,9	48,3	31	186	50	250	12,1	48,4	0	0	0	0	0	0	532,7
Nº 9	34,5	241,5	51,7	310,2	12,1	60,5	1,7	6,8	0	0	0	0	0	0	619
Nº 10	46,6	326,2	17,2	103,2	34,5	172,5	1,7	6,8	0	0	0	0	0	0	608,7
Nº 11	67,2	470,4	20,7	124,2	10,3	51,5	1,7	6,8	0	0	0	0	0	0	652,9
Nº 12	12,1	84,7	36,2	217,2	8,6	43	6,9	27,6	36,2	108,6	0	0	0	0	481,1
Nº 13	29,3	205,1	17,2	103,2	15,5	77,5	37,9	151,6	0	0	0	0	0	0	537,4
Nº 14	65,5	458,5	29,3	175,8	3,4	17	1,7	6,8	0	0	0	0	0	0	658,1
Nº 15	56,9	398,3	24,1	144,6	13,8	69	5,2	20,8	0	0	0	0	0	0	632,7
Nº 16	39,7	277,9	53,4	320,4	5,2	26	1,7	6,8	0	0	0	0	0	0	631,1

CIBERDEFENSA

N°	Condición	Sub-condición	Componente	Observaciones
1	Gestión de riesgo y de cambio.			--
	1. a	Capacidad de anticipar la crisis (CERT)		Ex Condición 4
2	Conocimiento profundo de la organización (interna y externa)			--
	2. a	Área de cibernética con capacidad y participación en el nivel de la organización gerencial y de toma de decisión.		Ex Condición 3
3	Procesos continuos y operacionales en cualquier circunstancia.			Ex Condición 6
		-	Estructura del sistema de información (hardware e software)	Ex Condición 8
		-	La protección física del patrimonio tecnológico	Ex Condición 13
4	Garantizar regulación en las infraestructuras críticas.			Ex Condición 7
5	Desarrollo de ejercicios y modelos de simulación.			Ex Condición 9
6	Cooperación privada, estadual, nacional e regional			Ex Condición 11
	6. a	Actualización del marco legal.		Ex Condición 10
7	Formación y especialización del capital humano.			Ex Condición 14
8	Implantación y actualización de las estratégicas de resiliencia cibernética (ciclo de vida).			Ex Condición 15
9	Dotación presupuestaria suficiente.			Ex Condición 16

CIBERDEFENSA

N°	Condición	Sub-condición	Componente	Observaciones
1	Gestión de riesgo y de cambio.			--
		1. a	Capacidad de anticipar la crisis (CERT)	Ex Condición 4
		1. b	Establecimiento de atributos de calidad basados en estándares e indicadores, a partir de diagnósticos continuos y métricas adecuadas.	Especialistas
			- Adecuada capacidad de rastreabilidad ante cualquier incidente de seguridad cibernética.	Especialistas
			- Automatización de respuestas a amenazas	Especialistas
2	Conocimiento profundo de la organización (interna y externa)			--
		2. a	Área de cibernética con capacidad y participación en el nivel de la organización gerencial y de toma de decisión.	Ex Condición 3
			- Formación adecuada en ingeniería social en todos los niveles y concientización de la organización, de todos los niveles de toma de decisión y de la sociedad sobre la importancia de la cibernética.	Especialistas

N°	Condición	Sub-condición	Componente	Observaciones
3	Procesos continuos y operacionales en cualquier circunstancia.			Ex Condición 6
		-	Estructura del sistema de información (hardware e software)	Ex Condición 8
		-	La protección física del patrimonio tecnológico	Ex Condición 13
		-	Incentivo al desarrollo seguro de software en el sector de programación de la organización.	Especialistas
		-	Establecimiento de controles de seguridad críticos y auditorias periódicas relativas a la resiliencia.	Especialistas
		-	Redundancia, segmentación del a información y cooperación.	Especialistas
4	Garantizar regulación en las infraestructuras críticas.			Ex Condición 7
		-	Estandarización de los sistemas a nivel Estado (infraestructura, software, procedimientos y políticas asociadas)	Especialistas
		-	Clara categorización y priorización de los activos a proteger.	Especialistas
5	Desarrollo de ejercicios y modelos de simulación.			Ex Condición 9

CIBERDEFENSA

N°	Condición	Sub-condición	Componente	Observaciones
6	Cooperación privada, estadual, nacional e regional			Ex Condición 11
		6. a	Actualización del marco legal.	Ex Condición 10
		6. b	Establecimiento de una estrategia nacional de cibernética.	Especialistas
			- Existencia de un glosario común estandarizado de términos relacionados con la cibernética para favorecer la cooperación.	Especialistas
			- Necesidad de crear un ambiente de confianza mutua entre las organizaciones orientadas a la defensa cibernética.	Especialistas
7	Formación y especialización del capital humano.			Ex Condición 14
			- Formación del personal vinculado a las áreas de defensa cibernética, seguridad informática y sistemas.	Especialistas
			- Construcción de equipos multidisciplinarios.	Especialistas
8	Implantación y actualización de las estratégicas de resiliencia cibernética (ciclo de vida).			Ex Condición 15
			- Disponibilidad de una plataforma común para compartir datos y firmas digitales de agresiones cibernéticas.	Especialistas
9	Dotación presupuestaria suficiente.			Ex Condición 16

CIBERDEFENSA

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

MUCHAS GRACIAS

VISIÓN MILITAR Y EMPRESARIAL DE LA CIBERDEFENSA EN LOS NIVELES TÁCTICO/TÉCNICO, OPERACIONAL/GERENCIAL Y ESTRATÉGICO/DIRECTIVO