III. OTRAS DISPOSICIONES

CONSEJO DE SEGURIDAD NUCLEAR

5690 *Resolución de 26 de mayo de 2020, del Consejo de Seguridad Nuclear, por la que se publica el Convenio con la Universidad Complutense, para la realización de un «Ejercicio de ciberseguridad en los sistemas del Consejo de Seguridad Nuclear».*

El Presidente del Consejo de Seguridad Nuclear y el Vicerrector de Relaciones Institucionales de la Universidad Complutense, han suscrito, con fecha 25 de mayo de 2020, un Convenio para la realización de un «Ejercicio de ciberseguridad en los sistemas del Consejo de Seguridad Nuclear».

Para general conocimiento, y en cumplimiento de lo establecido en el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispongo la publicación en el «Boletín Oficial del Estado» del referido Convenio, como anejo a la presente Resolución.

Madrid, 26 de mayo de 2020.–El Presidente del Consejo de Seguridad Nuclear, Josep Maria Serena i Sender.

ANEJO

Convenio entre el Consejo de Seguridad Nuclear y la Universidad Complutense, para la realización de un «Ejercicio de ciberseguridad en los sistemas del Consejo de Seguridad Nuclear»

REUNIDOS

De una parte: Don Josep Maria Serena i Sender, Presidente del Consejo de Seguridad Nuclear (en adelante CSN), cargo para el que fue nombrado por el Real Decreto 227/2019 de 29 de marzo (BOE número 77 de 30 de marzo), en nombre y representación de este Organismo, en virtud de lo establecido en el artículo 36.1.p) del Estatuto del Consejo de Seguridad Nuclear, aprobado por el Real Decreto 1440/2010, de 5 de noviembre, con domicilio en la calle Justo Dorado, núm. 11 de Madrid y número de identificación fiscal Q2801036-A.

De otra parte: Don Juan Carlos Doadrio Villarejo, Vicerrector de Relaciones Institucionales, en nombre y representación de la Universidad Complutense de Madrid (en adelante UCM), actuando por delegación del Rector según Decreto rectoral 19/2019, de 14 de junio, de establecimiento de los Vicerrectorados de la UCM, de delegación de competencias y de diversas cuestiones de índole organizativa, publicado en el «Boletín Oficial de la Comunidad de Madrid» de 19 de junio de 2019.

Ambos intervienen para la realización de este acto por sus respetivos cargos y en el ejercicio de las facultades que, para convenir en nombre de las Entidades a que representan, tienen conferidas y, a tal efecto,

EXPONEN

Primero.

Que el CSN es el único organismo competente en materia de seguridad nuclear y protección radiológica y tiene legalmente asignadas las funciones que en dichos ámbitos establece el artículo 2 de su Ley de Creación (Ley 15/1980, de 22 de abril).

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

Segundo.

Que el artículo 14 de su Ley de Creación establece la obligación del CSN de facilitar el acceso a la información y la participación del ciudadano y de la sociedad civil en su funcionamiento, facilitando dicho acceso a través del uso de las tecnologías de la información y la comunicación.

Tercero.

Que, en el ejercicio de sus funciones, el CSN hace un amplio uso de las tecnologías de la información, y que es interés del CSN proteger la información como activo fundamental para el desarrollo de su misión y sus funciones, garantizando su confidencialidad, integridad y disponibilidad, así como la continuidad de los sistemas y tecnologías de la información, bajo cualquier circunstancia y minimizando los riesgos de daño.

Cuarto.

Que el CSN reconoce la importancia de una seguridad informática robusta y efectiva para el funcionamiento exitoso de su infraestructura de tecnologías de la información y la protección contra la amenaza que representan las actividades maliciosas a través de las redes informáticas.

Quinto.

La UCM, según se recoge en sus Estatutos aprobados por Decreto 32/2017, de 21 de marzo, del Consejo de Gobierno de la Comunidad de Madrid (BOCM de 24 de marzo de 2017), tiene entre sus funciones la creación, desarrollo, transmisión y crítica de la ciencia, de la técnica y de la cultura, la difusión, la valorización y la transferencia del conocimiento al servicio de la cultura, de la calidad de vida y del desarrollo económico, la difusión del conocimiento y la cultura a través de la extensión universitaria y la formación continuada, así como favorecer el intercambio científico, la movilidad académica y la cooperación para el desarrollo de los pueblos.

Sexto.

Que la UCM prevé entre sus competencias reflejadas en sus Estatutos, el establecimiento de relaciones con otras entidades para la promoción y desarrollo de sus fines institucionales.

Séptimo.

Que ambas partes consideran aconsejable promover una cooperación entre ellas con la finalidad de que los estudiantes de la UCM puedan tener la oportunidad de obtener un aprendizaje sobre la seguridad de las Tecnologías de la Información de manera práctica, fortaleciendo asimismo el sistema de ciberseguridad del CSN y la eficacia de su infraestructura.

Octavo.

Que las Partes consideran que la colaboración entre ellas en este campo contribuirá al mejor cumplimiento de los objetivos propios de cada una de ellas, garantizándose que los servicios públicos que les incumben se prestan de modo que se logren los objetivos que tienen en común; y que el desarrollo de dicha cooperación se guía únicamente por consideraciones relacionadas con el interés público.

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

Por todo ello, las Partes convienen en formalizar el presente Convenio con sujeción a las siguientes

CLÁUSULAS

Primera. *Objeto.*

El objetivo general de este Convenio es la realización de un «Ejercicio de ciberseguridad en los sistemas del Consejo de Seguridad Nuclear».

El alcance de las actividades que se considera necesario realizar para alcanzar este objetivo se detalla en la Memoria Técnica que se adjunta a este Convenio como Anexo 1.

Segunda. *Obligaciones de las partes.*

Son obligaciones de la UCM dentro de este Convenio:

– Realizar las actividades que se describen en la Memoria Técnica (anexo 1) que se adjunta, relacionadas con los objetivos descritos en la cláusula primera, en la forma y con las garantías que en la misma se describen.

– Poner a disposición del CSN los resultados, métodos, códigos, metodologías, y, en general, toda la información que se genere durante la realización de las actividades objeto de este Convenio, guardando la debida confidencialidad acerca de la misma.

Son obligaciones del CSN dentro de este Convenio:

– Facilitar la ejecución por parte de la UCM de las actividades que son objeto del Convenio.

– Verificar la información facilitada por la UCM como resultado de las actividades objeto de este Convenio e informarle de sus conclusiones y de las actuaciones llevadas a cabo como consecuencia de ellas.

Tercera. *Responsabilidad.*

Las consecuencias aplicables en caso de incumplimiento de las obligaciones y compromisos asumidos por cada una de las partes en el presente Convenio y, en su caso, los criterios para determinar la posible indemnización por dicho incumplimiento se regirán según lo establecido en la Memoria Técnica (Anexo 1).

Cuarta. *Financiación.*

El Convenio no tendrá coste económico para ninguna de las Partes.

Quinta: Seguimiento del Convenio.

Las Partes crearán una Comisión de Seguimiento, designando respectivamente como Coordinadores Técnicos del Convenio:

Por el CSN: El subdirector de Tecnologías de la Información.

Por la UCM: Los coordinadores del Grupo de Hacking Ético de la Facultad de Informática.

Los Coordinadores Técnicos serán responsables de controlar el desarrollo del Convenio y de adoptar, por mutuo acuerdo, las decisiones necesarias para la buena marcha de las actividades contempladas en el mismo. Para ello, podrán asesorarse de los expertos que consideren oportuno.

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

Sexta. *Modificación.*

Los términos del Convenio se podrán revisar o modificar en cualquier momento a petición de cualquiera de las Partes, de manera que puedan introducirse, de mutuo acuerdo, tales modificaciones o revisiones.

Séptima. *Régimen jurídico.*

Este Convenio queda sometido al régimen jurídico de los convenios, previsto en el capítulo VI del título preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, teniendo naturaleza administrativa.

La interpretación del Convenio se realizará bajo el principio de buena fe y confianza legítima entre las Partes, que convienen en solventar de mutuo acuerdo las diferencias que pudieran presentarse en su aplicación. Para ello, surgida la controversia, cada parte designará un representante, si bien, en el caso de no lograrse común Convenio, estas someterán la cuestión a los tribunales competentes de la jurisdicción contencioso-administrativa.

Octava. *Confidencialidad.*

Las Partes conceden, con carácter general, la calificación de información reservada a la generada en aplicación de este Convenio, por lo que asumen de buena fe el tratamiento de restricción en su utilización por sus respectivas organizaciones a salvo de su uso para el destino o finalidad pactados o de su divulgación, que habrá de ser autorizada previamente caso por caso por cada una de las Partes.

Asimismo, cada una de las Partes se compromete a mantener de forma confidencial la información y/o documentación que le haya sido facilitada por las otras Partes y que, por su naturaleza, o por haberse hecho constar expresamente, tenga carácter confidencial.

Esta obligación de confidencialidad se mantendrá en vigor una vez finalizado el presente Convenio.

Novena. *Propiedad intelectual e industrial.*

Los derechos de propiedad industrial e intelectual que recaigan sobre los trabajos o resultados de las actividades que se realicen dentro del alcance de este Convenio pertenecerán exclusivamente a las Partes, como únicos titulares de los mismos, por lo que ninguna entidad podrá divulgar dichos trabajos o resultados ni realizar explotación alguna de los derechos reconocidos sobre los mismos, incluyendo su cesión a terceros, sin contar con la previa aprobación escrita de las otras Partes.

Décima. *Vigencia y prórroga.*

El presente Convenio se perfeccionará por la prestación del consentimiento de las partes mediante su firma. Tendrá una vigencia de 2 años contados a partir de su publicación en el «Boletín Oficial del Estado» previa inscripción en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación del sector público estatal. Si fuera necesario variar su plazo de ejecución, el Convenio podrá ser objeto de prórroga por hasta 2 años adicionales por mutuo acuerdo de las partes, siempre que se respete lo establecido en el artículo 49, letra h, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y la prórroga sea compatible con las obligaciones presupuestarias legalmente establecidas. En este caso, se formalizará la oportuna Cláusula Adicional incluyendo las condiciones de la prórroga con anterioridad a la fecha del vencimiento del Convenio.

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

Undécima. *Extinción y suspensión.*

El presente Convenio se extinguirá por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en alguna de las causas de resolución previstas en el artículo 51.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Asimismo, las partes por motivos razonables, podrán rescindir o suspender temporalmente este Convenio, preavisando con al menos un mes de antelación a la fecha en que la resolución deba ser efectiva.

Las Partes manifiestan su plena conformidad con el presente Convenio, en Madrid a 25 de mayo de 2020.–Por el Consejo de Seguridad Nuclear, el Presidente, Josep Maria Serena i Sender.–Por la Universidad Complutense, el Vicerrector de Relaciones Institucionales, Juan Carlos Doadrio Villarejo.

ANEXO 1

Memoria técnica

Ejercicio de ciberseguridad sobre los sistemas del CSN

Propósito

El Ejercicio de ciberseguridad sobre los sistemas del CSN tiene el propósito de:

– Permitir a los estudiantes inscritos en el Grupo de Hacking Ético de la Facultad de Informática de la Universidad Complutense de Madrid ejercitarse de forma práctica en dichas materias, de forma controlada, en un entorno real en producción.

– Contribuir a la mejora de la seguridad de los sistemas de información del CSN mediante la identificación de las vulnerabilidades y compromisos de seguridad que puedan ponerse de manifiesto durante su ejecución.

Este documento establece un entendimiento común entre las Partes del esfuerzo de colaboración requerido para la ejecución del Ejercicio. Los resultados de sus esfuerzos se utilizarán únicamente con fines pacíficos y conforme a lo previsto en el mismo.

La participación de cada Parte en el Ejercicio se basa en los mejores esfuerzos. Las disposiciones de este documento no implican ningún compromiso firme de recursos de ninguna de las Partes.

Organización

La realización del Ejercicio será gestionada por el CSN a través del jefe de área de Sistemas y Comunicaciones y, en su ausencia, por una persona designada por él.

La UCM nombrará a un miembro de su personal que trabaje en el dominio de la ciberseguridad (el "Supervisor") para que se relacione con el CSN en la preparación y ejecución del Ejercicio y lo represente en cualesquiera asuntos y comunicaciones relacionados con el Ejercicio.

El Supervisor identificará el tipo y el alcance del trabajo que desea realizar de acuerdo con el objetivo del Ejercicio; supervisará a los estudiantes de la UCM que participen en el Ejercicio (los "Participantes"); y comunicará al CSN, antes del inicio de cualquier prueba, el cronograma, las direcciones IP desde las cuales se realizarán sus actividades y cualquier otra información relevante sobre la misma.

La participación en el Ejercicio no constituirá una relación laboral entre el CSN y el Supervisor, cualquier otro miembro del personal de la UCM que se involucre en el Ejercicio, o cualquier Participante.

El CSN no ofrecerá remuneración ni por el trabajo realizado ni por la información generada como resultado del Ejercicio. El CSN emitirá un certificado acreditativo a los estudiantes del Grupo de Hacking Ético de la Facultad de Informática de la Universidad Complutense de Madrid que hayan participado en el Ejercicio de ciberseguridad.

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

Contribuciones de las partes

El CSN hará visible a la UCM sus sistemas de información a través de Internet.

El Supervisor proporcionará orientación y supervisión suficientes a los Participantes para probar la seguridad de los sistemas de información del CSN de manera benigna y vigilada.

Participación y conducta

Para poder participar en el Ejercicio, los Participantes deben:

– Encontrarse inscritos en el Grupo de Hacking Ético de la Facultad de Informática de la Universidad Complutense de Madrid.

– Obtener el respaldo del Supervisor designado por la UCM para su participación en el Ejercicio.

Con anterioridad a su participación en el Ejercicio, cada Participante deberá manifestar su conformidad con respetar el marco ético establecido en Código Ético adjunto a la presente Memoria Técnica, firmando y devolviendo al CSN una copia de dicho Código. El Supervisor se comprometerá a garantizar que se cumpla este requisito con respecto a cada Participante.

En particular, el Código Ético requiere que los Participantes mantengan la confidencialidad de toda la información obtenida de, y sobre, las instalaciones y los sistemas de información del CSN como consecuencia de su participación en el Ejercicio, y solo la divulguen dentro del marco del Ejercicio o cuando el CSN haya dado expresamente su permiso por escrito para que el Participante individual pueda hacerlo.

El Código Ético se aplicará y deberá ser observado en todo momento por los Participantes durante su participación en el Ejercicio, y, cuando corresponda (por ejemplo, obligaciones de confidencialidad), los Participantes seguirán cumpliendo esta obligación con posterioridad a la finalización de su participación en el Ejercicio.

El CSN se reserva el derecho de excluir del Ejercicio a un Participante cuando tenga evidencia o sospeche que está, o ha estado violando el Código Ético.

El Supervisor habrá de dejar claro a los Participantes, que el Código Ético no permite ni excusa la actividad delictiva de ningún tipo. El CSN seguirá el criterio de tolerancia cero frente a dicha actividad, que queda estrictamente prohibida en la ejecución del Ejercicio. Si la UCM, o cualquier Participante consideran, en cualquier momento, que al ejecutar o tomar parte en el Ejercicio corre el riesgo de infringir la legalidad, deberá informar al Supervisor quien, a su vez, trasladará dichas inquietudes al CSN y esperará sus instrucciones antes de proceder con el Ejercicio. Dicho deber es igualmente de aplicación para el propio Supervisor, si considerara que se dan las circunstancias anteriormente señaladas. La UCM deberá asegurarse de que su participación en el Ejercicio no vulnere las leyes aplicables.

Resultados

Una vez que los Participantes hayan completado su trabajo, cada Participante debe:

– informar de manera precisa y completa de todos sus hallazgos al Supervisor, quien a su vez los transmitirá al CSN;

– asegurarse de que los registros que conserve con respecto a sus hallazgos se mantengan confidenciales y que solo los pongan a disposición de su Supervisor y de compañeros Participantes de la UCM que también participen en el Ejercicio, quedando excluida cualquier otra comunicación a terceros;

– solicitar la aprobación previa y por escrito del CSN en caso de que deseen publicar o hacer públicos sus hallazgos (por ejemplo, para su inclusión en tesis académicas, documentos o presentaciones).

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

Responsabilidad

Cada Parte soportará su propia pérdida y daño en relación con su participación en el Ejercicio.

Cada Parte mantendrá a la otra libre de daños y la indemnizará por cualquier pérdida, daño o lesión sufrida como resultado de negligencia grave o mala conducta intencional en la ejecución de su contribución al Ejercicio. Esta responsabilidad no se extenderá a reclamaciones por pérdidas, daños o lesiones directas o indirectas, incluidas, entre otras, la pérdida de ganancias, ingresos o contratos.

Detalles de contacto

7.1 Los datos de contacto del gestor del Ejercicio por parte del CSN son los siguientes:

José Manuel Sánchez Anguí.
Jefe de Área de Sistemas y Comunicaciones.
c/ Pedro Justo Dorado Dellmans, 11.
28040 Madrid.
Teléfono 913460175.
Correo-e: jmsa@csn.es.

7.2 Los datos de contacto del Supervisor son los siguientes:

José Luis Vázquez Poletti.
Facultad de Informática de la Universidad Complutense de Madrid.
C/ Profesor José García Santesmases, 9.
28040 Madrid.
Teléfono 913947600.
Correo-e: jlvazquez@fdi.ucm.es.

Código ético (Adjunto a la Memoria Técnica)

1. Aplicación: este Código ético se aplicará y será observado en todo momento por todos los Participantes durante su participación en el Ejercicio de ciberseguridad en los sistemas del CSN («el Ejercicio»).

2. Participación: solo participaran en el Ejercicio las personas que:

i. se encuentren inscritos en el Grupo de Hacking Ético de la Facultad de Informática de la Universidad Complutense de Madrid;

ii. tengan el respaldo del Supervisor designado por la UCM para su participación en el Ejercicio.

3. Conducta: los Participantes se comportarán de la manera más ética y competente y mostrarán integridad en todo momento en relación con su participación en el Ejercicio. En particular, en el transcurso de su participación en el Ejercicio, los Participantes deben:

a) tomar todas las precauciones necesarias para garantizar la conducta ética y el alto nivel de atención requerido para participar en el Ejercicio;

b) usar solo la propiedad del CSN de la forma en que haya sido autorizada por el CSN y con el conocimiento y consentimiento del CSN;

c) asegurarse de no violar las reglamentaciones nacionales, las reglamentaciones de la institución a la que están afiliados o de su Proveedor de servicios de Internet («ISP»), no involucrarse en prácticas engañosas como soborno, chantaje o prácticas financieras inadecuadas en relación con el Ejercicio. Si un Participante tiene dudas sobre la legalidad de su trabajo, debe cesar sus actividades de inmediato y plantear el problema a su Supervisor;

cve: BOE-A-2020-5690
Verificable en https://www.boe.es

d) asegurarse de que, durante su participación en el Ejercicio, el tráfico de red se mantenga mínimo y no afecte la estabilidad general de la red que están utilizando o la de su ISP;

e) asegurarse de que los equipos de red, los servicios informáticos o las aplicaciones web alojados en el CSN, por un ISP intermedio o por su institución, no se vean comprometidos, se les impida funcionar, se modifiquen, estén sujetos a un ataque de denegación de servicio o se rompan;

f) tener mucho cuidado de no alterar ni eliminar ninguna página web, cuenta, datos u otra información alojada en el CSN o en otro lugar.

4. Alcance: a los fines de participar en el Ejercicio, los Participantes solo investigarán las instalaciones y redes de tecnologías de la información del CSN conectadas al dominio de la red del CSN que les sean indicadas al Supervisor por el CSN durante el desarrollo del Ejercicio.

5. Divulgación: los participantes informaran de todos los hallazgos resultantes de su participación en el Ejercicio a su Supervisor y al CSN, detallando donde exista o pueda existir una debilidad de seguridad en los sistemas del CSN.

6. Confidencialidad: toda la información obtenida por los Participantes de su participación en el Ejercicio debe considerarse confidencial y tratarse como tal. Los Participantes no pueden hacer copias ni almacenar datos del CSN que descubran como parte de sus actividades en el Ejercicio. Los Participantes acuerdan que, al final de su participación en el Ejercicio, borrarán todos los datos del CSN que hayan recopilado durante el Ejercicio. Los Participantes acuerdan no dar, vender o transferir dicha información a ninguna entidad que no sea el CSN sin el consentimiento previo por escrito del CSN.

7. Conflictos de intereses: los Participantes deberán revelar al CSN y a su Supervisor cualquier conflicto de intereses que puedan surgir, o que podrían considerar que surge de su participación en el Ejercicio.

8. Uso no autorizado: en el transcurso del Ejercicio, los Participantes nunca usarán a sabiendas software o procesos que se hayan obtenido o retenido de manera ilegal o poco ética.

9. Actividades maliciosas: los Participantes no deben asociarse con atacantes maliciosos o comunidades clandestinas, ni participar en actividades maliciosas como parte del Ejercicio. Solo la infraestructura del CSN debe investigarse en el Ejercicio y solo con el propósito de exponer, en lugar de explotar, las debilidades que puedan existir.

cve: BOE-A-2020-5690
Verificable en https://www.boe.es