Modelo Homologado de Unidades de Policía Cibernética

CONTENIDO

I. FUNDAMENTOS NORMATIVOS 2

II. TENDENCIAS Y DIAGNÓSTICO 4

III. MODELO HOMOLOGADO DE UNIDADES DE POLICÍA CIBERNÉTICA 8

IV. IMPLEMENTACIÓN DEL MODELO 12

V. SUBPROGRAMA "MODELO HOMOLOGADO DE UNIDADES DE POLICÍA CIBERNÉTICA" 15

I. FUNDAMENTOS NORMATIVOS

- El **Plan Nacional de Desarrollo 2013-2018**: Dentro de su meta México en Paz establece en el objetivo 1.2 Garantizar la Seguridad Nacional a través de la estrategia 1.2.3, encaminada a Fortalecer la Inteligencia del Estado Mexicano para identificar, prevenir y contrarrestar riesgos y amenazas de la Seguridad Nacional. Para lograrlo, determina dentro de sus líneas de acción "impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad.[1]"

- El **Programa Nacional de Seguridad Pública 2014-2018**: Identifica y explica la importancia y atención que amerita la ciberseguridad. Como uno de sus objetivos estratégicos se busca "asegurar que la política de Seguridad Nacional del Estado mexicano adopte una perspectiva multidimensional mediante la coordinación de las autoridades e instituciones competentes, para favorecer así la consecución de los objetivos e intereses nacionales" por medio del desarrollo de "[...] una política de Estado en materia de seguridad cibernética y ciberdefensa [...]"[2]. Para lograrlo, se han establecido una serie de líneas de acción orientadas a la materia*.

Estrategia 2.7 Detectar y atender oportunamente los delitos cibernéticos.

Líneas de Acción:

2.7.1 Fortalecer las capacidades y la infraestructura tecnológica de las instituciones de seguridad pública para prevenir e investigar delitos cibernéticos.

2.7.2 Desarrollar investigación científica para la prevención e investigación de los delitos cibernéticos.

2.7.3 ***Implementar acciones contra delitos cibernéticos de mayor impacto: pornografía infantil****, fraude, extorsión, usurpación de identidad y contra derechos de autor.*

[1] Plan Nacional de desarrollo 2013-2018

[2] Programa para la Seguridad Nacional 2014-2018

2.7.4 Diseñar protocolos de operación para la prevención de delitos cibernéticos en las instancias que administran información considerada reservada o confidencial.

2.7.5 ***Promover la creación y fortalecimiento de unidades especializadas en la prevención e investigación de delitos que se cometen por internet.***

2.7.6 Desarrollar un modelo de policía cibernética para las Entidades Federativas.

2.7.7 ***Generar indicadores y estadísticas de delitos informáticos para el diseño de estrategias de prevención.***

2.7.8 Impulsar acciones para consolidar los esquemas de seguridad cibernética que coadyuven al desarrollo de la economía digital.

2.7.9 Fortalecer la seguridad de la infraestructura tecnológica estratégica del país."

- **Acuerdos del Consejo Nacional de Seguridad Pública.**

El Acuerdo 12/XL/16. Elaboración de un Modelo Homologado de Unidades de Policía Cibernética. (Aprobado en su cuadragésima sesión ordinaria celebrada el 30 de agosto de 2016)

El Consejo Nacional de Seguridad Pública acuerda que el Comisionado Nacional de Seguridad, por conducto de la Policía Federal y el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, elaboren un Modelo Homologado de Unidades de Policía Cibernética y el proceso gradual para su implementación. Además, la Procuraduría General de la República desarrollará un programa nacional de capacitación especializado en la materia.

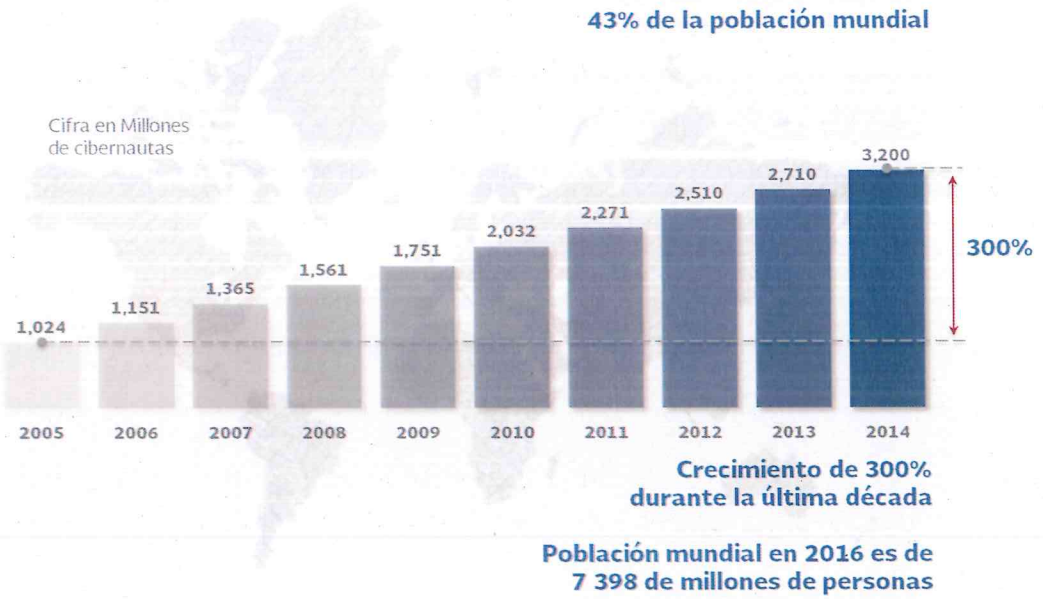
El Acuerdo 06/XLI/16. Modelo Homologado de las Unidades de Policía Cibernética. (Aprobado en su cuadragésima primera sesión ordinaria celebrada el 20 de diciembre de 2016)

En cumplimiento a los Acuerdos, 12/XL/16 del Consejo Nacional de Seguridad Pública y 7 de la XVI Sesión Ordinaria de la Conferencia Nacional de Secretarios de Seguridad Pública, el Consejo Nacional de Seguridad Pública aprueba el Modelo Homologado de Unidades de Policía Cibernética que deberá ser implementado a partir de 2017, para lo cual las entidades federativas se comprometen a asignar recursos del Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP).

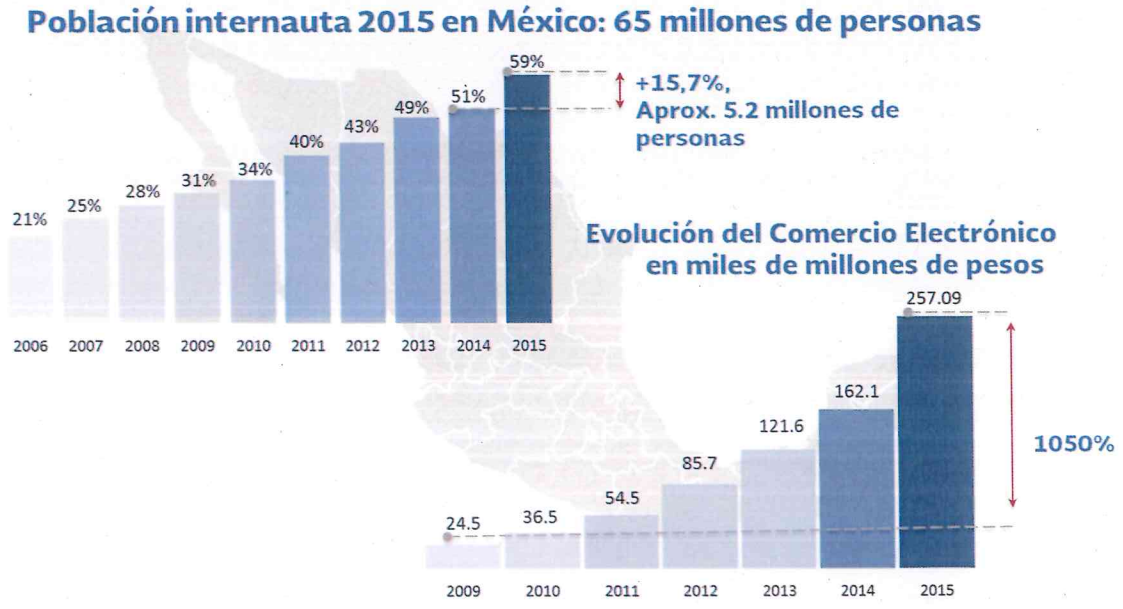
II. TENDENCIAS Y DIAGNÓSTICO

Las tendencias en ciberseguridad a nivel mundial muestran que los ciberdelincuentes se están orientando hacia el aprovechamiento de las vulnerabilidades de los nuevos equipos tecnológicos interconectados para poder robar la información confidencial de los cibernautas con la finalidad de realizar actividades delictivas.

- **Cibernautas a Nivel Mundial** [3].

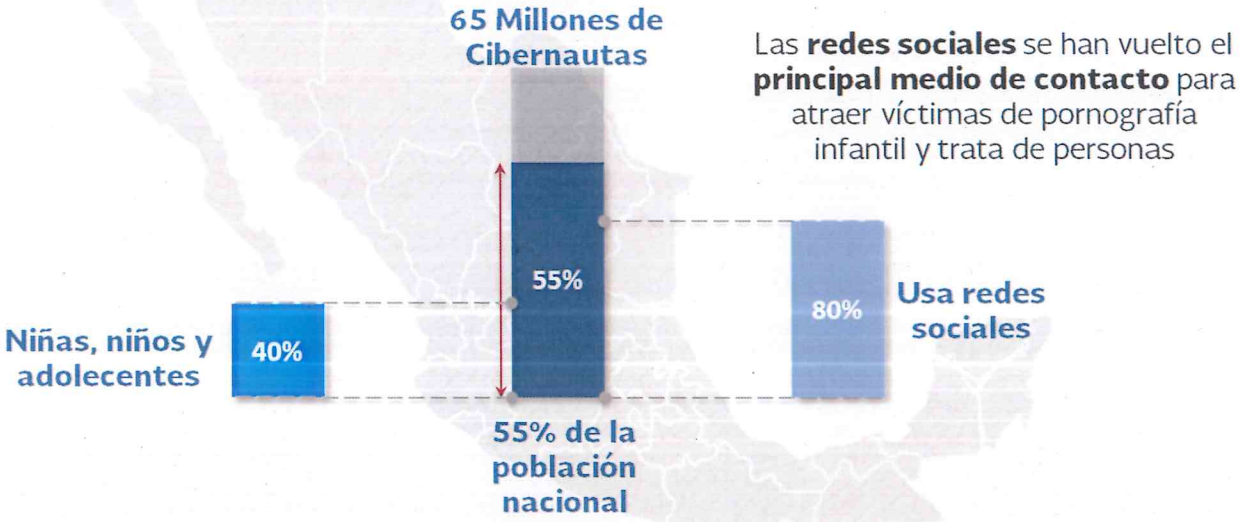


- **Cibernautas y Comercio Electrónico en México**[4].

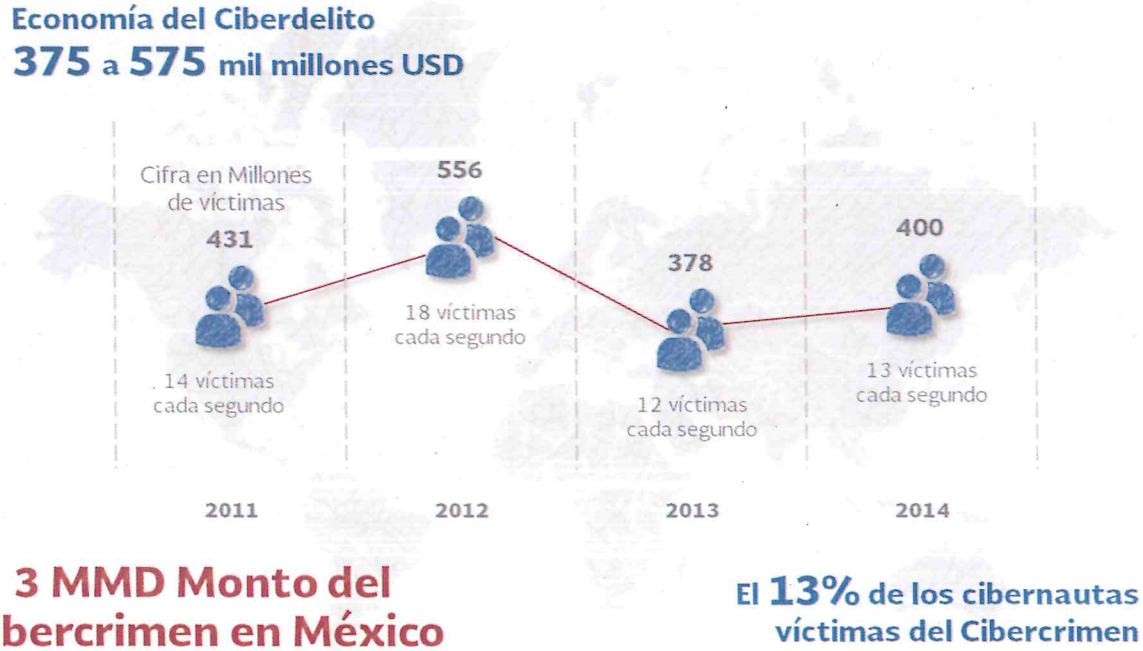


[3] *Fuente: International Telecommunications Union (ITU), ICT Indicators 2005 a 2014,*
[4] *Fuente: Día Mundial de Internet 2015, AMIPCI*

- **Facebook es la red social más utilizada en México**[5].



- **La Economía del Ciberdelito** [6].



[5] *Fuente: Día Mundial de Internet 2015, AMIPCI*
[6] *Fuente: 2013 Reporte Norton Press Deck MEXICO*
http://es.scribd.com/doc/185270894/2013-Reporte-Norton-Press-Deck-MEXICO

Debido a la creciente importancia de las tecnologías de la comunicación y con base en lo establecido en el Programa Nacional de Seguridad Pública 2013-2018, en 2014, la Policía Federal desarrolló un Modelo de Policía Cibernética con el fin de atender la estrategia de "*detección y atención oportuna de los delitos cibernéticos*" a través del fortalecimiento de las capacidades humanas, tecnológicas y la infraestructura para atender incidentes de seguridad cibernética.

Finalmente, para abril de 2016, la PF y el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) crearon y aplicaron un cuestionario para medir el nivel de madurez de las Policías Estatales en el ámbito de seguridad cibernética a través de cinco vectores: legislación, recursos humanos, equipamiento e infraestructura, operación y mecanismos de difusión y control.

- **Legislación**

A través de la aplicación del sondeo, los resultados arrojaron que a nivel nacional la mayor parte de las Entidades Federativa realizan actividades de prevención, atención e investigación de delitos cibernéticos y tienen una legislación acorde a la operación de las unidades de policías cibernéticas estatales.

- **Recursos humanos**

Las Entidades Federativas que tienen una unidad cibernética indican que cuentan con el personal suficiente para la ejecución de actividades de prevención, atención e investigación de delitos cibernéticos, en su mayoría indican que el personal ha recibido capacitación especializada en este tipo de delitos; sin embargo solo algunas unidades cuentan con alguna certificación en la materia.

- **Equipamiento e infraestructura**

En este vector, el nivel de cumplimiento no es alto se requiere habilitar acciones necesarias para el fortalecimiento en equipamiento y la infraestructura de las instalaciones de las Unidades con la participación del SESNSP.

- **Operación**

Para las tareas de ejecución, algunas Entidades Federativas cuentan con Manuales de Procedimientos para la operación cibernética, se sugiere realizas reuniones regionales de trabajo para la estandarización de la operación de las Unidades.

- **Mecanismos de difusión y control**

El estudio demostró que, en su mayoría, la ciudadanía no está informada respecto a las estadísticas referentes a delitos cibernéticos ni a los mecanismos de denuncia. Respecto de los años anteriores, la perspectiva de incidencia en ese tipo de delitos es incremental, siendo los daños económicos los que más prevalecen.

Asimismo, no se ha llevado a cabo la generación e implementación de indicadores básicos sobre ciberdelitos para homologar un lenguaje común en la materia; con esta acción se incrementaría el nivel de madurez de los mecanismos de difusión y control.

Como resultado del diagnóstico, se definieron **tres niveles de madurez**:

- **Nivel 2.** Estados que cuentan con unidades cibernéticas establecidas y en operación.
- **Nivel 1.** Estados que cuentan con unidades cibernéticas con operación básica.
- **Nivel 0.** Estados que cuentan con unidades cibernéticas con operación mínima o no cuentan con unidad cibernética.

III. MODELO HOMOLOGADO DE UNIDADES DE POLICÍA CIBERNÉTICA

- **Objetivo**

  Sentar las bases de coordinación para incrementar la capacidad del Estado Mexicano en la prevención y atención de Delitos Cibernéticos proponiendo un modelo de operación para las Policías Cibernéticas Estatales, así como los canales de comunicación. que sirvan como marco de implementación para la creación y fortalecimiento de las Policías Cibernéticas del país mediante la capacitación y especialización de policías en activos.

El Modelo de Policía Cibernética Estatal está basado en el Modelo de Policía Cibernética Federal con el cual se sentarán las bases de coordinación para incrementar la capacidad del Estado Mexicano en la prevención, atención e investigación de Delitos Cibernéticos, así como la gestión de seguridad de la información, mediante la implementación y/o fortalecimiento de las Policías Cibernéticas Estatales del país.

El Modelo incluye:

- Los **procesos** de operación de la Policía Cibernética Estatal.
- La **metodología** de implementación basada en 5 fases.
- Los **recursos materiales y humanos** para la operación de una Unidad Cibernética Estatal.
- Las **capacidades** necesarias para la integración de los procesos operativos.

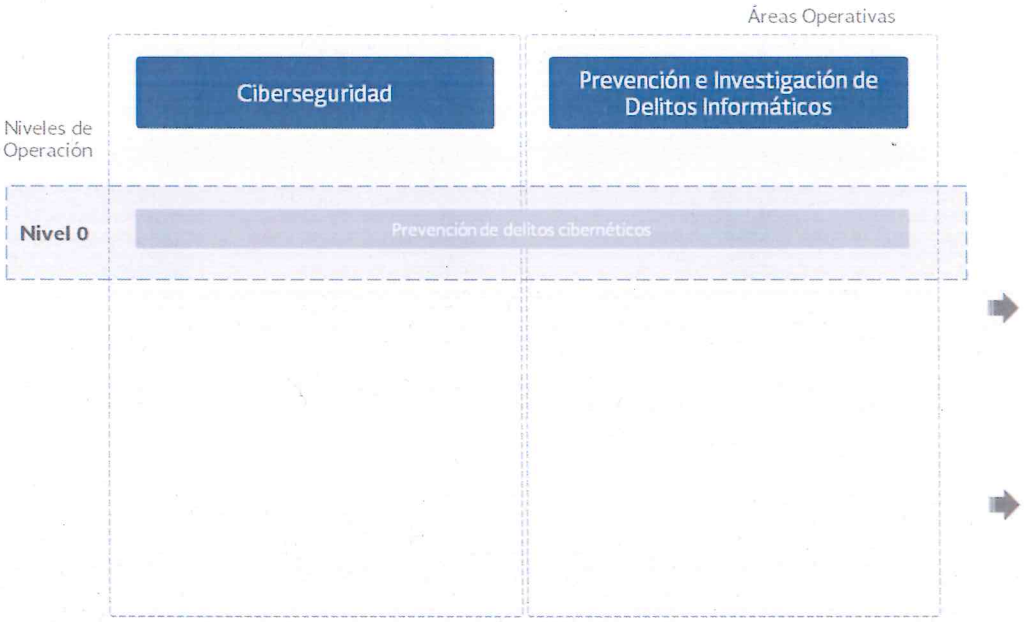
MODELO ESTATAL

PROCESOS DEL MODELO DE POLICÍA CIBERNÉTICA ESTATAL

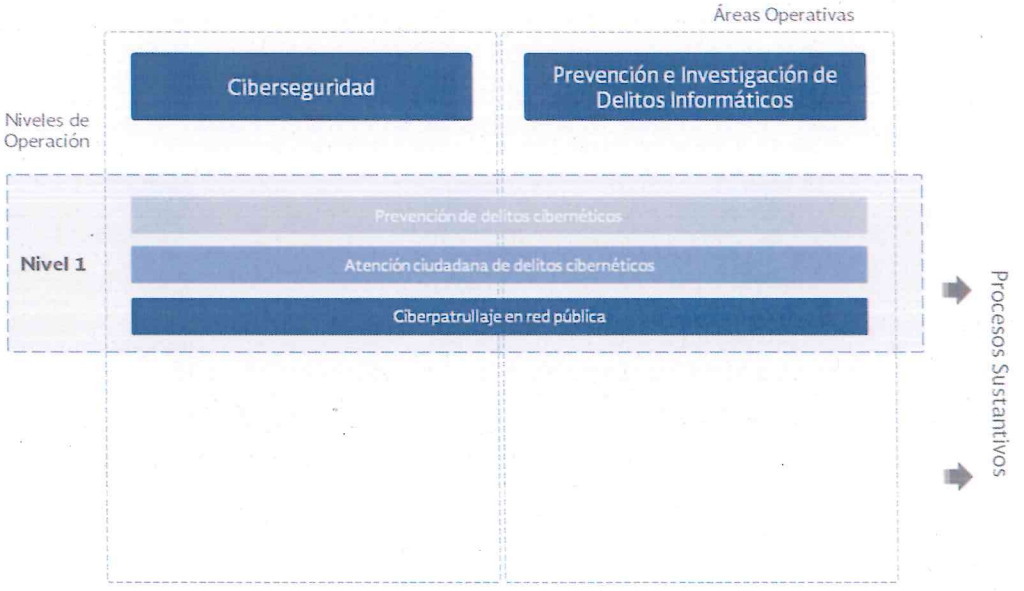
	Departamento	Proceso	Objetivo
Prevención	Campañas de Prevención y Capacitación en Delitos Cibernéticos	**Proceso de Campaña de Prevención de Delitos Cibernéticos**	Promover la cultura de prevención en delitos cibernéticos para fortalecer la atención ciudadana y formalizar convenios de colaboración para impulsar las campañas de prevención.
Atención	Atención Ciudadana a de Delitos Cibernéticos	**Proceso de Atención a Denuncias Ciudadanas**	Atender las denuncias sobre hechos relacionados a conductas o delitos cibernéticos, con la finalidad de orientar al ciudadano y, en su caso, canalizarlo con la autoridad competente
		Proceso de Generación de Estadísticas de Ciberseguridad	Correlacionar la información sobre el comportamiento de los delitos cibernéticos en la población para fortalecer las estrategias de prevención que atienden a la ciudadanía.
Reacción	Identificación y Análisis de Incidentes Cibernéticos	**Proceso de Atención a Incidentes Cibernéticos**	Analizar y resolver incidentes de seguridad informática, manejando la información de manera segura acorde a las políticas de seguridad para reducir y mitigar los riesgos y amenazas de ataques cibernéticos.
Investigación	Investigación de Delitos Cibernéticos	**Proceso de Investigación de Delitos Cibernéticos**	Atender los requerimientos emitidos por los ministerios públicos, autoridades competentes y áreas de la policía, para apoyar la investigación, probablemente constitutivos, de delitos cibernéticos.
	Análisis Forense en Dispositivos Electrónicos	**Proceso de Extracción y Análisis de Información en Dispositivos Electrónicos**	Atender los requerimientos de extracción de información contenida en dispositivos de almacenamiento electrónico y de comunicaciones por parte de autoridades competentes y áreas de la Policía para la obtención de indicios y/o evidencias que permitan la prevención, investigación y combate de delitos electrónicos.
	Patrullaje Cibernético	**Proceso de Patrullaje Cibernético**	Identificar las probables conductas constitutivas de delitos cibernéticos cometidas a través de Internet mediante la búsqueda de datos en fuentes públicas de información que nos permitan la generación de inteligencia y nuevas líneas de investigación en colaboración con otras unidades de policía, instituciones de los tres órdenes de gobierno y autoridades competentes.
Gestión	Seguridad de la Información	**Proceso de Identificación y Análisis de Riesgos en Seguridad de la Información**	Identificar, evaluar, priorizar y tratar los riesgos relacionados a la confidencialidad, integridad y disponibilidad de la información manejada dentro de la Policía Cibernética.

NIVELES DE MADUREZ DE LA POLICÍA CIBERNÉTICA ESTATAL

Nivel 0



Nivel 1



Nivel 2


Áreas Operativas
Ciberseguridad
Prevención e Investigación de Delitos Informáticos
Niveles de Operación
Prevención de delitos cibernéticos
Atención ciudadana de delitos cibernéticos
Ciberpatrullaje en red pública
Nivel 2
Investigación de delitos cibernéticos
Identificación y análisis de incidentes cibernéticos
Análisis forense en dispositivos Electrónicos
Seguridad de la información
Procesos Sustantivos

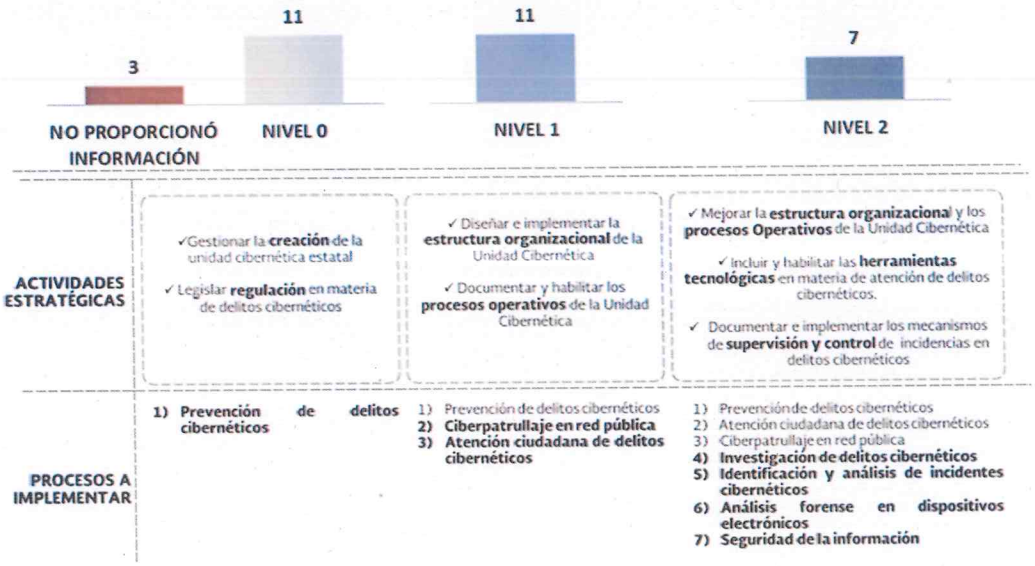
IV. IMPLEMENTACIÓN DEL MODELO

La implementación de la Policía Cibernética en cada gobierno estatal, dependerá de la estrategia y estructura de la Seguridad Pública y Procuración de Justicia. Para un estado que cuente con una Secretaría de Seguridad Pública y una Procuraduría General de Justicia Estatal, se recomienda la implementación de la Policía Cibernética dentro de la Secretaría de Seguridad Pública.

Se prevé que para la implementación del Modelo, en las entidades federativas que ya cuenten con una Unidad de Policía Cibernética, el Modelo servirá de base para la reestructuración en materia de prevención, atención, patrullaje e investigación de delitos cibernéticos, a través de un diagnóstico que permitirá a los estados desarrollar programas de capacitación para el personal, así como llevar a cabo las acciones necesarias para el fortalecimiento de la infraestructura y equipamiento de las instalaciones.

En el caso de que la entidad no cuente con una Unidad de Policía Cibernética, es necesario que, de manera paralela a su creación e implementación del Modelo, el estado proponga las medidas legislativas que le permitan un marco legal apropiado para su funcionamiento; el modelo tiene considerada la creación o implementación de dicha Unidad, apoyando la conformación de su estructura orgánica.

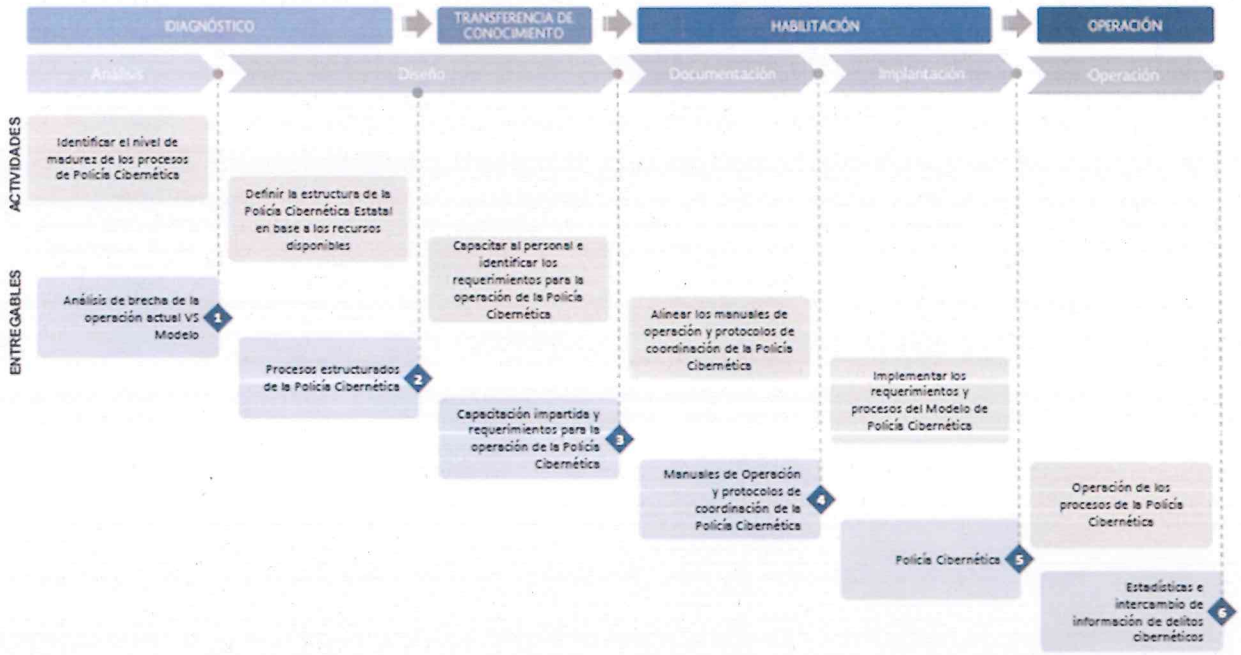
ESTRATEGIA DE IMPLEMENTACIÓN POR NIVEL DE MADUREZ



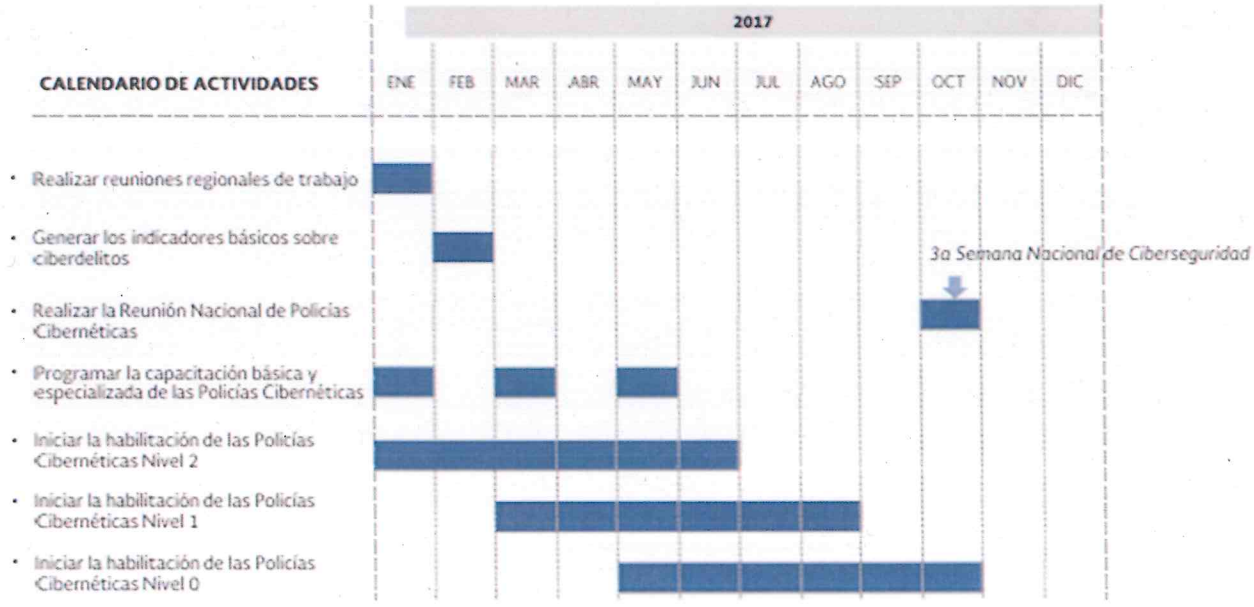
ESTRATEGIA DE IMPLEMENTACIÓN

PROGRAMA GENERAL DE IMPLEMENTACIÓN

PROGRAMA DE IMPLEMENTACIÓN DETALLADO

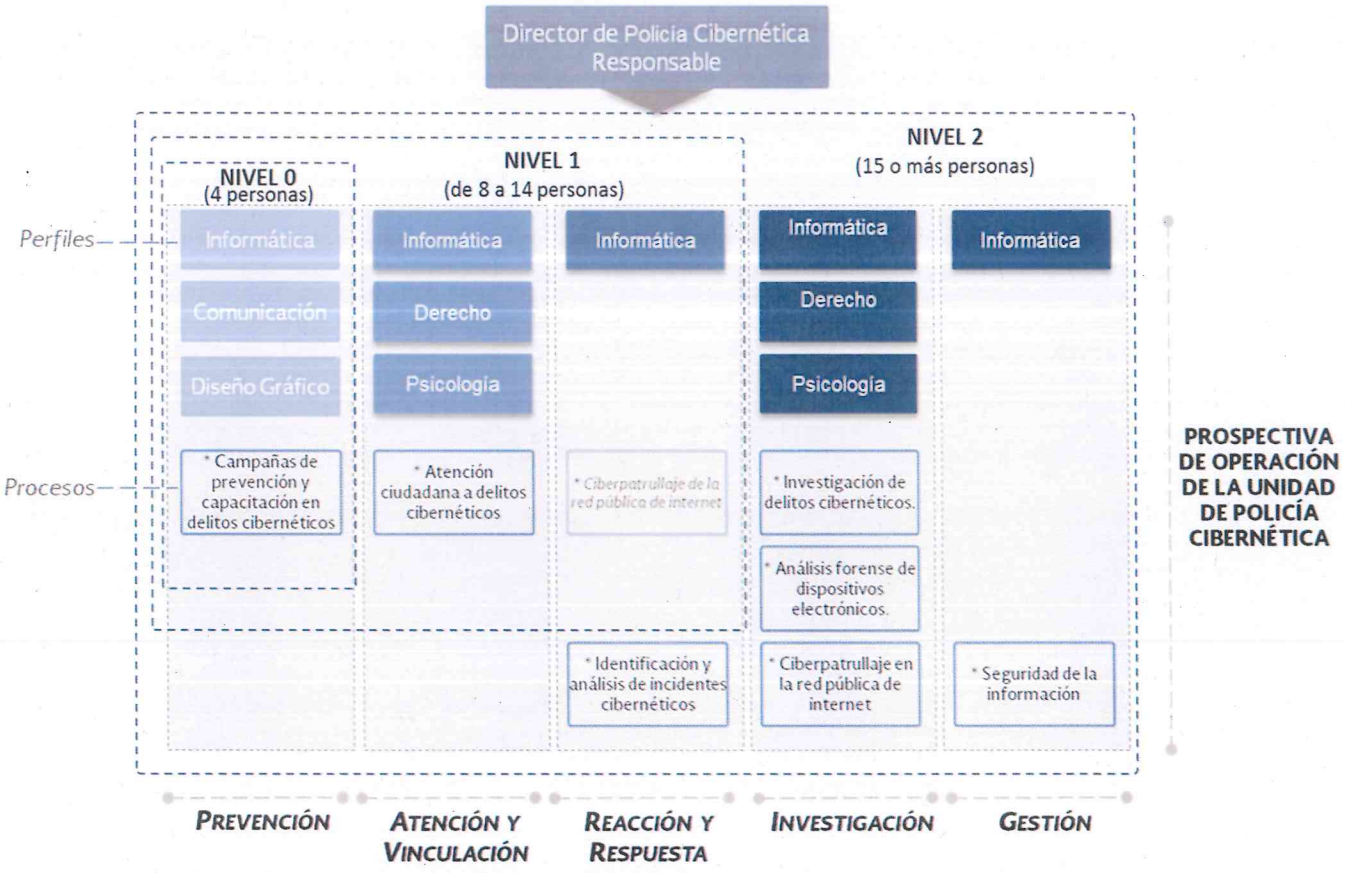


Como parte de la Estrategia de Implementación, se han generado una serie de actividades para habilitar a las Policías Cibernéticas en las entidades federativas a Nivel Nacional.



V. SUBPROGRAMA "MODELO HOMOLOGADO DE UNIDADES DE POLICÍA CIBERNÉTICA"

- **Proyección de integrantes de las Unidades de Policía Cibernética.**



- **Conceptos de Gasto asociados al Subprograma.**

Principales rubros de equipamiento de las Unidades de Policía Cibernética

- ✓ Mobiliario y equipo de oficina.
- ✓ Uniformes.
- ✓ Equipo de comunicaciones y sistemas especiales.
- ✓ Equipo para video wall del centro de monitoreo de ciberseguridad.
- ✓ Equipo para el centro de datos de ciberseguridad (site).

- **Programa de Formación para Integrantes de las Unidades de Policía Cibernética**

Objetivo

La Comisión Nacional de Seguridad, a través de la Policía Federal (PF) y el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) mediante el diseño curricular del Subprograma del Modelo Homologado de Unidades de Policía Cibernética, formarán y actualizarán al personal para coadyuvar en la implementación de un Modelo de Unidad de Policía Cibernética que impulse la prevención, atención e Investigación de los delitos cibernéticos a lo largo del territorio nacional, atendiendo de forma oportuna todas las denuncias ciudadanas en la materia, coadyuvando en la reducción de delitos cometidos en agravio de niñas, niños y adolescentes, incrementando el nivel de seguridad de la red pública de Internet y con ello al mejoramiento de la calidad de vida dentro de la sociedad, impulsando el crecimiento del comercio electrónico del país.

En relación a lo anterior y de conformidad a la madurez de las unidades de policía cibernética de las entidades federativas, se proponen tres etapas de capacitación.

ESTRUCTURA CURRICULAR

Básico. Cuando el policía acaba de ingresar a la Unidad o no tiene más de 1 año en ella, deberá cursar el presente programa curricular básico para realizar sus funciones en la Unidad de Policía Cibernética, sin importar la madurez de la Unidad.

Modulo	No.	Clave de la Materia	Seriación	Asignatura	Horas
Formación Especializada Madurez 0	1	101	N/A	Estrategias de Prevención de Delitos Cibernéticos	25
	2	102	N/A	Amenazas Dentro del Internet (Delitos Cibernéticos)	25
	3	103	N/A	Nuevas Tecnologías y el Uso del Internet de las Cosas	10
	4	104	N/A	Introducción de Seguridad de la Información	20
					80

Intermedio. Cuando el policía se encuentra en activo en la unidad de policía cibernética podrá cursar el siguiente programa curricular de especialización intermedia para mejora en sus funciones.

Modulo	No.	Clave de la Materia	Seriación	Asignatura	Horas
Formación Especializada Madurez 1	1	201	N/A	Ciberpatrullaje en la Red Pública de Internet	10
	2	202	N/A	Pornografía Infantil y Trata de Personas en Internet	15
	3	203	N/A	Malware, Amenazas y Ataques	15
	4	204	N/A	Seguridad en Redes	10
	5	205	N/A	Seguridad en Dispositivos Móviles	10
	6	206	N/A	Password: Enfrentar el Control de Accesos	10
					70

Avanzado. Cuando el policía se encuentra en activo en la unidad de policía cibernética podrá cursar el siguiente programa curricular de especialización avanzada para mejorar sus funciones.

Modulo	No.	Clave de la Materia	Seriación	Asignatura	Horas
Formación Especializada Madurez 2	1	301	N/A	Prevención, Respuesta y Administración de Incidentes	20
	2	302	N/A	Sistemas de Detección y Prevención de Intrusos y Monitoreo	10
	3	303	N/A	Análisis de Vulnerabilidades y Pruebas de Penetración	20
	4	304	N/A	Ethical Hacking	20
	5	305	N/A	Análisis Forense	20
	6	306	N/A	Fundamentos de la Norma ISO/IEC 27001:2013, Sistema de Gestión de la Seguridad de la Información	10
					100

- **Guía de Criterios Básicos de Infraestructura para las Unidades de Policía Cibernética**

OBJETIVO

Definir los criterios básicos de infraestructura para los espacios físicos de trabajo, mobiliario y equipamiento, con los que deben contar las Unidades de Policía Cibernéticas en las entidades federativas, con la finalidad de cumplir con el Modelo Homologado de Unidades de Policía Cibernética y con ello atender de manera oportuna las denuncias de la ciudadanía en materia de delitos cibernéticos.

Por lo anterior, de no existir Unidad de Policía Cibernética o si la misma no cuenta con instalaciones propias, se sugiere realizar las gestiones necesarias entre las autoridades estatales para que dichas Unidades, preferentemente se ubiquen dentro de las instalaciones de su Centro de Comando, Control, Comunicación y Cómputo (C4) o su similar en la Entidad Federativa.

Cabe hacer mención, que la presente guía únicamente será considerada para el ejercicio presupuestal del Fondo de Aportaciones para la Seguridad Pública (FASP) del año 2017, en tanto se diseña y elabora la Guía Arquitectónica para la Unidad de Policía Cibernética.

OBJETIVOS PARTICULARES

1. Homologar la infraestructura en la que operan las Unidades de Policía Cibernéticas y garantizar un espacio de trabajo adecuado que les permita realizar sus funciones con eficiencia, y a la vez garantice un espacio de atención de las personas en situación de víctima.

2. Orientar a las entidades federativas en el proceso de consolidación de su policía cibernética, mediante el establecimiento de los modelos de infraestructura aquí descritos, los cuales reúnen las características básicas de operación en términos de seguridad y funcionalidad, y ofrecen condiciones de flexibilidad y adaptabilidad para las condiciones específicas de cada estado.

3. Garantizar que con independencia del lugar físico en el cual los integrantes de la policía cibernética desarrollen su actividad cuenten con un especio digno, así como con el mobiliario y equipo que les permita: generar estrategias, preparar documentos, dar seguimiento a solicitudes de investigación y atención a las denuncias ciudadanas, así como realizar cualquier otra actividad necesaria requerida a la Unidad.

Tabla de espacios mínimos requeridos para el Modelo de "Madurez 0" compartiendo recursos.

No.	ESPACIO
1	Recepción – Módulo de Información común
2	Área Directiva
3	Área de Diseño Gráfico
4	Sala de Juntas
5	Área de Archivo

Tabla de espacios mínimos requeridos para el Modelo de "Madurez 1" compartiendo recursos.

No.	ESPACIO
1	Recepción – Módulo de Información común
2	Área Directiva
3	Área de Monitoreo de Ciberseguridad
4	Área Jurídica
5	Área de Psicología
6	Área de Diseño Gráfico
7	Sala de Juntas
8	Site
9	Área de Archivo

Tabla de espacios mínimos requeridos para el Modelo de "Madurez 2" compartiendo recursos.

No.	ESPACIO
1	Recepción – Módulo de Información común
2	Área Directiva
3	Área de Monitoreo de Ciberseguridad
4	Área Jurídica
5	Área de Psicología
6	Área de Diseño Gráfico
7	Área de Investigación
8	Laboratorio de Electrónica Forense
9	Laboratorio Malware
10	Sala de Juntas
11	Site
12	Área de Archivo

Tabla de espacios mínimos requeridos para el modelo de "madurez 2" ex profeso.

No.	ESPACIO
1	Recepción – Módulo de Información
2	Sala de Espera
3	Área Directiva
4	Área de Monitoreo de Ciberseguridad
5	Área Jurídica
6	Área de Psicología
7	Área de Diseño Gráfico
8	Área Investigación
9	Laboratorio de Electrónica Forense
10	Laboratorio Malware
11	Sala de Juntas
12	Salón de Usos Múltiples
13	Site
14	Área de Archivo
15	Área de Cocineta
16	Sanitario
17	Séptico
18	Estacionamiento

Elaboró:	Autorizó:
Ing. Oliver González Barrales Comisario Director General del Centro Especializado en Respuesta Tecnológica	**Dra. Patricia Rosa Linda Trujillo Mariel** Comisaria General Titular de la División Científica