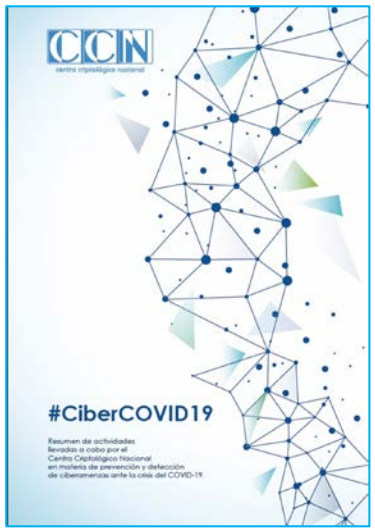
Desinformación

Toolkit para la Detección

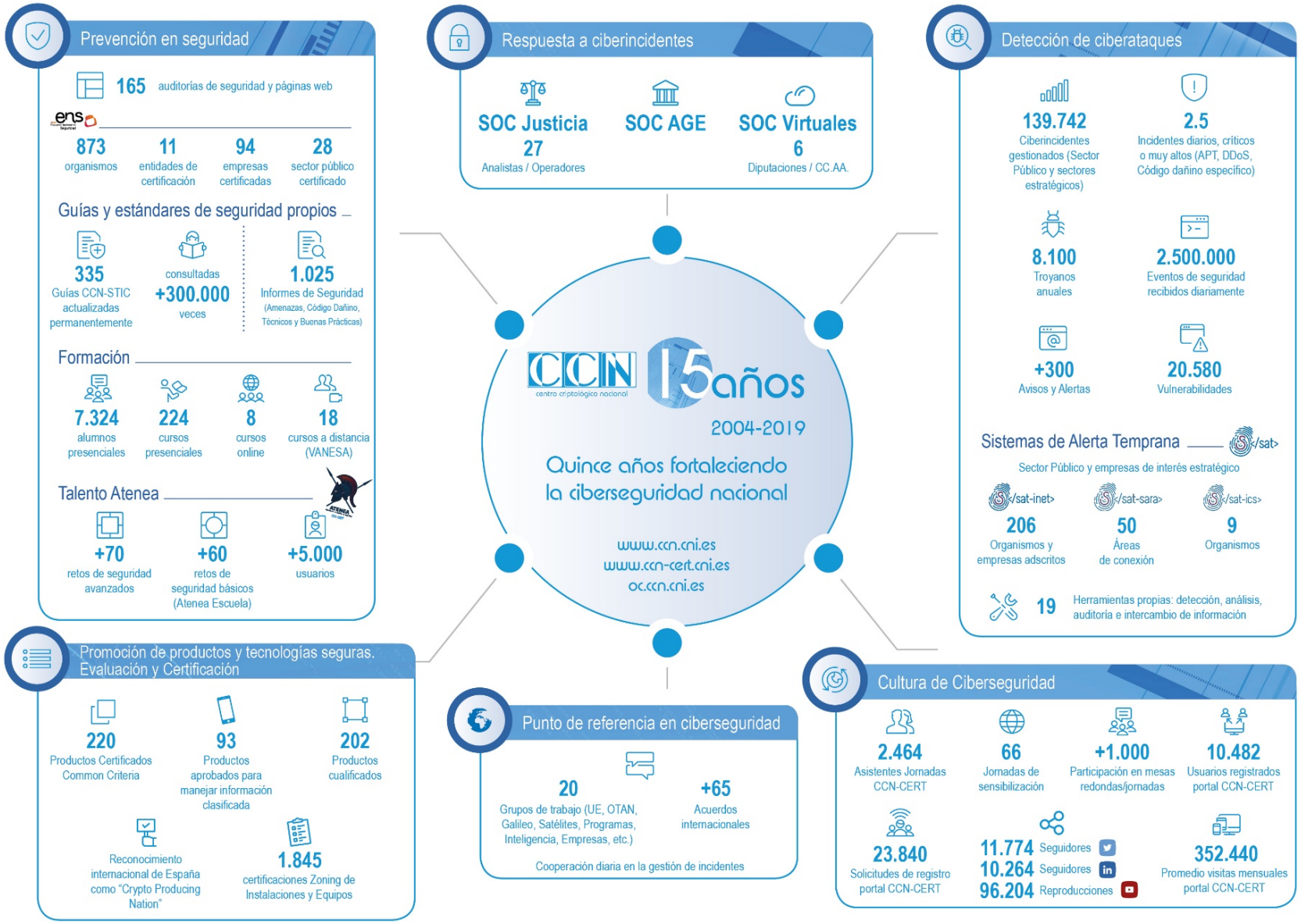


http://ccn-cert.net/ciberv-chile
Contraseña: C1b3rCHILE2020

centro criptológico nacional

centro criptológico nacional 15 años

Centro Criptológico Nacional



CCN centro criptológico nacional

Prevención

Actividades para fomentar el uso seguro de la tecnología ante la pandemia del COVID-19.

Aspectos clave impulsados por el CCN

Iniciativa	Concienciación	Formación	Colaboración
#CiberCOVID19	35	22	35
Creación del hashtag para informar de campañas de ransomware.	infografías elaboradas con recomendaciones de seguridad.	actividades de formación a distancia impulsadas por el CCN.	empresas ofrecen sus servicios a la Administración.

Campaña de concienciación

Recomendaciones de seguridad ante las campañas de malware, phishing y desinformación bajo el hashtag #CiberCOVID19 y #NoTeInfectesConElMail.

6
infografías con buenas prácticas para prevenir posibles ataques.

29
consejos para concienciar en el buen uso de la tecnología.

Informes de seguridad. Cooperación público-privada.

Ante la generalización del teletrabajo, el CCN elabora documentación con pautas de seguridad para garantizar la seguridad de las organizaciones.

5
Informes elaborados con pautas de seguridad para situaciones de teletrabajo.

35
empresas, coordinadas por el CCN, ofrecen sus servicios a la Administración.

Coordinadas por el CCN-CERT, diferentes empresas que operan en nuestro país en el sector de la ciberseguridad, deciden ofrecer de manera altruista algunos servicios y soluciones para diferentes organizaciones, principalmente del sector público. Los informes del CCN recogen el alcance y el público objetivo al que estas empresas brindan sus productos y servicios.

"El CCN-CERT fortalece la ciberseguridad nacional ante la crisis del COVID-19"

Formación

Ante la crisis generada por el COVID-19 y la importancia que tiene la ciberseguridad en estos momentos, el Centro Criptológico Nacional ha desarrollado nuevas actividades formativas disponibles para todos los usuarios en la página web del CCN-CERT.

1
nuevo curso online sobre principios y recomendaciones básicas de ciberseguridad.

21
sesiones de formación en directo y a distancia para impulsar el teletrabajo seguro

Las sesiones de formación a distancia se realizan a través de VANESA, solución desarrollada por el CCN-CERT para facilitar la tarea de formación y sensibilización con toda su comunidad de referencia.

Sensibilización

El CCN ha recopilado toda su actividad relacionada con el #CiberCOVID19 en www.ccn-cert.cni.es/cibercovid19

Vigilancia

Actividades de vigilancia para realizar prospectiva de la ciberseguridad, persiguiendo determinar la superficie de exposición de los sistemas y reducir el tiempo de respuesta de posibles incidentes ante la pandemia del COVID-19.

Actividades destacadas

Dominios	Subdominios	Soluciones	SOC
114	+1,6K	2	2
dominios de hospitales, agencias y empresas públicas, auditados.	subdominios relacionados con el sector salud, analizados.	soluciones de seguridad para incrementar la vigilancia.	centros de operaciones de ciberseguridad para garantizar el teletrabajo.

Auditorías de páginas web del sector salud

Durante la pandemia del COVID-19 y con el objetivo de conseguir un ciberespacio más seguro y confiable, el CCN está llevando a cabo la evaluación de la superficie de exposición en entidades de diferentes Comunidades Autónomas relacionadas con el sector salud, identificando los dominios y subdominios vinculados a cada una de ellas, y las vulnerabilidades asociadas a sus servicios y aplicaciones.

Para ello, se están realizando pruebas en base a técnicas no intrusivas y de reducida interacción para disponer de un análisis básico que permita recopilar la información necesaria para determinar la superficie de exposición (los resultados obtenidos se trasladan a la solución ANA). Además, se está ofreciendo a cada una de las entidades la posibilidad de llevar a cabo análisis de mayor alcance sobre los servicios, aplicaciones o pruebas de auditorías llevadas a cabo.

114
dominios de hospitales, agencias y empresas públicas, auditados.

+1,6k
subdominios relacionados con el sector salud, analizados.

Soluciones para incrementar la vigilancia

Permite una vigilancia más allá del acceso remoto, al establecer una conexión segura y verificada, entre el usuario y los sistemas corporativos, monitorizando de manera continua el comportamiento de la conexión. EMMA ofrece visibilidad de los dispositivos conectados a una red corporativa y tiene capacidad de respuesta ante alertas.

Incrementa la capacidad de vigilancia y permite conocer la superficie de exposición de los sistemas. Esta solución facilita la gestión eficiente de la detección de vulnerabilidades y de la notificación de alertas, ofreciendo recomendaciones para un tratamiento oportuno de las mismas.

2
soluciones de seguridad para incrementar la vigilancia.

"Es prioritario reforzar la capacidad de prevención, monitorización, vigilancia y respuesta a incidentes."

Centros de Operaciones de Ciberseguridad (SOC)

Los Centros de Operaciones de Seguridad (SOC) permiten aumentar las capacidades de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones, y se mejora también la capacidad de respuesta de cualquier organización ante posibles ataques.

2
centros de operaciones de ciberseguridad para garantizar el teletrabajo.

A través de los Centros de Operaciones de Ciberseguridad que el CCN-CERT opera, se está velando por las conexiones remotas seguras, con el objetivo de garantizar que el teletrabajo se desempeña en unas condiciones de seguridad óptimas. Desde estos Centros, se están implementando los planes de acción y las medidas necesarias para la detección de ataques de campañas de phishing.

CCN
centro criptológico nacional

Detección

Actividades de detección de las campañas de malware que emplean temáticas relacionadas con la pandemia del COVID-19.

Actividades destacadas

Dominios
102k
nombres de sitios web detectados que hacen referencia al COVID-19.

Informes
14
Informes de análisis de código dañino con temática COVID-19-

Recopilación
3
listas negras publicadas con indicadores de compromiso.

Vulnerabilidades
18
alertas publicadas sobre riesgos y vulnerabilidades en servicios externos.

Sistema de Alerta Temprana

El CCN-CERT está trabajando a través del Sistema de Alerta Temprana, que permite la actuación antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Este sistema de vigilancia facilita la detección rápida de incidentes y anomalías en la Administración y en las empresas de interés estratégico que dispongan de este servicio.

En la tercera semana de marzo, el número de incidentes de phishing en organismos públicos aumentó un 75% con respecto a semanas anteriores. No obstante, esta situación solo se dio a finales del mes indicado.

Dominios

El CCN-CERT está brindando apoyo y colaboración a todas las organizaciones ante cualquier emergencia que puedan sufrir. Todo ello, con el firme propósito de mantener su papel como centro de alerta y respuesta nacional ante posibles incidentes.

102k
nombres de sitios web detectados que hacen referencia al COVID-19

57k
dominios, de los 80.000 detectados, se crearon en el mes de marzo.

También se ha detectado que algunos troyanos como **Trickbot y Emotet** -programas que aparentemente realizan una función útil para quien lo ejecuta, pero que en realidad realiza una acción que el usuario desconoce, generalmente dañina - han evolucionado sus tácticas, técnicas y procedimientos para evadir la detección, utilizando las noticias relacionadas con el coronavirus.

"Repunte de campañas de phishing relacionadas con la pandemia del COVID-19"

Listas negras, informes y vulnerabilidades

De todos los dominios detectados, algunos de ellos tienen fines legítimos y otros están dedicados a realizar campañas de spam o phishing, entre otras acciones. Para frenar estas campañas y reducir el impacto en organizaciones e instituciones, el CCN-CERT ha recopilado en tres listas los indicadores de compromiso que permiten la detección y bloqueo de estas campañas.

14
informes de análisis de código dañino que hacen uso de la temática del COVID-19

18
alertas y avisos publicados sobre riesgos y vulnerabilidades en servicios externos.

3
listas negras publicadas con indicadores de compromiso.

Asimismo, el Centro Criptológico Nacional está alertando de vulnerabilidades en sistemas operativos, navegadores y servicios de ciberseguridad, para urgir a usuarios y administradores la implementación de parches de seguridad con el fin de evitar la exposición a ataques externos.

Respuesta

Actividades de respuesta e intercambio de información sobre las campañas de malware relacionadas el COVID-19.

Actividades destacadas

Análisis
318
investigaciones sobre amenazas que utilizan la narrativa del COVID-19.

Soluciones
2
soluciones del CCN para responder a ciberataques desplegados en la red.

Coordinación nacional
44
CERTS nacionales, en contacto para fomentar el intercambio.

Seguridad ampliada
125
representantes de CC.AA. y servicios de salud, en un mismo grupo de trabajo.

Análisis e investigación de campañas

A través de REYES, herramienta desarrollada por el CCN-CERT para el intercambio y análisis de información sobre ciberamenazas, se han realizado 264 investigaciones sobre amenazas que utilizan la narrativa del COVID-19. De manera extraordinaria, se está facilitando el acceso a esta solución a los organismos pertenecientes a la comunidad de referencia del CCN para que dispongan de información actualizada sobre indicadores de compromiso y brechas de seguridad.

Asimismo, con el objetivo de reducir la superficie de exposición, se han activado, para Comunidades Autónomas y para el sector salud, dos plataformas (Trillion y HIBP) que permiten conocer si una organización ha sufrido una brecha de seguridad, así como la posible exposición de credenciales robadas.

318
investigaciones sobre amenazas que utilizan la narrativa del COVID-19.

+40k
elementos de información recopilados sobre campañas motivadas por el COVID-19.

Impulso al despliegue de soluciones para responder a ciberataques

MicroCLAUDIA: centro de vacunación que, mediante el despliegue de "vacunas" permite prevenir la infección de equipos informáticos. Esta solución está orientada a complementar y ampliar las funcionalidades de los antivirus para evitar que el código dañino más, como el ransomware, se ejecute en sus entornos.

CLAUDIA: solución del CCN-CERT que permite tener una visión más completa de lo que ocurre en los ordenadores de una organización. Su objetivo principal es la detección de código dañino complejo y de Amenazas Persistentes Amenazas (APT).

2
soluciones del CCN para mejorar la seguridad del trabajo en remoto.

"Comunidad y confianza, bases de nuestra ciberseguridad"

Coordinación nacional y grupos de intercambio

El CCN y la Secretaría General de Administración Digital han activado el Grupo de trabajo de Seguridad Ampliado, compuesto por 125 representantes de departamentos de seguridad de Comunidades y Ciudades Autónomas, servicios de salud de CC.AA. y el Ministerio de Sanidad, con el objetivo de reforzar la seguridad del sector sanitario. Este grupo constituye el principal instrumento de coordinación.

125
representantes de CC.AA. y servicios de salud, en un mismo grupo de trabajo

6
grupos de intercambio de información en los que participa el CCN.

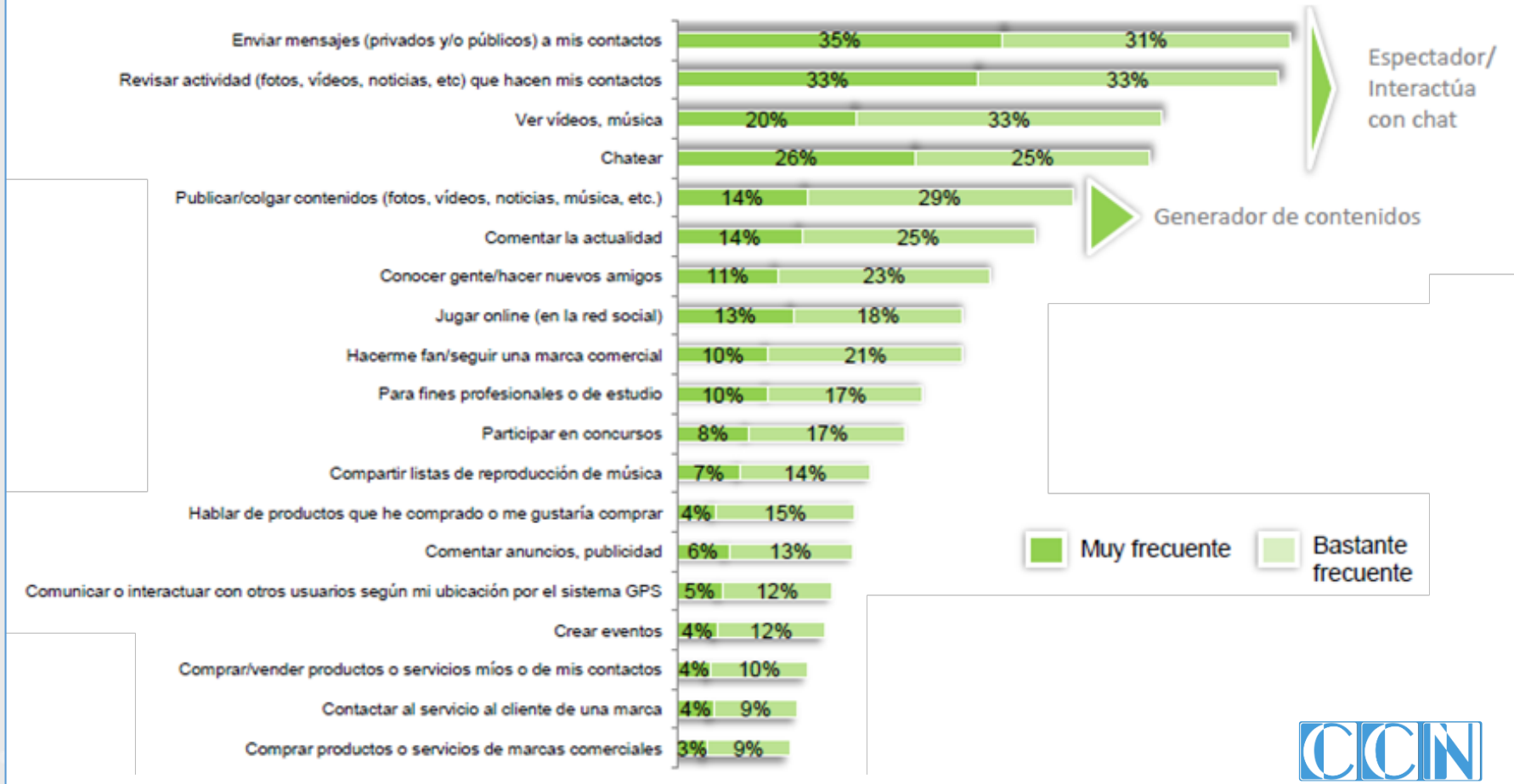
44
CERTS nacionales, en contacto para fomentar el intercambio.

Asimismo, el CCN está participando en seis grupos de intercambio de información, nacionales e internacionales, para optimizar la cooperación frente a posibles problemas de seguridad informática. Entre estos grupos destaca el foro CSRIT.ES compuesto por 44 equipos nacionales de respuesta a incidentes de seguridad (CERT) públicos y privados, y que dispone de un canal de comunicación para el intercambio de información sobre amenazas relacionadas con el COVID-19.

CCN
centro criptológico nacional

Redes Sociales

Los motivos principales para pertenecer a una red social (por lo menos en aquellas donde es necesario crear un perfil), es el **mantenerse en contacto** con amigos y conocidos, o **crear nuevos contactos.**



centro criptológico nacional

Huella Digital

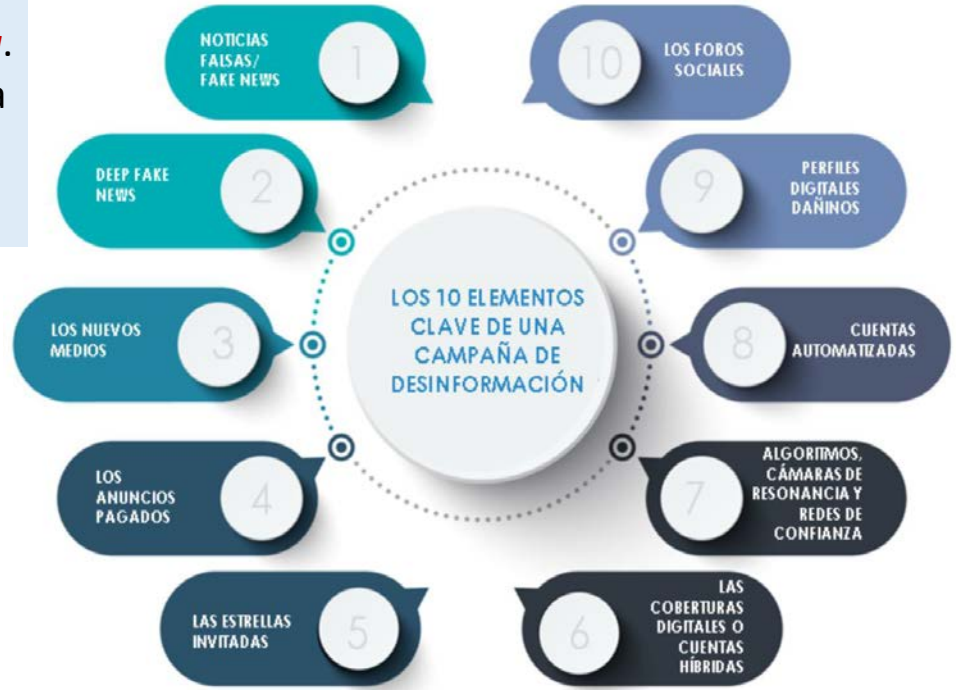
La **"huella digital" de nuestra vida, consciente o desapercibida, tendrá un enorme valor económico en el futuro,** y se podrá vender e intercambiar por efectivo, descuentos, productos o servicios que cada vez están más personalizados y adaptados al cliente.

Capacidad de predecir / influir

A través de un acuerdo comercial con Facebook (uso app *ThisIsYourDigitalLife* para tests de personalidad), CAMBRIDGE ANALYTICA recolectó más de 50 millones de datos de usuarios, permitiendo explotar su actividad en redes sociales privadas para luego utilizarla mediante la técnica del *microtargeting* para ANUNCIOS POLÍTICOS durante las elecciones presidenciales de 2016 en EE.UU.

Desinformación

Una campaña sistemática y maliciosa de distribución de desinformación entre la opinión pública pueden derivar en *indeseadas consecuencias para una democracia*. La manera más efectiva de articular una prevención eficaz y una resiliencia efectiva ante las acciones de desinformación es PROTEGIENDO y ORIENTANDO al eslabón habitualmente más vulnerable de estos ataques: LOS CIUDADANOS.



Consecuencias de un ataque de desinformación

Necesidad de un **TOOLKIT**, cuyo objeto sea *establecer los marcadores preventivos, los indicadores de presencia y las características constituyentes* que permitan identificar una campaña de desinformación **de una manera temprana, objetivada y basada en la evidencia**.

La Desinformación se debe Afrontar como Amenaza

Diferentes estudios sobre el uso de Internet y los hábitos de consumo de información digital sugieren que cerca del **90 por ciento de la población española entre 16 y 65 años puede ser potencialmente víctima** de un ataque de desinformación

Contramedidas

- **Analizar** la fuente de las noticias.
- Mantenerse **alerta** de contenidos patrocinados de **origen desconocido**.
- **Desconfiar** de **estrellas invitadas**.
- **Pensamiento crítico** y cabeza fría.
- **Tú puedes** parar un conflicto.

Como actuar frente a las campañas de desinformación en el ciberespacio, se ha convertido en uno de los **retos de seguridad para un Estado**.

CCN centro criptológico nacional

La Desinformación se debe Afrontar como Amenaza

1. Atribución

2. Causalidad

3. Objetivar la amenaza

4. Neutralización de la amenaza

5. Contranarrativa

CCN
centro criptológico nacional

Protocolo para Analizar la Desinformación

Fases	Área de acción	Alcance	Descripción de medidas
1. Definición	-	-	Fase inicial de las operaciones en la que se define si la monitorización de posibles acciones de desinformación podría estarse llevando a cabo para afectar de manera general a varios dominios de la realidad o como interferencia específica sobre dominios específicos, como procesos electorales, economía o seguridad internacionales, u otras. La aproximación del alcance en este punto no es detectar contenidos falsos o desinformativos, sino establecer las funciones y condiciones de preparación de un sistema de monitorización enfocado en el conjunto total de información que esté siendo difundida en el contexto de los dominios de interés definidos, para posteriormente recolectar toda esa información en bruto para clasificarla en función de su potencial amenazante.
2. Obtención masiva de información	Monitorización de contenidos	Dominio	Centrada en el dominio o los dominios de realidad definidos en fase 1.
		Palabras Clave	Centrada en palabras clave específicas seleccionadas por representar el dominio o los dominios de monitorización.
		Semántica	Centrada en construcciones lingüísticas específicas, expresiones escritas o contenido multimedia que podrían estar relacionados con el dominio de interés.
	Monitorización de fuentes	Identidades de interés	Observación de identidades conocidas sobre las cuales ya existe una evaluación previa respecto de que son referenciales en el dominio de interés monitorizado.
		Identificación de bots	Marcado de identidades que tienen probabilidad de ser bots o agentes máquina operando en la distribución de contenidos monitorizados en el dominio de interés.
		Identificación de interacciones por dominio	Clasificación y baremación de las interacciones más significativas con contenidos por parte de IDI y de bots.

Indicadores asociados a falta de transparencia

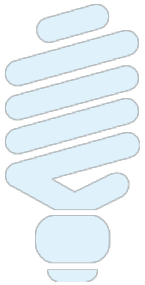
Menos de cinco años de antigüedad

No aparecen personas responsables o personas ajenas al periodismo o la información lideran el proyecto

Las **noticias no están firmadas** o están copiadas de otros medios

No aparece el nombre de la empresa editora

Posiciona el contenido mediante el uso de **cuentas automatizadas** en redes sociales



No aparece una dirección de correo

No aparece un número de teléfono visible

Publica noticias falsas

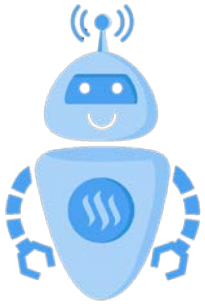
Publica noticias manipuladas

No aparece una sede física

Protocolo para Analizar la Desinformación

Fases	Área de acción	Alcance	Descripción de medidas
1. Definición	-	-	Fase inicial de las operaciones en la que se define si la monitorización de posibles acciones de desinformación podría estarse llevando a cabo para afectar de manera general a varios dominios de la realidad o como interferencia específica sobre dominios específicos, como procesos electorales, economía o seguridad internacionales, u otras. La aproximación del alcance en este punto no es detectar contenidos falsos o desinformativos, sino establecer las funciones y condiciones de preparación de un sistema de monitorización enfocado en el conjunto total de información que esté siendo difundida en el contexto de los dominios de interés definidos, para posteriormente recolectar toda esa información en bruto para clasificarla en función de su potencial amenazante.
2. Obtención masiva de información	Monitorización de contenidos	Dominio	Centrada en el dominio o los dominios de realidad definidos en fase 1.
		Palabras Clave	Centrada en palabras clave específicas seleccionadas por representar el dominio o los dominios de monitorización.
		Semántica	Centrada en construcciones lingüísticas específicas, expresiones escritas o contenido multimedia que podrían estar relacionados con el dominio de interés.
	Monitorización de fuentes	Identidades de interés	Observación de identidades conocidas sobre las cuales ya existe una evaluación previa respecto de que son referenciales en el dominio de interés monitorizado.
		Identificación de bots	Marcado de identidades que tienen probabilidad de ser bots o agentes máquina operando en la distribución de contenidos monitorizados en el dominio de interés.
		Identificación de interacciones por dominio	Clasificación y baremación de las interacciones más significativas con contenidos por parte de IDI y de bots.

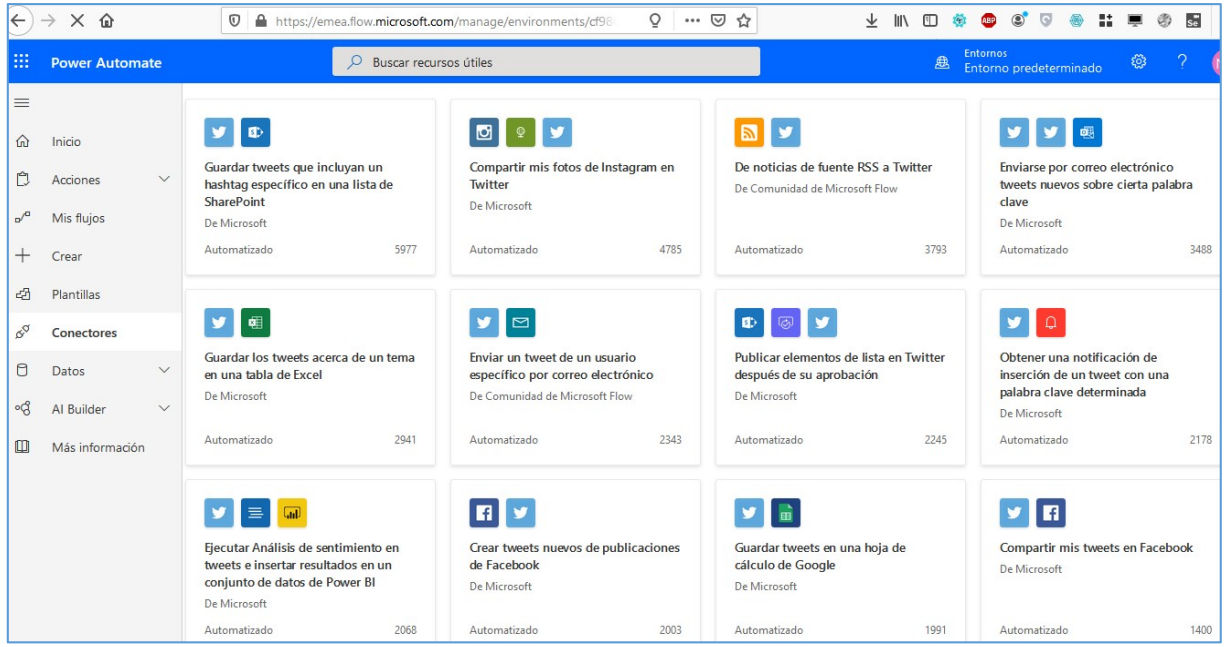
2 Recolección de Información

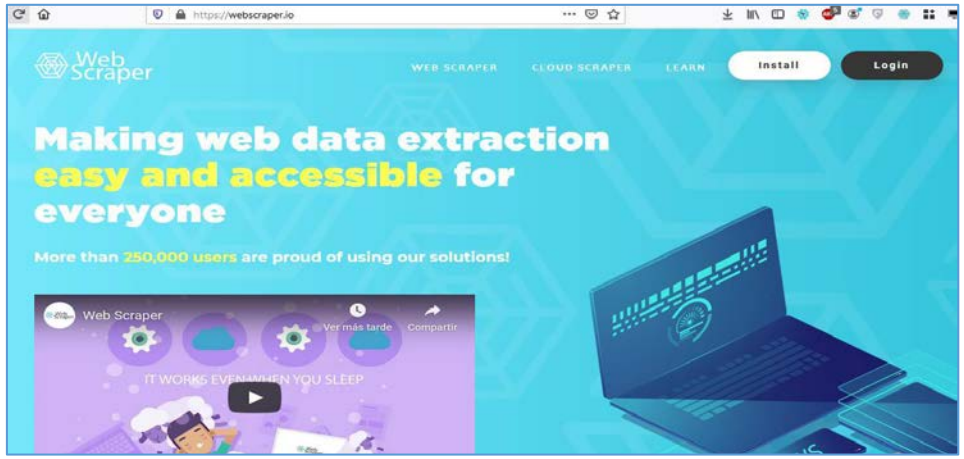


Identificación de los perfiles más influyentes en cada comunidad.

La visualización de la red de perfiles que presentan una alta actividad en cada comunidad es un **indicador** de que puede haber una red **de perfiles automatizados que intentan deliberadamente posicionar cierta narrativa** en la conversación digital.

Sin embargo, este indicador *no mide la influencia real* de estas presuntas cuentas automáticas.





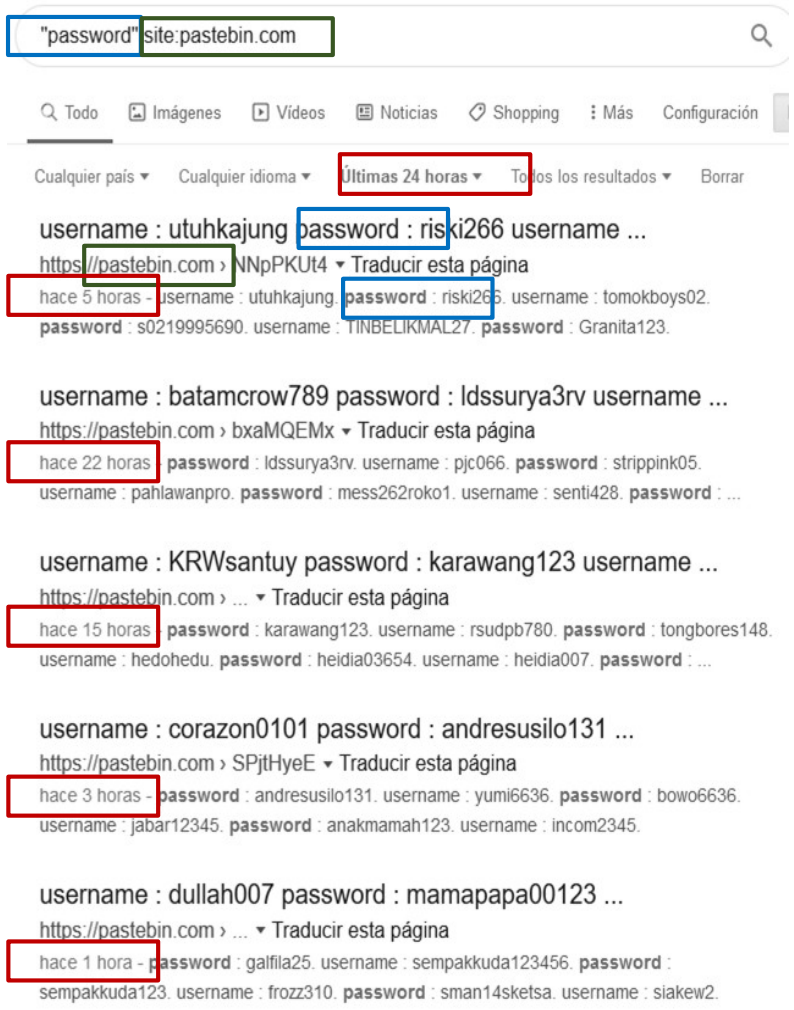
centro criptológico nacional

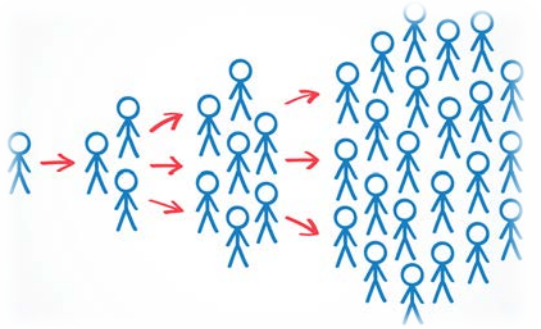
2 Recolección de Información

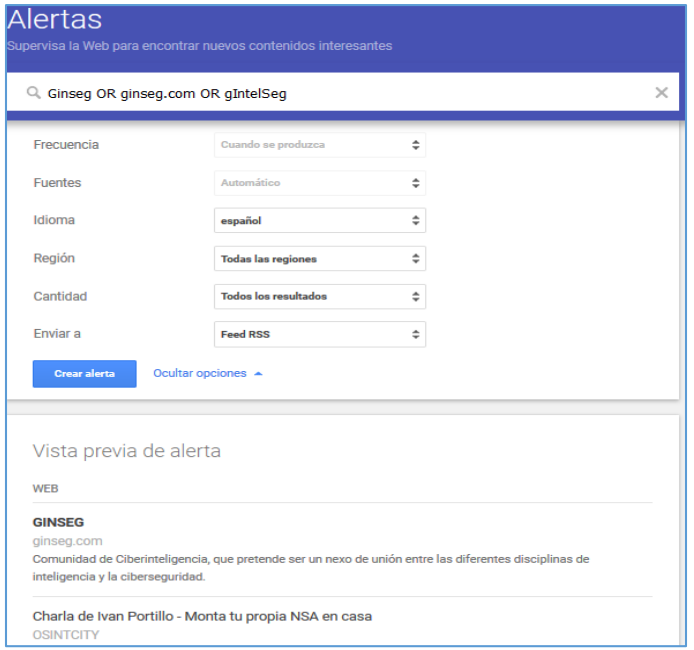
Identificación de los dominios más compartidos en cada comunidad.

Analizar los medios y las plataformas digitales cuyas noticias y mensajes se están distribuyendo **con mayor viralidad** en toda la conversación.

Este proceso es muy importante porque **permite determinar la presencia en la conversación de medios de difícil trazabilidad, plataformas de noticias de creación reciente o medios extranjeros** que se dedican a introducir maliciosamente ciertas narrativas que contribuyen a la polarización de la opinión pública.







CCN centro criptológico nacional

2 Recolección de Información

Análisis de contenido de los perfiles y dominios maliciosos. Detección de amenazas y vulnerabilidades explotadas por actores maliciosos.

Una vez detectada y localizada la red de presuntos perfiles y plataformas digitales maliciosas, es necesario realizar un **seguimiento detallado de las narrativas que se generan y distribuyen en la conversación con el objetivo de alterar y polarizar la opinión pública.**

- **Fake news.** Noticias que *no tienen relación con hechos reales*, pero que pueden ser creíbles y, sobre todo, *atractivas para el lector*. El principal objetivo de esta noticia es erosionar o cuestionar la confianza de los ciudadanos en sus instituciones públicas.

- **Medias verdades.** Narraciones que *se basan en algún hecho real*, que proporciona una dosis de credibilidad, pero que ha sido manipulado y aderezado con falsedades, transmitiendo un mensaje fraudulento en envoltorio con apariencia de veracidad.

- **Noticias manipuladas sobre aspectos de polarización social.** Un tercer grupo de narrativas maliciosas serían aquellas que, *aunque basadas en hechos reales*, magnifican ciertas puntos de debate social en los Estados democráticos para, desde ellos, incrementar la tensión y la polarización manipulando la componente emocional de las informaciones.

Protocolo para Analizar la Desinformación

Fases	Área de acción	Alcance	Descripción de medidas
3. Evaluación	Clasificación	Falsos contenidos	Clasificación y baremación de información obtenida en bruto sobre su índice de falsedad
		Contenidos desinformativos	Clasificación y baremación de información obtenida en bruto en función de su potencial sesgo amenazante.
	Alcance	Nacional	Evaluar si la diseminación de información ya clasificada es nacional en origen.
		Exterior	Evaluar si la diseminación de información ya clasificada procede del extranjero en origen.
	Riesgo	Intenciones	Según la clasificación y alcance evaluados sobre la información en bruto, proporcionar una inferencia sobre probables intenciones de amenaza.
		Capacidades	En función de la infraestructura dilucidada en la fase 2 y de la evaluación realizada, proponer una hipótesis sobre las potenciales capacidades de la amenaza.
4. Planificación	Definición de las reglas de respuesta	-	Una vez evaluada como amenaza una infraestructura que disemina contenidos falsos o desinformativos en un dominio de interés, definir las reglas de respuesta en el despliegue de capacidades operacionales según las necesidades tácticas y estratégicas nacionales y el marco legal aplicable.
	Hoja de ruta operacional	Desactivación	Diseño y preparación de recursos para desactivar la amenaza si ésa fuera la opción elegida en las reglas de respuesta.
		Vigilancia	Diseño y preparación de recursos para efectuar un seguimiento de la amenaza, si fuera la opción elegida en las reglas de respuesta.
		Instrucción judicial	Diseño y preparación de recursos para encausar judicialmente a la amenaza si fuera la opción elegida en las reglas de respuesta.
		Inteligencia	Diseño y preparación de recursos para desplegar operaciones de inteligencia sobre la amenaza si fuera la opción elegida en las reglas de respuesta.

Evaluación

En las campañas de desinformación se **analiza el contenido de las publicaciones**, para desentrañar …

- La **narrativa empleada** por el atacante;
- La **infraestructura de canales** mediante los cuales se transmiten las publicaciones;
- y el **comportamiento de las identidades** que diseminan los contenidos, para elaborar un perfilado del "ejército desinformativo" desplegado por el atacante.
- A partir de esos elementos, se **infieren las intenciones y las capacidades de la campaña desinformativa**.
- El reto es anticiparse intentando **identificar** a actores disruptivos coordinados y no reales, **desplegar contramedidas** de contención, **mitigación** y, en su caso, **desactivación** de la infraestructura desinformativa.

Evaluación

Más del **90 % de índice de desconfianza**, por lo tanto alta posibilidad de ser una **plataforma desinformativa**.

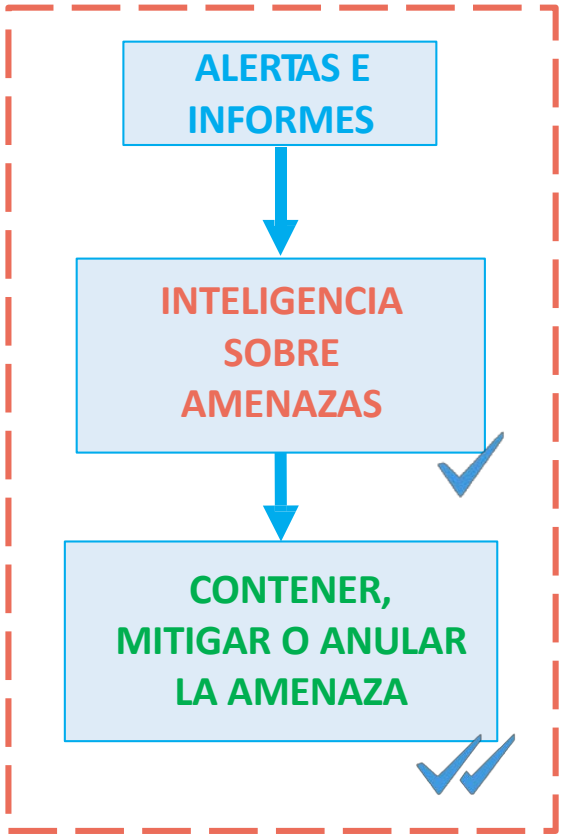
Seguimiento diario de sus narrativas para la elaboración de los **informes quincenales**.

Productos del Servicio

- **Alerta Situacional o Alerta de Incidente.**
  - Información descriptiva.
  - Evaluación. Incluye propuesta de atribución.
  - Peligrosidad. Nivel de peligro que se estima.

- **Informes de Seguimiento:**
  - Evolución de una alerta concreta o conjunto de alertas.
- **Informes de Reconocimiento.**
  - Reconocimiento de un foro o perfil de usuario,
  - Análisis de contactos, relaciones, comentarios, etc…

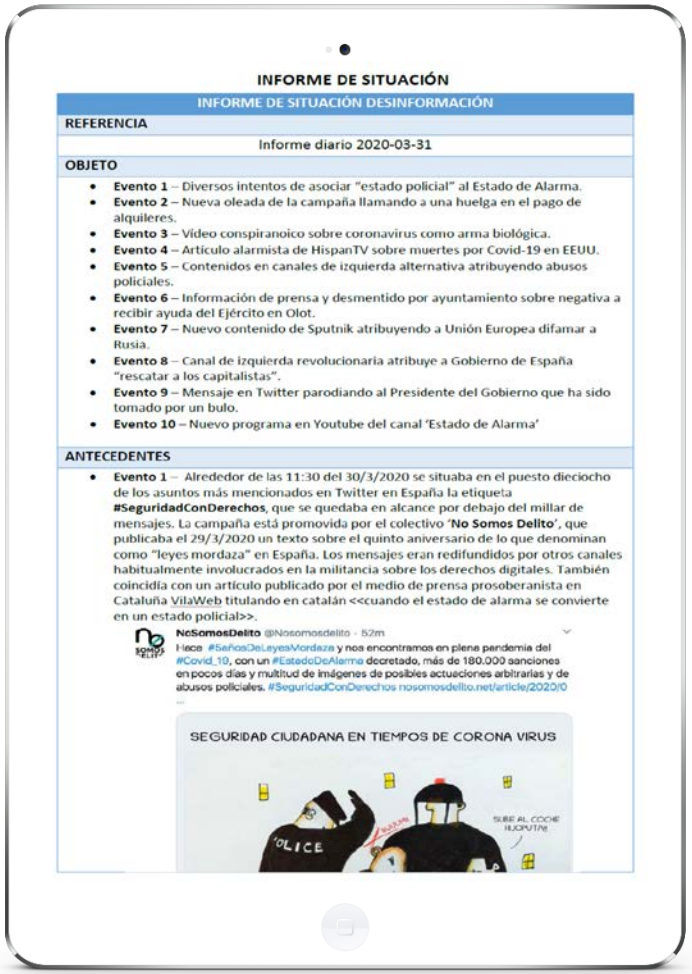
- **Informes de Identidad.**
  - Descripción ampliada de la presencia de una identidad en el ciberespacio.
  - Narrativas, comportamientos, intenciones y contactos del objetivo.



Productos del Servicio

Entregables

- Informe diario
- Informe agregado/semanal ELISA



INFORME DE SITUACIÓN

INFORME DE SITUACIÓN DESINFORMACIÓN

REFERENCIA

Informe diario 2020-03-31

OBJETO

- **Evento 1** – Diversos intentos de asociar "estado policial" al Estado de Alarma.
- **Evento 2** – Nueva oleada de la campaña llamando a una huelga en el pago de alquileres.
- **Evento 3** – Vídeo conspiranoico sobre coronavirus como arma biológica.
- **Evento 4** – Artículo alarmista de HispanTV sobre muertes por Covid-19 en EEUU.
- **Evento 5** – Contenidos en canales de izquierda alternativa atribuyendo abusos policiales.
- **Evento 6** – Información de prensa y desmentido por ayuntamiento sobre negativa a recibir ayuda del Ejército en Olot.
- **Evento 7** – Nuevo contenido de Sputnik atribuyendo a Unión Europea difamar a Rusia.
- **Evento 8** – Canal de izquierda revolucionaria atribuye a Gobierno de España "rescatar a los capitalistas".
- **Evento 9** – Mensaje en Twitter parodiando al Presidente del Gobierno que ha sido tomado por un bulo.
- **Evento 10** – Nuevo programa en Youtube del canal 'Estado de Alarma'

ANTECEDENTES

- **Evento 1** – Alrededor de las 11:30 del 30/3/2020 se situaba en el puesto dieciocho de los asuntos más mencionados en Twitter en España la etiqueta **#SeguridadConDerechos**, que se quedaba en alcance por debajo del millar de mensajes. La campaña está promovida por el colectivo '**No Somos Delito**', que publicaba el 29/3/2020 un texto sobre el quinto aniversario de lo que denominan como "leyes mordaza" en España. Los mensajes eran redifundidos por otros canales habitualmente involucrados en la militancia sobre los derechos digitales. También coincidía con un artículo publicado por el medio de prensa prosoberanista en Cataluña VilaWeb titulando en catalán <<cuando el estado de alarma se convierte en un estado policial>>.

NoSomosDelito @Nosomosdelito · 52m
Hace #SeñasDeLeyesMordaza y nos encontramos en plena pandemia del #Covid_19, con un #EstadoDeAlarma decretado, más de 180.000 sanciones en pocos días y multitud de imágenes de posibles actuaciones arbitrarias y de abusos policiales. #SeguridadConDerechos nosomosdelito.net/article/2020/0

USO OFICIAL

CCN-CERT ELISA-08/20

Informe de seguimiento de narrativas desinformativas ELISA
Especial Coronavirus V (23-30 marzo 2020)

<e/elisa>
Estudio Simplificado de fuentes abiertas

Marzo 2020

USO OFICIAL

centro criptológico nacional

Protocolo para Analizar la Desinformación

Fases	Área de acción	Alcance	Descripción de medidas
5. Respuesta	Aplicación de la Hoja de Ruta	-	Despliegue de los recursos y tácticas decididas en la fase 4.
	Contramedidas de resiliencia	-	Despliegue de los recursos necesarios para proteger a los objetivos a victimizar por la campaña desinformativa de los efectos perjudiciales y tóxicos de esa campaña.
	Contranarrativa	-	Producir narrativas para inyectar en medios de comunicación web general y redes sociales para contrarrestar los efectos de los contenidos falsos o desinformativos.
	Contradecepción	-	Diseñar y poner en práctica recursos de contradecepción si de la evaluación realizada en la fase 4 se concluye que la intención de la amenaza es la decepción.

En las campañas de desinformación *no se analiza el contenido de las publicaciones*, sino el *comportamiento de los perfiles*, lo que hacen "*behind the scenes*".

Es *improbable frenar una operación de desinformación una vez se ha desencadenado*. Lo que se intenta es *anticiparse* analizando preventivamente su infraestructura de operaciones y metodologías de difusión de información, *intentando identificar a actores disruptivos coordinados y no reales*.

Soluciones de Seguridad

CCN
centro criptológico nacional

Proveer Servicios / Dar Soluciones

Auditoría

- /inés>
- /pilar>
- /amparo>
- /clara>
- /rocío>
- /emma>
- /ana>

Detección

- /sat-inet>
- /sat-sara>
- /sat-ics>

Análisis

- /gloria>
- /maría>
- /marta>

Vigilancia

- /carmen>
- /claudia>
- /reyes>
- /elisa>

Intercambio

- /lucía>
- /loreto>

Formación

- /vanesa>

ATENEA

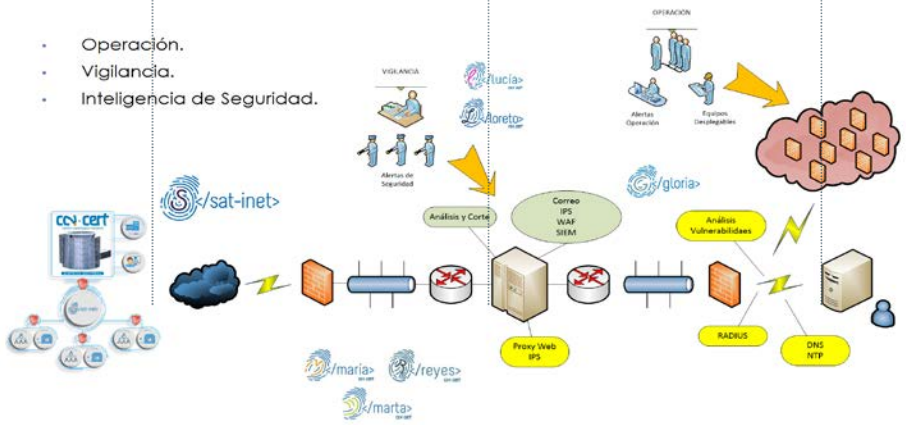
Las “chicas” del CCN que nos ayudan a estar protegidos

por Comunicación dooingIT
en ciberseguridad, Ciberseguridad para todos, RGPD, tecnología
en 23/10/2019

Estos días leía un artículo en el que ponía que menos del 25% de las mujeres se dedican a la ciberseguridad. Quizás tenga mucho que ver también ese número con el hecho de que el número de mujeres en carreras tecnológicas (las llamadas STEM) es muy pequeño. Pero este artículo no va de eso, en dooingIT tenemos a una de las que suma a ese 25%, por lo que no nos podemos quejar ... este artículo va de Pilar, Carmen, Lucía, Loreto .... ¿Quiénes son?

ens Esquema Nacional de Seguridad

- Operación.
- Vigilancia.
- Inteligencia de Seguridad.



SOC AGE
SOC SGNTJ

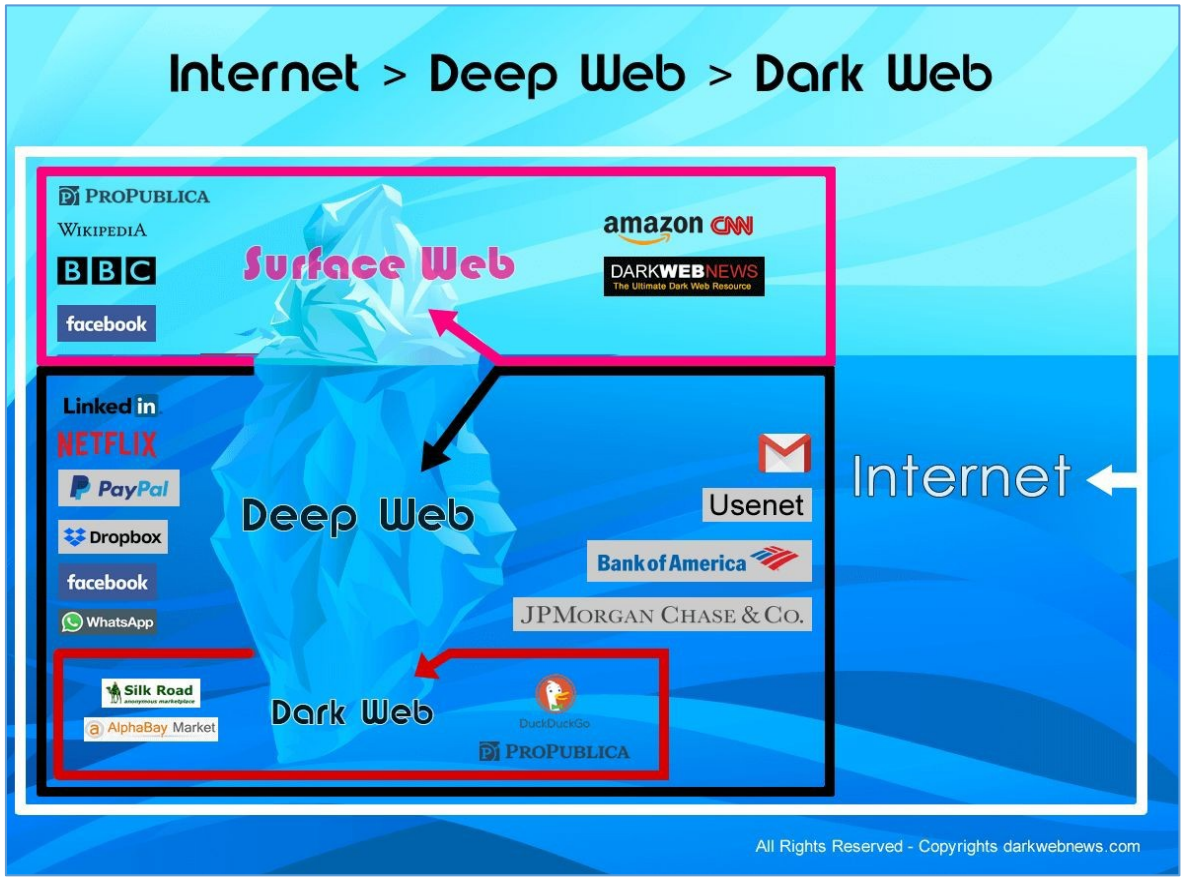
CCN
centro criptológico nacional

Servicio de Cibervigilancia

La misión de un Servicio de Cibervigilancia es **PROPORCIONAR INFORMACIÓN DE VALOR** sobre la presencia de **CIBERAMENAZAS** que permita adoptar decisiones para prevenirlas, mitigarlas, controlarlas, contenerlas o anularlas.

- Combatir nuevo modelo de conflicto (**acciones deliberadamente ambiguas**) cuyo objetivo es **desestabilizar el estado** adversario y **polarizar a su sociedad**.
- **Evitar generar dudas** sobre la *integridad del proceso* o *sus participantes* (**injerencia de los estados en procesos electorales**).
- Disponer de *observatorios digitales* para realizar un seguimiento de lo que sucede, realizar **prospectiva digital**, en el ciberespacio.
- Optimizar el Servicio de Cibervigilancia articulando su estructura interna a través del despliegue de dos (2) equipos:
  - **Equipo de Alerta:** elaboración de contenidos para el Equipo de Análisis.
  - **Equipo de Análisis**: la evaluación pone en contexto a la amenaza y proporciona a los sistemas de respuesta una mayor capacidad de decisión y acción inteligente.

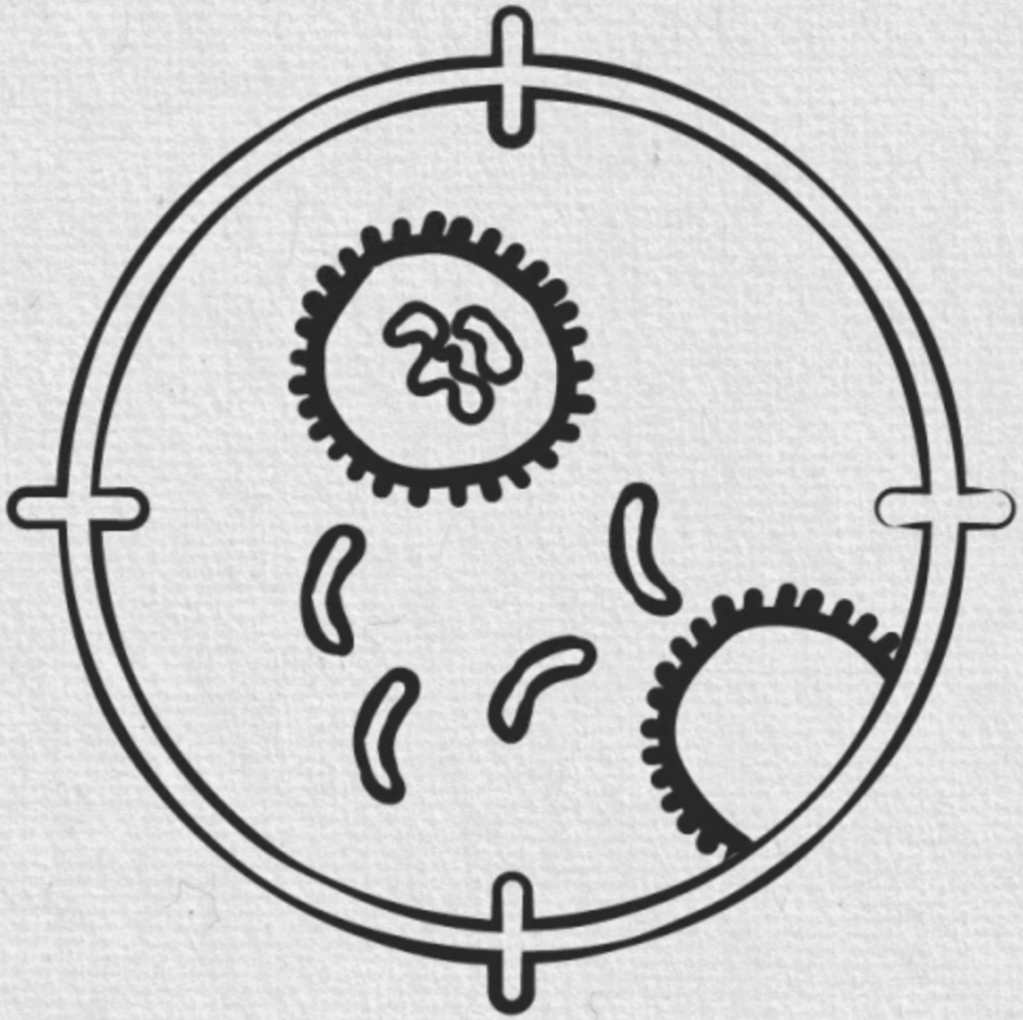
Ciberterritorios a Explorar



Desmontando el Mito

CCN
centro criptológico nacional

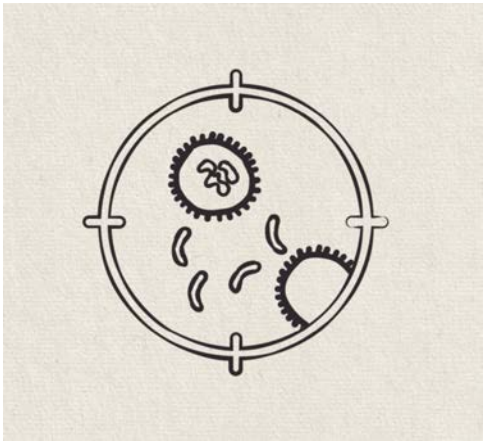
Objetivo: Buscar la “colmena” de la desinformación



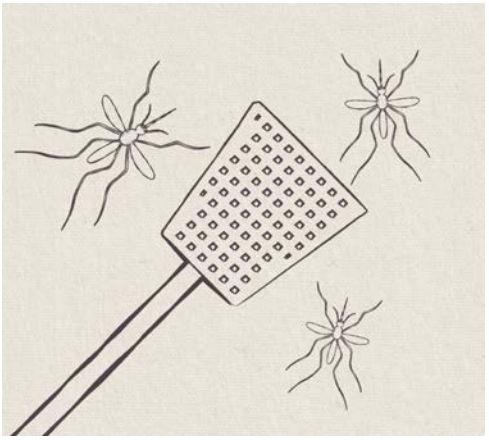
ELISA

Una herramienta para la identificación y prevención temprana de la desinformación en su primera fase operativa

Prevenible



Fuera de control



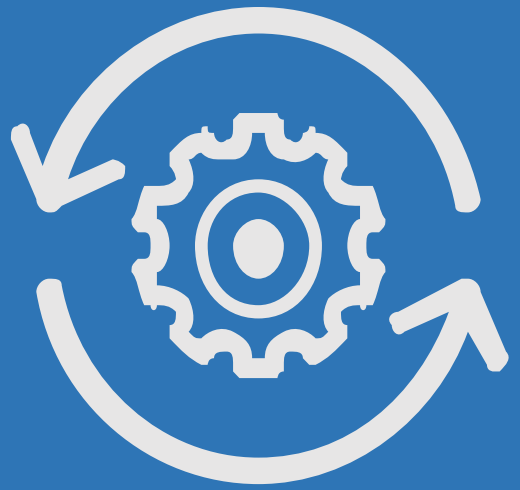
CCN
centro criptológico nacional

Valor añadido y aportación a la determinación de la desconfianza

- Implementa una metodología para la detección temprana de acciones de desinformación:
- Objetiva las características que cumplen las narrativas desinformativas
- Define los indicadores clave para la detección temprana de las narrativas desinformativas
- Identifica, en base a indicadores, las plataformas que difunden contenido desinformativo y malicioso
- Detección temprana de las principales narrativas desinformativas que se generan y distribuyen para erosionar el contrato social del Estado.
- Evidenciar la convergencia y posible coordinación entre diferentes plataformas, canales y actores desinformativos que comparten y difunden el mismo contenido malicioso

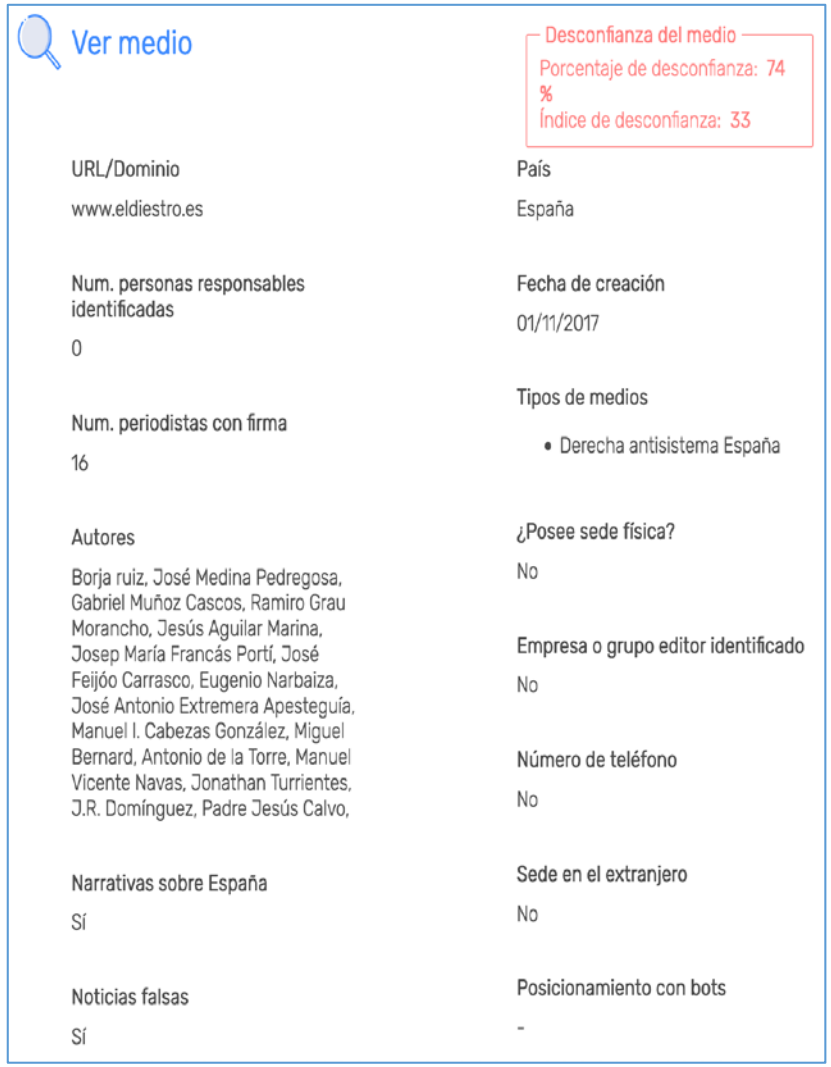
Características de las narrativas desinformativas

elisa
Estudio Simplificado de fuentes abiertas



- Opacas: se generan por plataformas, canales y actores digitales de escasa transparencia y trazabilidad.
- Simulan veracidad: Utilizan la distorsión del contenido narrativo y de la identidad de sus emisores para intentar crear en el receptor una "apariencia de verdad" o una "verdad alternativa", manipulando creencias o emociones de quienes son audiencia potencial de los mensajes.
- Antisistémicas: atacan las vulnerabilidades del contrato social de las sociedades democráticas.

Índice de desconfianza sobre canales/plataformas digitales



Indicadores que definen las características del canal

Característica	Puntos ponderación
Menos de un año de antigüedad	2
0 personas responsables identificadas	2
0 autores reales con firma	2
1-5 periodistas con firma	1
No tiene sede física	0,5
No existe una empresa/grupo editor identificado	0,5
No aparece dirección de correo electrónico	0,5
No aparece número de teléfono	0,5
Publica noticias falsas	3
Publica noticias manipuladas	1
Sede en un país extranjero	2
Posiciona contenido con bots	2
Total posible	17
Alto indicador de maliciosidad	>10

Índice de desconfianza sobre canales/plataformas digitales

Indicadores de definición de narrativas

Narrativas maliciosas que difunde	Puntos ponderación
Anti Immigración	2
Anti Semitismo	4
Pro Homofobia	1
Pro Islamofobia	1
Anti Vaticano/Papa/Catolicismo	1
Anti Globalismo/Anti Nuevo orden mundial	4
Anti feminismo/Igualdad	1
Denigra instituciones/autoridades del Estado	1
Pro movimientos independentistas	1
Pro movimientos identitarios nacionalistas anti-secesionistas	1
Difunde imagen de Estado como violento y/o corrupto	1
Fomenta Revisionismo histórico	1
Fomenta conspiración Chemtrails	2
Teorías conspirativas de alteración elecciones	2
Teorías conspirativas de redes de pederastia vinculadas al Estado/instituciones	2
Desprestigio a medios de comunicación tradicionales	1
Anti sistema financiero/pro regreso del patrón oro/anti economía liberal	4
Anti vacunas/anti farma/anti ciencia/	4
Vida extraterrestre	1
Negación versión oficial atentados/crímenes	2
Anti multeralismo (OTAN/UE/Euro/UN/FMI/Banco Mundial)	2
Anti tratados libre comercio/liberalismo/globalismo	1
Defensa de Eurasia/vinculación con Aleksandr Duguin	4
Supremacismo racial	1
Utiliza redes sociales alternativas (VK.gab.ai...)	1
Anti americanismo	1
MK Ultra/políticas de control social	1
Pro anonymous/wikileaks	1
Anti europeísmo/Anti Euro	2
Negación cambio climático	1
Gran alerta por el cambio climático	1
Alerta 5G	1
Total posible	52
Alto indicador de maliciosidad	>23

Índice de desconfianza sobre canales/plataformas digitales

Apoyo expreso a países/movimientos políticos extranjeros

Rusia/Líderes nacionalismo ruso | Irán | China | Nacionalismo húngaro | Alt Right EEUU | Venezuela/Chavismo | Italia/Nacionalismo/populismo italiano | Francia/Frente Nacional | Francia/Chalecos amarillos | Movimientos independentistas europeos | Extrema derecha española (ADÑ -Respeto) y/o Europea | UK/Brexit | Populismo/nacionalismo Brasil | Populismo Argentina | Bolivarismo/indigenismo | Corea del Norte | Bashar Al Assad | Palestina | Grupos terrorista etno/nacionalistas | Grupos terroristas religiosos | Grupos eco-terroristas

Colaboración/sinergia/publicación cruzada con canales extranjeros. Publican contenido de estas webs

RT | Sputnik | Telesur | Hispan TV | CCCTV | SANA | Otros medios financiados o patrocinados por gobiernos extranjeros…

Indicadores que definen el apoyo expreso a países/movimientos políticos extranjeros

País/movimiento social/político	Puntos ponderación
Rusia/Líderes nacionalismo ruso	2
Irán	2
China	1
Nacionalismo húngaro	1
Alt Right EEUU	1
Venezuela/Chavismo	1
Italia/Nacionalismo/populismo italiano	1
Francia/Frente Nacional	1
Francia/Chalecos amarillos	1
Movimientos independentistas europeos	1
Extrema derecha española (ADÑ -Respeto) y/o Europea	1
UK/Brexit	1
Populismo/nacionalismo Brasil	1
Populismo Argentina	1
Bolivarismo/indigenismo	1
Corea del Norte	1
Bashar Al Assad	1
Palestina	1
Grupos terrorista etno/nacionalistas	1
Grupos terroristas religiosos	1
Grupos eco-terroristas	1
Total posible	23
Altas indicador de maliciosidad	>5

Indicadores que definen la colaboración/sinergia/publicación cruzada con canales de comunicación vinculados a gobiernos extranjeros. Publican contenido de estas webs, sus responsables colaboran con estas webs

Medio extranjero	Puntos ponderación
RT	1
Sputnik	1
Telesur	1
Hispan TV	1
CCCTV	1
SANA	1
Otros medios financiados o patrocinados por gobiernos extranjeros…	1
Total posible	7
Alto indicador maliciosidad	>2

Identificación del nivel de opacidad de plataformas desinformativas

		1.Fecha de creación	2. Personas responsables identificadas	3. Periodistas con firma	4. Sede física		5. Empresa/grupo editor identificado		6. Dirección de correo visible		7. Número de teléfono visible		8. Pubilca noticias falsas		9. Publica noticias manipuladas		11. Posiciona contenidos con bots/perfiles automatizados		
					4.1. Sí	4.2. No	5.1.Sí	5.2. No	6.1. Sí	6.2. No	7.1. Sí	7.2. No	8.1. Sí	8.2. No	9.1. Sí	9.2. No	11.1. Sí	11.2. No	11.3. N/S
1	https://www.geopolitica.ru/es	jul-00	1	360		1	1		1			1	1		1				1
2	https://katehon.com/es	dic-14	7	11		1	1		1			1	1		1				1
3	https://www.strategic-culture.org/	jun-10	0	100		1		1	1			1	1		1				1
4	https://www.voltairenet.org/es	ago-05	1	11		1	1		1			1	1		1				1
5	https://www.globalresearch.ca/	jun-01	1	8426		1	1		1			1	1		1				1
6	https://orientalreview.org/	ene-10	0	20		1		1	1			1	1		1				1
7	https://redinternacional.net/	mar-18	0	40		1		1	1			1	1		1				1
8	https://geopolitico.es/	3/8/16	0	3		1		1	1			1	1		1				1
9	http://elespiadigital.com/	2011	2	20		1		1	1		1		1		1				1
10	Joan Fdez. https://www.youtube.com/user/pppppee/videos	feb-07	0	0		1				1		1	1		1				1
11	https://adversariometapolitico.wordpress.com/	N/S	0	0		1				1		1	1		1				1
12	https://elmundodeloslocos.wordpress.com/	N/S	0	0		1		1		1		1	1		1				1
13	http://selenitaconsciente.com/	sep-15	1	0		1			1			1	1		1				1
14	https://berlinconfidencial.com/	mar-17	0	0		1		1		1		1	1		1				1
15	http://astillasderealidad.blogspot.com/	15/12/2011	0	0		1		1		1		1	1		1				1
16	http://www.verdadypaciencia.com/	14/08/2012	0	0		1		1		1		1	1		1				1
17	https://conspiracionesblog.wordpress.com/	sep-14	0	0		1		1		1		1	1		1				1
18	https://www.mundodesconocido.es/	ago-06	1	1		1		1		1		1	1		1				1
19	https://www.nostratv.com/	oct-16	1	5		1		1		1		1	1		1				1
20	http://rafapal.com/	mar-04	1	1		1	1		1			1	1		1				1
21	https://falsasbanderas.wordpress.com/	N/S	1	0		1	1			1		1	1		1				1
22	https://cazadebunkers.wordpress.com/	N/S	1	3		1		1		1		1	1		1				1
23	https://eladiofernandez.wordpress.com/	N/S	1	0		1				1		1	1		1				1
24	http://quienestadetras.emiweb.es/	Ago-2016	1	1		1		1	1			1	1		1				1
25	https://www.lanuevatribuna.com/	dic-17	1	1		1	1		1			1	1		1		1		
26	https://www.alertanacional.es/	ago-18	0	0		1		1		1		1	1		1				1
27	https://elarconte.com/	abr-17	1	1		1		1				1	1		1				1
28	Aquí la voz de Europa/Democracia Nacional. https://www.youtube.com	feb-16	2	9		1		1	1		1		1		1				1
29	https://www.elespañoldigital.com/	may-18	0	11		1		1		1		1	1		1				1
30	https://kaosenlared.net/	jun-01	0	37	1		1		1			1	1		1		1		
31	https://movimientopoliticoderesistencia.blogspot.com/	n/S	0	58		1		1		1		1	1		1				1
32	https://www.lahaine.org/	ago-01	0	24		1		1		1		1	1		1				1
33	https://contralapropagandamediatica.blogspot.com/	1/10/14	0	0		1		1		1		1	1		1				1
34	http://www.resumenlatinoamericano.org/	15/08/2013	1	13	1			1	1			1	1		1				1
35	http://plataformadistritocero.blogspot.com/	30/09/2012	0	0		1		1		1		1	1		1				1
36	http://www.alfredojalife.com/; https://www.youtube.com/channel/U	1/1/10	1	1		1	1		1			1	1		1				1
37	http://canaltlv1.com/	1/1/12	1	17	1		1		1			1	1		1				1
38	https://benjaminfulford.net/	9/12/09	1	1		1		1	1		1		1		1				1
39	https://thetruthrevolution.net/	12/2/16	0	0			1	1		1		1	1		1				1
40	www.alterinfo.ch	6/9/18	0	1		1		1		1		1	1		1		1		
41	http://www.whatdoesitmean.com/	12/11/03	0	0		1		1		1		1	1		1				1
			21	15		37		27		21		38	41		41				
			51.20%	36.50%		90.24%		65.80%		51.20%		92.60%	100%		100%				

CCN
centro criptológico nacional

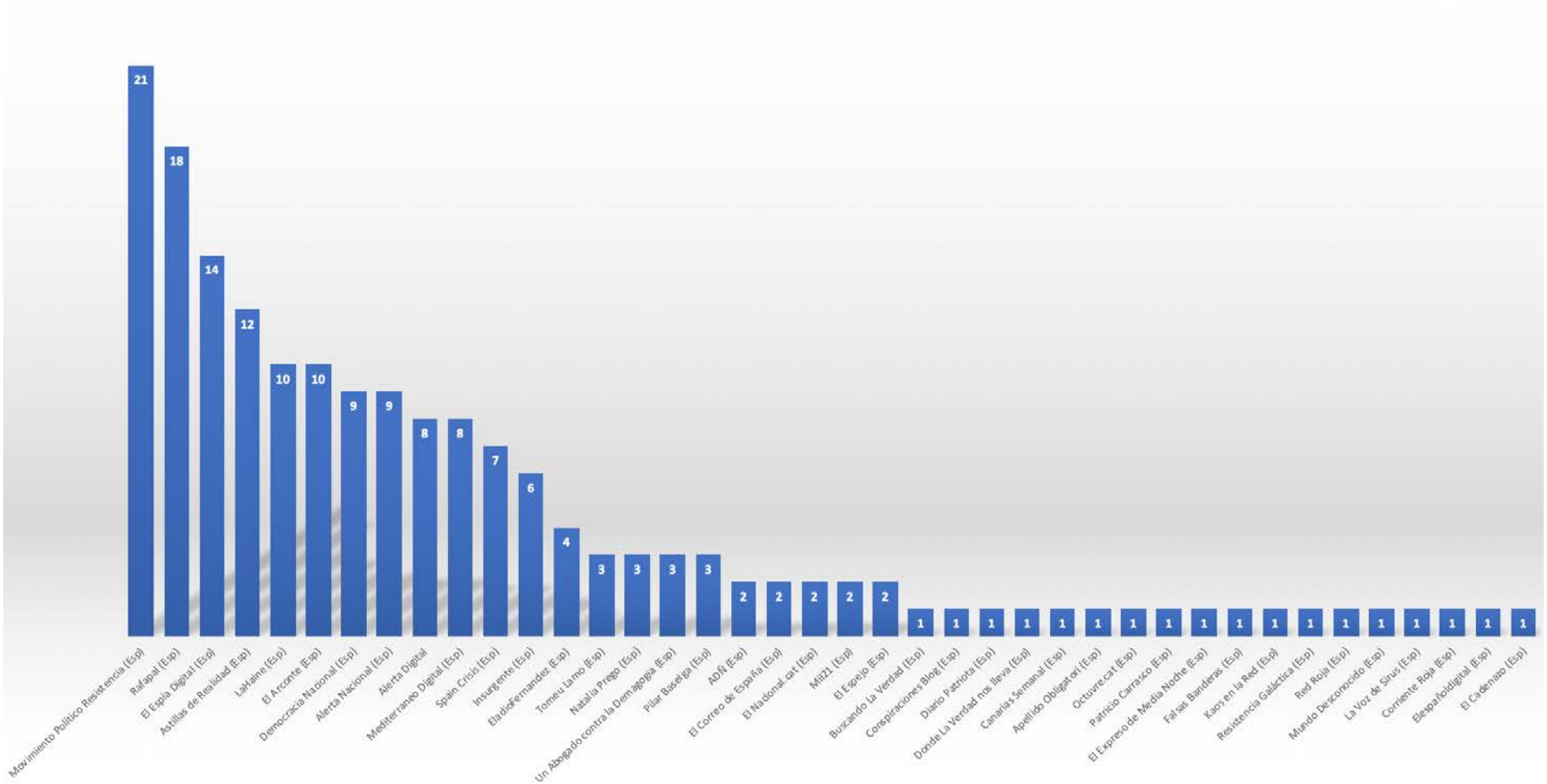
Indicadores asociados a las narrativas antisistema

- Contrarias a la credibilidad del pensamiento científico
- Contrarias a la credibilidad de las instituciones públicas nacionales
- Contrarias a la credibilidad de las instituciones públicas multilaterales
- Contrarias a la credibilidad de las instituciones y el sistema financiero
- Contrarias a la credibilidad de los medios de comunicación
- Contrarias a la cohesión social y el pluralismo de la Sociedad
- Creación de enemigos externos

Detección de narrativas maliciosas sobre el coronavirus en España

ELISA

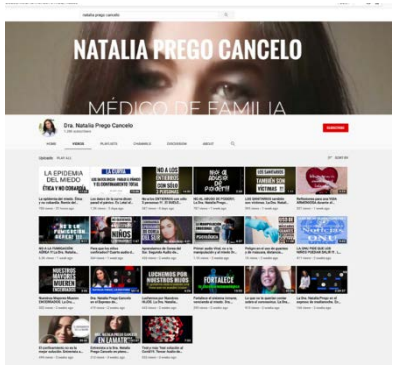
Estudio simplificado de fuentes abiertas



centro criptológico nacional

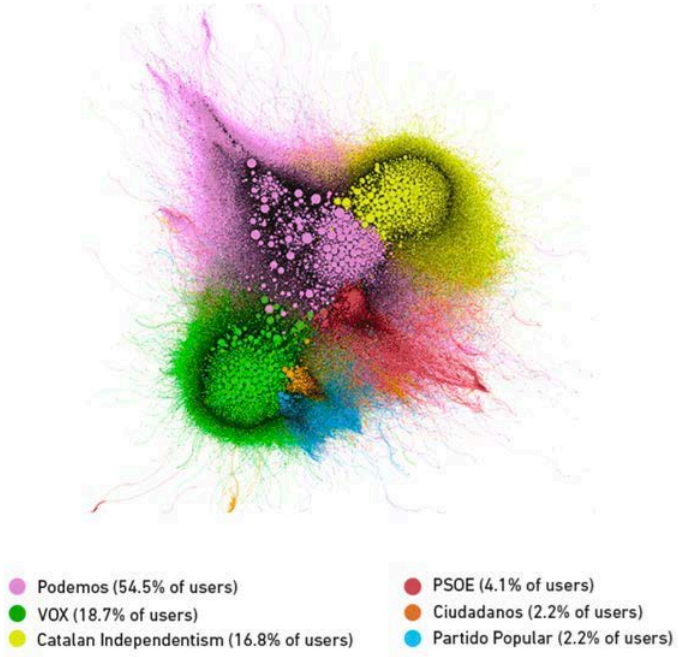
Contenidos desinformativos más activos sobre el coronavirus en España

El seguimiento diario de estas **74 plataformas digitales** del 25 de abril al 2 de mayo ha permitido identificar un total de **500 narrativas maliciosas** (basadas en mentiras, medias verdades o hechos descontextualizados) sobre el origen y las consecuencias del coronavirus, tanto en España, como a nivel global.



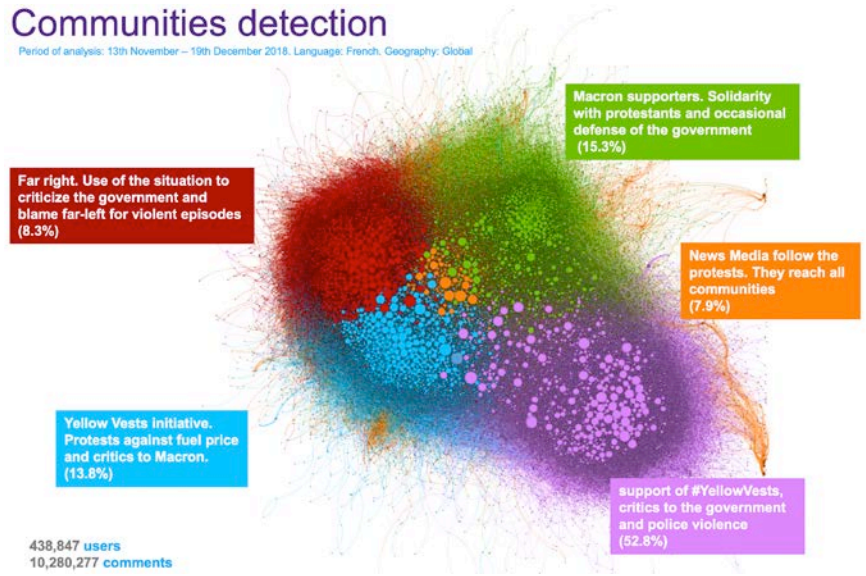
- Detectar la **magnitud de informaciones maliciosas** que se están generando en torno a una crisis de salud y política global y nacional.
- Identificar los **principales agentes de desinformación** sobre el coronavirus a nivel nacional e internacional.
- Identificar y comprender la probable colaboración entre **agentes desinformativos extranjeros y nacionales**.
- Identificar, agrupar y ordenar las **principales narrativas maliciosas** que se han generado en torno al coronavirus.

La desinformación se puede y debemos manejarla



Análisis de Comunidades

Análisis de Alta Actividad



Medios más Influyentes por Comunidad

centro criptológico nacional

Conclusiones

[CL/01] Ecosistema de la ciberseguridad

El **ECOSISTEMA DE LA CIBERSEGURIDAD** se enfrenta a un **INCREMENTO** constante en el número, sofisticación y complejidad de los ciberataques.

[CL/02] Implementar seguridad

No se puede dejar de hacer uso de la tecnología, pero se debe **IMPLEMENTAR SEGURIDAD**, utilizar **TECNOLOGÍA CERTIFICADA** y abusar del **SENTIDO COMÚN.**

[CL/03] Superficie de exposición

La **SUPERFICIE DE EXPOSICIÓN** es susceptible de **INCREMENTAR**: redes sociales, teléfonos móviles, BYOD, IoT… y hay que manejarla evitando ser un objetivo fácil de atacar (No ser un Objetivo Blando).

[CL/04] Tiempos de respuesta

La ciberseguridad pasa por **MEDIR**, conocer la superficie de exposición y reducir al mínimo los **TIEMPOS DE RESPUESTA.**

[CL/05] Mejora continua

Adoptar la **MEJORA CONTINUA** como reto a lograr, foto dinámica a optimizar progresivamente **EN BASE A COMPROMISOS E HITOS** adoptados por todos los actores involucrados.

[CL/06] Buenas Prácticas

Educar al usuario de la tecnología en procedimientos y **BUENAS PRÁCTICAS** reduce la superficie de exposición,

La importancia de Construir Comunidad

CN-CERT centro criptológico nacional

CCN centro criptológico nacional

Aproximación posibilista…

Camino a seguir…

1. Estrategia de ciberseguridad.
2. Gobernanza de la ciberseguridad.
3. **Desarrollo reglamentario posibilista.**
4. CSIRT de referencia, sectoriales y SOCs.
5. **Capacidad de detección y alerta temprana.**
6. **Incremento de vigilancia (SOC).**
7. Capacitación y búsqueda de talento.
8. **Cooperación pública-privada. (comunidad**)
9. Intercambio de información. (confianza)
10. Comunicación y promoción. (ser referencia)

… Ciberseguridad es un asunto de Seguridad Nacional

CCN centro criptológico nacional

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@ccn.cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

</loreto>

http://ccn-cert.net/ciberv-chile

Contraseña: C1b3rCHILE2020

CCN centro criptológico nacional 15 años

CCN centro criptológico nacional ccn-cert centro criptológico nacional ccn-pytec centro criptológico nacional