



## SOCIAL ENGINEER CAPTURE THE FLAG (SECTF)

### EKOPARTY 2020

### BASES Y CONDICIONES (v1.0)

#### CONSIDERANDO:

- Que las actividades que se desarrollan en la Ekoparty están relacionadas con la investigación, la difusión y la promoción del uso de tecnologías y sistemas de información y comunicación, al servicio de la humanidad;
- Que un CTF sirve para mostrar, a través de un método práctico, distintas técnicas de explotación de vulnerabilidades y las maneras de defenderse de las mismas;
- Que se trata de una dinámica conocida y aplicada en una gran cantidad de eventos de seguridad a nivel mundial;
- Que el objetivo de un CTF basado en estrategias de ingeniería social es estimular el sentido común y promover el trabajo en equipo;
- Que un CTF especializado en vishing contribuye a la concientización, herramienta fundamental para prevenir ataques de ingeniería social;
- Que, como en toda competencia, ciertas reglas deberán ser respetadas por los participantes y asistentes;
- Que ganar la competencia sirve para ayudar a incrementar la seguridad de los potenciales objetivos, no solamente para fines personales;
- Que se presume la buena fe por parte de todas aquellas personas que quieran participar de la Ekoparty;
- Que la intención de los organizadores (en adelante, **el comité organizador**) es continuar con la implementación de técnicas lúdicas de aprendizaje en materia de seguridad en las próximas ediciones, dejando una impronta positiva en la comunidad;

Por ello y, en virtud de la normativa vigente y del Código de Conducta elaborado en el marco de la Ekoparty, el SECTF de la edición 2020, se rige por las **bases y condiciones** que se establecen a continuación:

- 1) **OBJETO:** El SECTF es organizado en el marco de la edición 2020 de la Ekoparty Security Conference, comenzando el día 10 de Junio del año 2020 y finalizando el día 26 de Septiembre del año 2020. El mismo tiene como objetivo la promoción de herramientas



de concientización relacionadas con estrategias de ingeniería social, en especial, en lo que respecta a técnicas de vishing.

- 2) **PARTICIPANTES:** Podrán participar de la presente competencia todas aquellas personas que tengan 18 (dieciocho) años o más. Los menores de edad, conforme la legislación argentina, deberán contar con **AUTORIZACIÓN** de sus padres o representantes legales para participar, siendo estos últimos solidariamente responsables de la participación del/la menor en dichas actividades y eximiendo de responsabilidad alguna al comité organizador de la Ekoparty Security Conference sobre cualquier hecho y/o acto que pudiere suceder con motivo o en ocasión de dicha participación. En dicha autorización deberá constar, en forma expresa, la aceptación de las Bases y Condiciones del SECTF.
- 3) **FORMA DE PARTICIPAR:** Quienes desean participar (los **“participantes”** conjuntamente, o el **“participante”** individualmente) en el SECTF, deberán registrarse por equipos de hasta 3 (tres) personas, indicando el nombre del equipo y también el nombre y apellido verdadero de cada uno de sus integrantes. Un participante no puede integrar más de un equipo. Sin perjuicio de la posibilidad de los participantes de utilizar seudónimos durante la competencia y ante el público, el comité organizador de la Ekoparty Security Conference, deberá poder identificar a los miembros del equipo. En consecuencia, no podrán participar aquellas personas que provean datos falsos, incorrectos o incompletos al momento de la inscripción.  
El comité organizador no se responsabiliza por la veracidad de los datos proporcionados por los participantes.
- 4) **MODALIDAD Y PLAZO DE INSCRIPCIÓN:** Para participar de la presente competencia, los interesados deberán inscribirse en <https://www.ekoparty.org/survey/start/social-engineer-ctf-ekoparty-2020-4>, a partir del día 10 de Junio y hasta el día 26 de Junio , consignando los datos indicados en el punto anterior. No se admitirá ninguna solicitud fuera del plazo indicado.
- 5) **ETAPAS DE LA COMPETENCIA:** Los participantes deberán respetar las distintas fases en las que se divide el SECTF y presentar sus resultados en tiempo y forma<sup>1</sup>, a saber:
  - Primera fase: OSINT/Intel. Tiempo: 2 semanas.
  - Segunda fase: Selección de personas objetivo + Desarrollo del pretexto. Tiempo: 1 semana.
  - Tercera fase: Llamada. Tiempo: 1 semana
  - Cuarta fase: Ejecución del ataque: 24 al 26 de Septiembre del año 2020.
- 6) **LÍMITES DURANTE LA FASE DE OSINT:** Los participantes podrán recabar información utilizando exclusivamente fuentes abiertas<sup>2</sup>. No obstante, no está permitido

---

<sup>1</sup> Las fechas exactas serán comunicadas a los participantes oportunamente.

<sup>2</sup> Los participantes deberán emplear métodos pasivos de obtención de información y herramientas para recopilar datos a partir de fuentes públicamente accesibles y disponibles sin requerir autorización previa ni afectar la privacidad de terceros. A modo de ejemplo: medios de comunicación digitales y tradicionales (fuentes periodísticas como diarios o revistas; radio, tv; etc.); información gubernamental y financiera pública; blogs; foros; eventos; publicaciones institucionales y académicas; motores de búsqueda; repositorios de archivos y videos; bases de datos públicas; sitios web; información geoespacial de acceso público (IMINT); redes sociales



comunicarse previamente con el objetivo con el fin de obtener datos, ya sea por correo electrónico, chat, llamadas o cualquier medio de comunicación, para usar en el marco del evento.

Se podrá llamar a los números de teléfono obtenidos solamente para corroborar su exactitud y asegurar su utilidad al momento de la ejecución del ataque (“la llamada”). Cabe destacar que se podrá llamar únicamente a teléfonos argentinos y de uso profesional. Es decir, no se acepta llamar a teléfonos celulares personales o a dispositivos de uso doméstico.

Tampoco estará permitido recolectar información de forma física, en otras palabras, no es posible acercarse personalmente a las instalaciones del objetivo para obtener datos, en el marco del SECTF.

Queda prohibido acceder o intentar acceder fraudulentamente a las redes y sistemas de información y comunicación del objetivo, ya sea de forma remota o presencial, con el fin de reunir datos para participar del SECTF.

Toda información recolectada, enviada y/o utilizada que no provenga de fuentes abiertas, puede provocar la descalificación del equipo, sin perjuicio de la responsabilidad jurídica que pueda acarrear, para sus integrantes, el acto cometido.

Los participantes deberán asistir al Workshop “Introducción a OSINT e ingeniería social”, en el cual podrán obtener más herramientas para cumplir con esta fase de la competencia y evacuar sus dudas de forma segura<sup>3</sup>.

- 7) **SELECCIÓN DE OBJETIVOS:** Los participantes tendrán que presentar una lista de 10 (diez) personas jurídicas del sector privado con domicilio legal en la República Argentina que servirán como objetivo, de las cuales, el comité organizador, seleccionará 6 (seis), las que se darán a conocer en las etapas correspondientes. Para ello, distintos criterios serán tomados en cuenta, como la finalidad de la competencia, seguridad, interés general, ética, etc. En consecuencia, a modo de ejemplo, serán automáticamente descartados: organismos de gobierno, instituciones educativas, entidades del sector financiero, hospitales, clínicas y centros de salud, empresas de telecomunicaciones, empresas proveedoras de servicios considerados como esenciales o críticos (agua, electricidad, gas, salud, etc.).
- 8) **SELECCIÓN DE PRETEXTOS:** Los participantes presentarán oportunamente los pretextos para ejecutar el ataque. Los mismos deberán ser preparados en español y serán aceptados o rechazados por el comité organizador, siguiendo criterios similares a los expuestos en la cláusula anterior. Se solicita a los participantes que usen el sentido común y que consulten al comité organizador en caso de duda sobre los límites y alcances del pretexto y del plan de llamada. EL SECTF debe servir de inspiración y no de burla. Este CTF apunta a la excelencia, busca pretextos y estrategias originales, pero aplicados con

---

(SOCMINT). De esta manera, se pueden obtener nombres de usuario; direcciones de correo electrónico; nombres de dominio; IP; imágenes; videos; documentos; metadatos; números de teléfono; archivos públicos; mapas; rutinas, entre otros datos, siempre que cumplan con los requisitos mencionados en este documento y con la normativa vigente.

<sup>3</sup> Esta capacitación es gratuita. La fecha exacta de la misma será comunicada a los participantes oportunamente.



proporcionalidad y responsabilidad. Por ello, se tendrán en cuenta, además, los siguientes elementos:

- Los personajes utilizados por los participantes deben ser ficticios. No se permiten suplantaciones de identidad;
- Se encuentra prohibido relacionar la identidad ficticia a cualquier fuerza de seguridad, funcionario público o miembro del gobierno;
- No se permite llamar a familiares o personas que no trabajen para el objetivo;
- No se permite llamar a menores de edad ni hacerse pasar por menores de edad;
- El pretexto debe poner en evidencia las cualidades del participante sin humillar al objetivo;
- Los objetivos no deben transformarse en víctimas de infracciones penales;
- No se permite incitar al objetivo a cometer una infracción;
- No se permiten sobornos ni ofrecer recompensas a las empresas objetivos por participar en el pretexto;
- No se permite el uso de material erótico, pornográfico, sexualmente ofensivo o violento;
- No se permiten amenazas, extorsión, conductas hostiles o de ningún otro tipo tendientes a afectar el trato digno que merece todo individuo;
- No se permite generar pánico o hacerle creer al objetivo que se encuentra en una situación de riesgo;
- No se toleran pretextos racistas, discriminatorios, antiéticos y/o que pongan en peligro la seguridad de los objetivos, de los participantes, de los asistentes, de los organizadores y/o de terceros.
- El pretexto no debe violar ningún tipo de derecho de autor y/o marca comercial y/o cualquier otro tipo de derechos de terceros.
- El pretexto no puede generar ningún perjuicio patrimonial.

El comité organizador puede rechazar un pretexto que no cumpla con estos requisitos. Asimismo, se reserva el derecho de eliminar cualquier mensaje o contenido que sea abusivo, hostigador, difamatorio, obsceno, calumnioso, invasivo de la privacidad de terceros, discriminatorio, o que de cualquier forma viole derechos de terceros y/o disposiciones legales aplicables.

Si el participante distorsiona el pretexto durante la llamada y viola alguno de estos puntos, la misma podrá ser interrumpida y el participante puede ser descalificado, sin perjuicio de la responsabilidad jurídica que pueda acarrear, para el participante y su equipo, el acto cometido. El comité organizador no se responsabiliza por las conductas de los participantes que no respeten las reglas del SECTF (ver cláusula 16°).

- 9) **CRITERIOS DE CLASIFICACIÓN:** la clasificación se realiza de acuerdo a los puntos acumulados por la cantidad de hallazgos (flags) por el equipo competidor. La



organización informará a los participantes sobre el sistema utilizado de evaluación de los hallazgos, de acuerdo a la fase de la competencia.

- 10) **PRECLASIFICACIÓN Y CLASIFICACIÓN:** Según los criterios indicados en la cláusula anterior, la primera preclasificación tendrá lugar luego de la FASE I, etapa en la cual quedarán 16 (dieciséis) equipos sobre el total de anotados. Luego, clasificarán 12 (doce) equipos en la FASE III y, por último, 8 (ocho) equipos en la fase final.
- 11) **LA LLAMADA:** El orden de llamadas va a estar definido por el puntaje entre los equipos. El participante del equipo que realice la llamada, contará con un tiempo máximo de 20 (veinte) minutos para contactar a los objetivos y obtener la mayor cantidad de hallazgos posibles durante ese lapso, respetando los pretextos autorizados y las reglas aquí expuestas. La comunicación deberá realizarse en español. Durante ese tiempo, el equipo competidor podrá realizar más de una llamada a sus diferentes objetivos.
- 12) **HALLAZGOS:** Los hallazgos son los datos obtenidos durante la llamada telefónica y dependerán, en gran parte, de la información recolectada en las fases previas. El jurado determinará su valor, siempre y cuando, su obtención haya sido posible sin violar ninguna de las reglas de la competencia ni la legislación nacional.  
Los hallazgos deben relacionarse con temas corporativos: proveedores de servicios (delivery, soporte técnico, restauración; limpieza; desinfección; residuos; seguridad física); productos y servicios utilizados y/u ofrecidos por la empresa; medidas de seguridad; redes; dispositivos; antivirus; hardware y software; instalaciones; ingreso y egreso de personal (por ejemplo, control de identidad, badges, horarios); responsabilidades sobre distintos puestos, etc.  
No se permitirá recolectar durante la llamada ni durante las fases anteriores: contraseñas; datos bancarios; datos confidenciales; datos amparados por secreto profesional, propiedad intelectual o relacionados con la vida privada y familiar de los empleados que representan al objetivo.
- 13) **JURADO:** Las decisiones del jurado serán inapelables. Asimismo, el jurado puede quitar puntos, expulsar o descalificar a los participantes si lo considera pertinente. El mismo está integrado por: Carlos Garay, Emiliano Piscitelli, Ariel Kennedy, Hector Pardinás, Jorge Martín Vila.
- 14) **PREMIOS:** Los premios serán anunciados por la organización en el transcurso de la competencia. Los 3 (tres) primeros equipos recibirán premios.  
Ekoparty Security Conference podrá reproducir, distribuir y publicar, de modo total o parcial, en cualquier modalidad que considere necesaria y en todos los soportes conocidos y por cualquier medio de difusión, los resultados del SECTF y su ganador, utilizando su seudónimo para proteger su identidad, si éste así lo desea y manifiesta.
- 15) **CONSENTIMIENTO:** La participación en el SECTF supone la plena aceptación de sus bases. El participante toma conocimiento que, en caso de no estar de acuerdo con alguna de estas condiciones, deberá abstenerse de participar en la presente competencia.  
De forma complementaria, una vez aprobada la inscripción, los participantes de los equipos deberán firmar una **DECLARACIÓN**, en la cual, manifestarán expresamente la



aceptación de las bases y condiciones, asumiendo tener la capacidad legal suficiente y la responsabilidad jurídica en caso de violación a la legislación argentina vigente, al Código de Conducta de la Ekoparty Security Conference y a las reglas expuestas en el presente documento. La misma deberá ser remitida vía email a **socialctf@ekoparty.org**, en forma simultánea al envío de la lista de objetivos, indicando los datos personales solicitados durante la inscripción y una dirección de correo electrónico de contacto.

Asimismo, los participantes se comprometen a comunicar fehacientemente, por escrito, al comité organizador cualquier modificación de los datos aportados, así como la revocación del consentimiento efectuado. En caso de haber leído este párrafo de los términos y condiciones legales, el participante, de forma opcional, podrá obtener puntaje extra en la competencia al enviar este hallazgo vía email a **socialctf@ekoparty.org**. En caso de modificación de las presentes bases y condiciones, el comité organizador notificará a los participantes por escrito y actualizará el documento que podrá ser consultado en el sitio web de la Ekoparty Security Conference durante toda la competencia.

16) **RESPONSABILIDAD:** EL CTF es un desafío, pero no deja de ser un juego.

No es posible establecer una lista taxativa de las conductas en las que los participantes puedan transgredir las reglas. No obstante, si el comité organizador es notificado o detecta algún comportamiento que de forma flagrante o manifiesta exceda los límites aquí establecidos, procederá a penalizar al participante y a su equipo. Las sanciones pueden ir desde la quita de puntos a la descalificación. Además, podrá interrumpir la competencia en caso de detección de alguna conducta hostil, abusiva o ilícita, así como también expulsar al participante de la conferencia y, eventualmente, impedir su ingreso a las próximas ediciones.

En ningún caso la Ekoparty Security Conference, sus directores, organizadores, empleados y/o representantes serán responsables por cualquier daño directo, indirecto, incidental, especial o punitivo, que pudiera ser causado por la participación en el presente SECTF o por el uso de los materiales autorizados.

En el caso en que un tercero formulase un reclamo extrajudicial o judicial durante o después de la competencia, a raíz de la violación de alguno de los puntos mencionados en este documento, los participantes y/o sus representantes legales, asumen la obligación de mantener totalmente indemnes a los organizadores de la Ekoparty Security Conference frente al reclamo indicado.

Cualquier usuario que tenga sospechas de prácticas fraudulentas en la ejecución de la competencia o que contraríen su espíritu, debe remitirlas por correo electrónico a **socialctf@ekoparty.org**

Cabe recordar que la Ekoparty es un encuentro entre personas respetuosas, inclusivas, y conscientes de la importancia de interactuar de forma constructiva. Tratemos de evitar situaciones en las que esta cláusula se vuelva aplicable.

17) **DATOS PERSONALES:** Los datos personales que los participantes comuniquen al comité organizador no serán comunicados al público y quedarán amparados bajo la Ley de Protección de Datos Personales 25.326. Su uso queda limitado a los términos referidos en el presente documento.



No obstante, el comité organizador se reserva el derecho a solicitar documentos oficiales probatorios que acrediten la identidad del participante en caso de que existan sospechas de actividad ilícita.

18) **CONFIDENCIALIDAD:** El público presente durante la llamada, personalmente o a distancia, queda sometido a reglas de confidencialidad específicas. Los espectadores deberán guardar silencio; no podrán interrumpir las conversaciones; no podrán ejecutar ningún sistema que pueda interferir con el normal funcionamiento del SECTF; no podrán tomar fotografías o realizar grabaciones ni divulgar información sobre los participantes del SECTF o detalles sobre los objetivos y hallazgos.

El participante que realizará la llamada, autoriza al comité organizador de la Ekoparty Security Conference a efectuar las grabaciones o capturas que estime pertinentes, con la finalidad de revisar los hallazgos ocurridos durante la misma. En caso de una posterior divulgación, la organización se encargará de anonimizar dicha comunicación para evitar la identificación de los interlocutores.

El participante que no desee revelar su identidad frente al público, está facultado para usar disfraces, caretas o cualquier elemento que le sirva a tal efecto, siempre que se ajusten al contexto en el que serán utilizados.

Ekoparty Security Conference se reserva el derecho a retirar enlaces y comentarios improcedentes publicados en su sitio web y redes sociales asociadas, y de tomar las medidas que fueren necesarias para ayudar a garantizar el respeto a la ley y la buena fe en la participación.

19) **REGLAS DE CONVIVENCIA:** El Código de Conducta de la Ekoparty Security Conference<sup>4</sup>, aplicable a la totalidad del público que asiste y participa del evento, establece una lista meramente ejemplificativa de las conductas o expresiones que pueden ser consideradas como gravemente inapropiadas o abusivas conforme a su standard de convivencia y que no serán toleradas bajo ningún supuesto. Las violaciones a dicho Código darán lugar a las sanciones siguientes, pudiendo aplicarse de manera alternativa o conjunta, según el caso:

- Solicitud de pedido de disculpas o retractación hacia la persona afectada;
- Solicitud de desistir en el tratamiento abusivo indicado;
- Advertencia disciplinaria que consiste en advertir que, de verificar la persistencia de la conducta abusiva señalada, se procederá a la exclusión de la conferencia temporal o permanente, según la gravedad que estime exclusivamente la organización respecto del incidente presentado;
- Exclusión automática temporal de participación en las actividades pautadas en la conferencia con la persona a la que se le atribuye el incidente o conducta abusiva;
- Exclusión automática temporal de los espacios físicos y virtuales de la conferencia, por el tiempo que determine unilateralmente la organización de la conferencia;
- Exclusión automática permanente de los espacios físicos y virtuales de la conferencia;

---

<sup>4</sup> <https://www.ekoparty.org/codigo-de-conducta>



- Denuncia del incidente a las autoridades administrativas, policiales, judiciales y/o las que correspondan conforme al incidente respectivo.

Ni la conferencia ni sus organizadores serán responsables por los costos adicionales incurridos u ocasionados, como consecuencia directa o indirecta, inmediata, mediata o remota, por la exclusión de la conferencia o de sus espacios y/o actividades físicas y/o virtuales de los infractores, como así tampoco por los costos adicionales incurridos u ocasionados, como consecuencia directa o indirecta, inmediata, mediata o remota, por ninguna de las medidas que se tomen para sancionar a los infractores.

20) CIRCUNSTANCIAS ESPECIALES: Cuando circunstancias imprevistas constituyan caso fortuito, fuerza mayor o similar que lo justifiquen, el comité organizador podrá suspender, cancelar o modificar, total o parcialmente el SECTF.

21) JURISDICCIÓN Y COMPETENCIA: Los participantes se comprometen a solucionar amigablemente con el comité organizador las diferencias que se pudieran presentar sobre cualquier aspecto relativo a la realización del SECTF. De no ser ello posible se someten a la jurisdicción de los Tribunales ordinarios y competentes de la Ciudad Autónoma de Buenos Aires, con renuncia expresa a cualquier otro fuero y/o jurisdicción que pudiere corresponderles. A los efectos de toda notificación judicial, el comité organizador de la Ekoparty Security Conference fija domicilio legal en Reconquista 617, piso 8, CABA.

Para más información sobre el SECTF, dirigirse a: [socialctf@ekoparty.org](mailto:socialctf@ekoparty.org)