Red Nacional de SOC

Código ético y de conducta profesional

CCN-CERT centro criptológico nacional

Febrero 2024

Índice

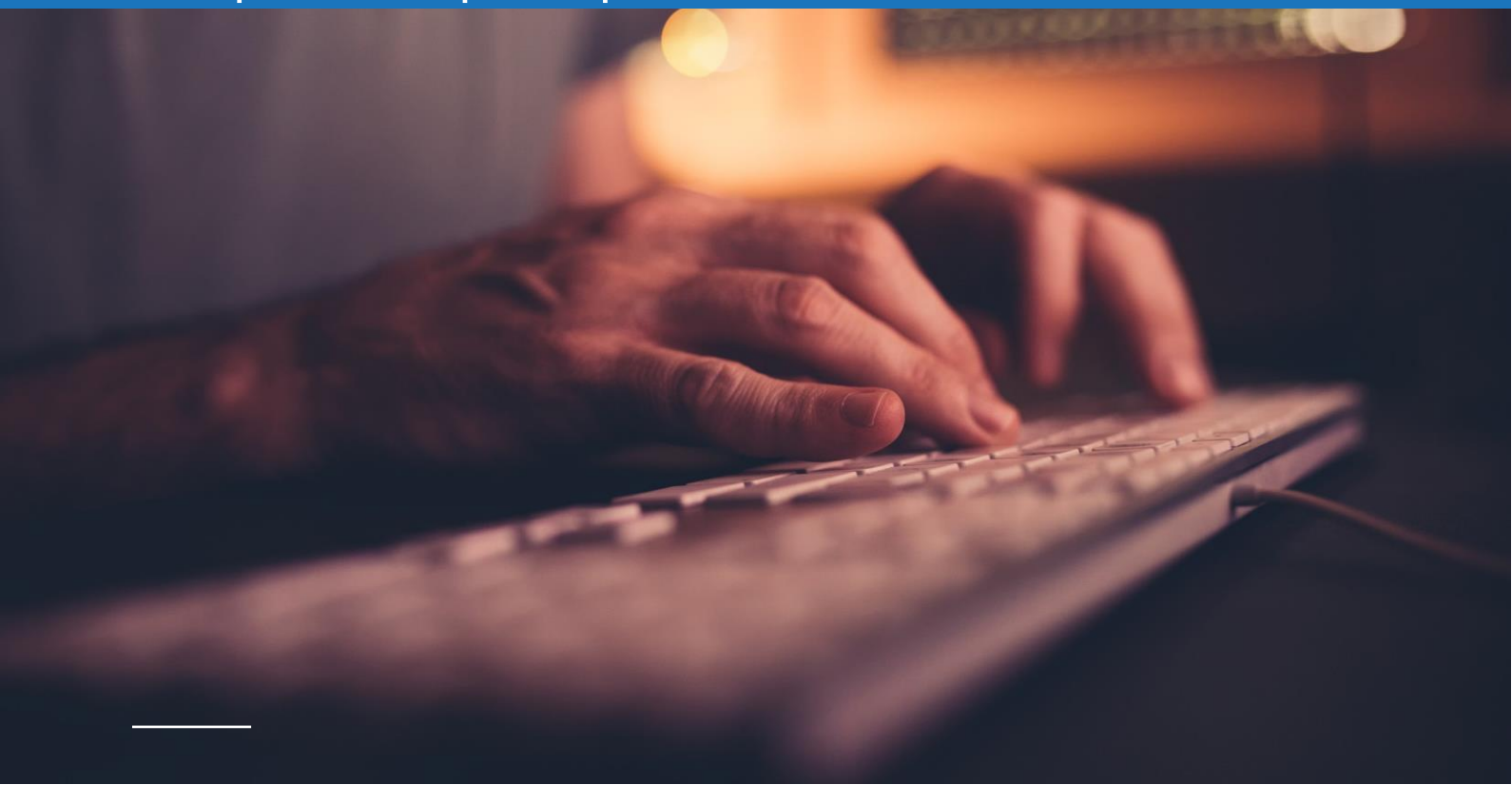
Contexto

El presente documento ha sido elaborado a partir del código de conducta propuesto por SIG Ethics de FIRST, un grupo de interés centrado en ayudar a mejorar en gran medida la comprensión mundial de los CSIRT y su funcionamiento.

La elaboración del mismo pretende establecer una serie de buenas prácticas y normas de conducta ética que contribuyan a una mejor operación de los Centros de Operaciones de Ciberseguridad (en adelante, SOC) que forman parte de la Red Nacional de SOC de cara a fomentar la relación, colaboración y coordinación entre ellos. Formar parte de la Red Nacional SOC implica la aceptación tácita del presente código de conducta por parte de las entidades..

Deberes de las entidades que forman parte de la Red Nacional de SOC (en adelante, RNS)

Las entidades que forman parte de la RNS se comprometen tácitamente a cumplir los deberes expuestos en el presente punto. Es responsabilidad de cada entidad garantizar el cumplimiento de estos deberes por parte de sus personas participantes en la red:



Deber de contribuir a la consecución de los objetivos de la RNS

Las entidades contribuirán en la medida de lo posible a la consecución de los objetivos de la RNS, siendo estos:

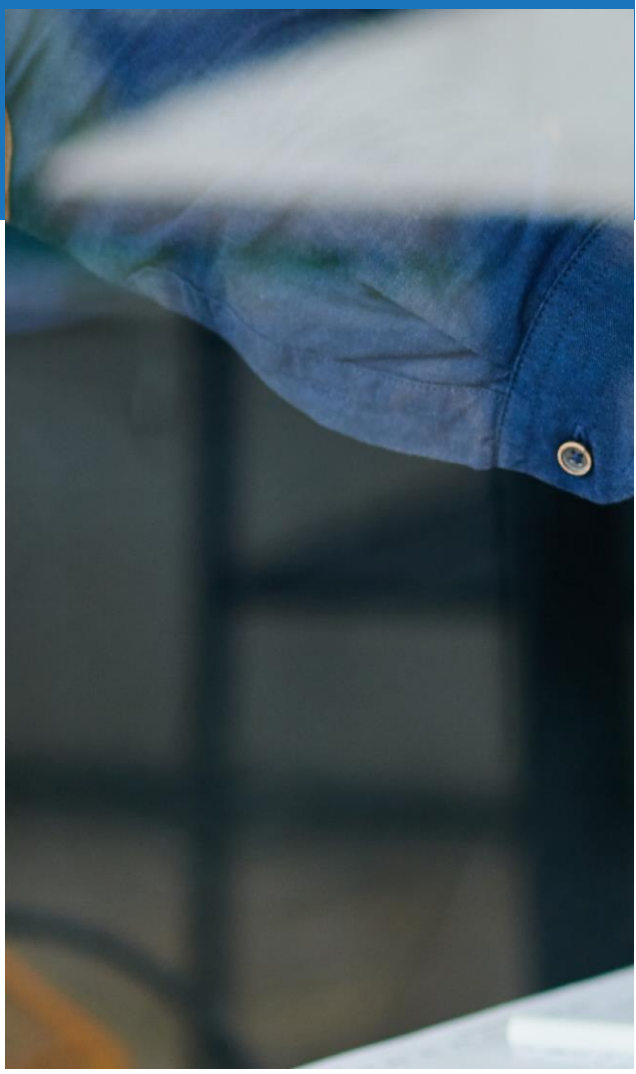
Compartir indicios de ataques para mejorar la detección y protección. Se quiere fomentar la colaboración entre todos los miembros de la red en la investigación y posible detección temprana de un ciberincidente basados en estos indicios.

Compartir información relevante sobre incidentes de seguridad y cualquier otro tipo de información de inteligencia que se considere de utilidad.

Lanzar acciones coordinadas y recomendaciones ante situaciones que así lo requieran.

Deber de asistencia a las reuniones de la RNS y presencia en el chat

Las entidades deberán asistir por norma general a las reuniones que se organicen y deberán estar presentes en el sistema de mensajería instantánea que se utiliza. Igualmente, deberán participar activamente en los grupos definidos dentro del sistema de mensajería instantánea.



Deber de confianza

La comunidad de la RNS se basa en esta confianza, y solo puede seguir funcionando de esta manera si puede existir un nivel de confianza razonable entre las entidades.

La confianza significa que las entidades solo deben **1) asumir compromisos que puedan cumplir**, **2) comportarse de manera previsible respecto de los demás miembros**, y **3) mantener la relación de confianza que tienen con otras entidades.**

Deber de revelación responsable de vulnerabilidades o indicios de ciberincidente

Las entidades que se enteren de una vulnerabilidad deben optar por una divulgación responsable y coordinada de la misma, cooperando con las partes interesadas con el objetivo de remediarla y reducir al mínimo el daño asociado a su divulgación.

En el caso de ser un indicio de detección, no se compartirán datos que identifiquen a la organización donde se ha detectado. El objetivo es conocer la forma del ataque y los patrones de comportamiento del malware o del atacante para poder ser detectados por los miembros de la RNS. Los miembros de la red pueden colaborar activamente en la investigación con los datos de las redes que protegen.

Deber de no intentar sacar provecho de los incidentes que sufran o gestionen otras entidades

Las entidades no deben intentar sacar provecho de incidentes que hayan sufrido o estén sufriendo otras entidades o su ámbito de actuación. El hecho de intentar obtener beneficio de una situación así es poco ético e irrespetuoso y puede dañar la relación con respecto a otras entidades.

Gestión de incumplimientos

Las entidades podrán alertar del incumplimiento de algunos de los deberes por parte de algún otro miembro. El CCN-CERT gestionará tales situaciones en coordinación con las entidades involucradas y atendiendo al presente código de conducta y al bien común de la iniciativa como consideración primordial.

El resultado de la investigación por parte del CCN-CERT podrá derivar en la expulsión de la red.

Red
Nacional de
SOC

Liderado por CCN-CERT