TLP:WHITE

Proyecto Código ético y de conducta profesional de FIRST

Los miembros de los equipos de respuesta en caso de incidente y de seguridad (Equipos) tienen acceso a muchos sistemas y fuentes de información digitales. Sus acciones pueden cambiar el mundo. Como miembro de esta profesión, un miembro de un Equipo debe reconocer la responsabilidad respecto de sus mandantes y de otros profesionales de la seguridad, así como respecto de la sociedad en general. La persona también debe reconocer su responsabilidad respecto de su propio bienestar.

Este Código se ha concebido para inspirar y guiar la conducta ética de todos los miembros del Equipo, incluidos los profesionales actuales y potenciales, los instructores, los estudiantes, las personas influyentes y cualquiera que utilice la tecnología informática de una manera que tenga repercusiones. El Código incluye principios formulados como declaraciones de responsabilidad, basados en el entendimiento de que el bien público es siempre la consideración primordial. Cada principio se complementa con directrices que ofrecen explicaciones para ayudar a los profesionales de la computación a comprender y aplicar el principio.

A continuación se presentan los deberes, pero no figuran por orden de importancia. Estos deberes no deben considerarse como requisitos absolutos, sino como se indica en el RFC2119 de la IETF para la definición de "DEBERÍA":

> "en determinadas circunstancias, pueden existir motivos válidos para hacer caso omiso de un elemento en particular, pero deben tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de optar por una vía diferente".

Para más información respecto de la manera de tratar posibles dilemas, véase el Apéndice A.

Deber de confianza

La confianza es la base de muchas relaciones entre los Equipos, y a menudo es necesaria antes de que pueda producirse un intercambio de información significativo. La comunidad de FIRST se basa en esta confianza, y sólo puede seguir funcionando de esta manera si puede existir un nivel de confianza razonable entre los Equipos.

La confianza significa que los miembros del Equipo sólo deben 1) asumir compromisos que puedan cumplir, 2) comportarse de manera previsible respecto de los demás Equipos (por ejemplo, respetar la norma TLP), y 3) mantener la relación de confianza que tienen con otros Equipos.

Inicialmente, la relación de confianza debe ser asumida y tener carácter transitivo, es decir, confianza la primera vez que se utiliza (*Trust on First Use* – TOFU), y hacer posible la confianza de los Equipos en los que confían otros Equipos.

Deber de revelación de vulnerabilidad coordenada

Los miembros del Equipo que se enteren de una vulnerabilidad deben optar por una divulgación coordinada de la misma, cooperando con las partes interesadas para remediar la vulnerabilidad de seguridad y reducir al mínimo el daño asociado a la divulgación. Las partes interesadas incluyen, entre otros, el informante de la vulnerabilidad, los proveedores afectados, los coordinadores, los defensores y los clientes, socios y usuarios.

Los miembros del Equipo deberían coordinarse con las partes interesadas correspondientes para acordar plazos y expectativas claros a efectos de la divulgación de la información, proporcionando suficientes detalles para permitir a los usuarios evaluar su riesgo y adoptar medidas defensivas viables.

Deber de confidencialidade

Los miembros del Equipo tienen el deber de mantener la confidencialidad cuando sea apropiado. Las solicitudes de mantener la confidencialidad de cierta información pueden hacerse de manera explícita, por ejemplo, usando el Protocolo de Semáforos (*Traffic Light Protocol* – TLP). Los miembros del Equipo deben respetar esas solicitudes siempre que sea posible. Si no es posible mantener en secreto la información debido, por ejemplo, a conflictos con los requisitos de la legislación local, con los contratos o con el deber de informar, el miembro del Equipo deberá informar inmediatamente de ese conflicto al propietario de la información.

Algunos deberes de confidencialidad se basan en leyes, reglamentos o costumbres. Si, durante la respuesta a un incidente, alguna de las partes está obligada a respetar o espera que se respete la confidencialidad sobre esta base, debe hacer todo lo posible por hacer explícita esa expectativa desde el principio. A partir de entonces, todas las partes deben atenerse a la expectativa antes mencionada de respetar las solicitudes explícitas de mantener la confidencialidad de la información siempre que sea posible.

Deber de acuse de recibo

Los Equipos reciben información de muchas fuentes diferentes: investigadores, clientes, otros Equipos, entidades gubernamentales, etc. Los miembros de los Equipos deben responder a las consultas de manera oportuna, aunque sólo sea para confirmar que la solicitud ha sido recibida. Cuando sea posible, los miembros del Equipo deben establecer expectativas respecto de la siguiente actualización.

Deber de autorización

Los miembros de los Equipos tienen una necesidad y un derecho legítimos de entender cuáles son sus áreas de responsabilidad, actuando sólo en los sistemas a los que están autorizados a acceder. Los miembros de los Equipos deben ser conscientes de la manera en que sus acciones pueden afectar a los demás integrantes del Equipo y asegurarse de que no causen daños adicionales en el desempeño de sus funciones. Deben explicarse las posibles consecuencias de

esas acciones a los interesados afectados. Siempre que sea posible, se debería consultar a los mandantes antes de introducir cambios en sus sistemas.

Deber de informar

Los miembros del Equipo deben considerar que es su deber mantener informados a sus mandantes respecto de las amenazas y los riesgos actuales para la seguridad. Cuando los miembros del Equipo tienen información que puede o bien afectar negativamente o bien mejorar la seguridad, tienen el deber de informar a las partes pertinentes o a terceros que puedan ayudar, con el esfuerzo apropiado, teniendo debidamente en cuenta las obligaciones de confidencialidad, la normativa en materia de privacidad u otras obligaciones.

Deber de respetar los derechos humanos

Los miembros del Equipo deben ser conscientes de que sus acciones pueden repercutir en los derechos humanos de los demás, al compartir información, aplicar un posible sesgo en sus acciones o infringir los derechos de propiedad. Los miembros del Equipo tienen acceso a una amplia gama de informaciones personales, delicadas y confidenciales en el curso de la gestión de los incidentes. Esta información debe manejarse de manera que se respeten los derechos humanos.

Durante la gestión de incidentes, los intervinientes no deben actuar de manera sesgada y deben hacer todo lo posible por eliminar el sesgo de sus procesos y de la toma de decisiones, ya sea la que llevan a cabo los intervinientes o la que se incorpora en los algoritmos.

A efectos de este principio, la noción de "propiedad" (Declaración de los Derechos Humanos de las Naciones Unidas: Artículo 17) incluye intangibles como la propiedad intelectual, así como las ideas y conceptos en general, con independencia de que estén legalmente protegidos (por ejemplo patentados).

Deber respecto de la salud del Equipo

Los Equipos tienen la responsabilidad de poder seguir prestando los servicios que han prometido a sus mandantes. Esta responsabilidad incluye la salud física y emocional del Equipo.

Con el fin de respetar a los miembros de un Equipo como personas y de permitir la viabilidad a largo plazo de mantener un nivel de servicio adecuado, un Equipo debe esforzarse por mantener un entorno de trabajo saludable, seguro y positivo que apoye la salud física y emocional de (todos) sus miembros. Para responder a una crisis, las operaciones "normales" deben contribuir a la salud emocional y a la reducción del estrés.

Deber respecto de la capacidad del Equipo

La gestión de incidentes es un tema en evolución que los miembros del Equipo deben estudiar continuamente. Un Equipo debe proporcionar a sus miembros recursos para que estudien, apliquen y avancen en los conocimientos tecnológicos y científicos dentro de su(s) área(s) de responsabilidad. La formación o los créditos educativos de CPE/CEU pueden contribuir a ello, pero los meros ejercicios de cumplimiento no son suficientes para cumplir este deber. El Equipo debe mantener una infraestructura tecnológica suficiente como para permitir la prestación de

sus servicios, incluidas medidas adecuadas para proteger dicha infraestructura frente a interferencias del exterior.

Deber de recopilación responsable

La recopilación de datos es necesaria para la respuesta en caso de incidente, pero debe establecerse un equilibrio entre el objetivo de la respuesta en caso de incidente y el respeto a los datos de las partes interesadas.

Durante una investigación, la cantidad de información que se necesita recopilar puede variar. Mientras avanzan en la respuesta a un incidente, los miembros del Equipo deben ir ajustando la información que están recopilando a la evolución de la necesidad.

Deben excluirse de los informes los datos que no sean directamente pertinentes a un incidente y su solución.

Los datos recopilados y extraídos deben manejarse de conformidad con la legislación aplicable y respetando la privacidad de los usuarios. Se debe pedir permiso antes de recopilar y procesar datos bajo control de un propietario de datos. Debe respetarse la normativa aplicable al tratamiento de los datos.

Los datos que puedan ayudar a otros equipos de respuesta en sus esfuerzos relacionados con otros incidentes deben ponerse a disposición de los mismos, posiblemente en forma redactada. La información que sea confidencial y de propiedad exclusiva sólo debería facilitarse con las protecciones adecuadas.

Antes de compartir datos con terceros con fines de mitigación, es preciso medir los riesgos en función de los beneficios. Los datos sólo deben compartirse si los beneficios superan claramente a los riesgos. Los datos sensibles deben almacenarse de manera que puedan ser fácilmente destruidos una vez que se haya dado por cerrado un incidente. Los datos recopilados deben ser destruidos de manera segura, con arreglo a las políticas de conservación de datos.

Deber de reconocimiento de los límites jurisdiccionales

Los miembros del Equipo deben reconocer y respetar los límites jurisdiccionales, los derechos legales, las normas y las autoridades de las partes involucradas en las actividades relacionadas con la respuesta a incidentes.

Las leyes, los reglamentos y otras cuestiones jurídicas, como son las relacionadas con la protección de la privacidad o las notificaciones en caso de quiebra de la seguridad de los datos, pueden diferir en función de las jurisdicciones implicadas. Los límites jurisdiccionales pueden venir determinados tanto por la ubicación física de las partes implicadas, como pueda ser el país o el domicilio, como por otros factores que afectan a dichas partes. Incluso dentro de un mismo país, las leyes y reglamentos pueden diferir entre las regiones políticas (por ejemplo, entre los distintos estados de los Estados Unidos) o entre los distintos negocios, industrias o sectores dentro de esa nación (por ejemplo, la atención de la salud, los servicios financieros, las instalaciones gubernamentales). Los EIISI nacionales pueden tener responsabilidades y/o autoridad atribuidas para las actividades que implican a los mandantes dentro de su propia jurisdicción, y también pueden colaborar con o "entregar" información y actividades a otras entidades que tienen autoridad para las jurisdicciones transfronterizas.

Los miembros del Equipo deben ser conscientes de las cuestiones clave que afectan a las jurisdicciones implicadas incluidas, entre otros, las normas de privacidad o los requisitos de notificación en caso de quiebra de la seguridad de los datos. Dado que las leyes y reglamentos de ciberseguridad y privacidad evolucionan y siguen actualizándose en todo el mundo, es aconsejable consultar con un asesor jurídico informado para obtener orientación siempre que las cuestiones impliquen múltiples límites jurisdiccionales.

Deber de razonamiento basado en pruebas

Los Equipos deben desarrollar su actividad sobre la base de hechos verificables. Cuando compartan información, como son los indicadores de compromiso o las descripciones de incidentes, los miembros del Equipo deben facilitar las pruebas y el alcance de forma transparente. Cuando ello no sea posible, deben darse junto con la información las razones para no compartir estas pruebas y el alcance.

Los miembros del Equipo deben abstenerse de divulgar o compartir rumores. Toda hipótesis debe señalarse claramente como tal.

La transparencia de las pruebas y de los procesos de razonamiento es importante incluso en el caso de intercambio automatizado, por ejemplo, durante el intercambio automatizado de grandes cantidades de información. En este caso, se debe comunicar una descripción del proceso de extracción de datos con un nivel de detalle que la haga inteligible.

Apéndice A

Lidiar con los dilemas

Los miembros del Equipo pueden encontrarse con frecuencia en una posición en la que ninguna acción parece satisfacer todos los principios éticos. En una situación de este tipo, hay que elegir a cuál de los principios hay que dar prioridad. En tales situaciones, se alienta a quienes manejan los incidentes a que reflexionen sobre cuáles son las partes interesadas y cómo pueden éstas verse afectadas por sus acciones, preferiblemente en un debate con un colega. Como regla general, debe elegirse la solución que suponga la menor infracción a este Código. En ocasiones, esto podría no ser posible, por ejemplo, debido a presiones externas. En tal caso, se recomienda proceder, señalando la existencia del dilema ético, y posiblemente expresando una protesta.