

# Bases Técnicas y Administrativas

## LICITACIÓN PARA DESARROLLO DE “PLATAFORMA WEB IRENESALUD.CL”

### FACULTAD DE MEDICINA - UNIVERSIDAD DEL DESARROLLO

## Contenido

<b>Términos y definiciones</b> .....	3
<b>Bases Administrativas</b> .....	5
<b>Antecedentes</b> .....	5
<b>Objetivo de la licitación</b> .....	5
<b>Etapas y Plazos</b> .....	6
<b>Entrega de la Oferta</b> .....	6
<b>Contactos y consultas</b> .....	7
<b>Criterios de admisibilidad y evaluación</b> .....	7
<b>Formalización de la licitación y contrato de servicios de desarrollo software</b> .....	9
<b>Bases Técnicas</b> .....	10
<b>Objetivo de la Plataforma web</b> .....	10
<b>Supuestos e insumos proporcionados por la contratante</b> .....	10
<b>Plan de trabajo, metodología, duración, hitos y entregables de desarrollo</b> .....	11
<b>Requerimientos Funcionales</b> .....	12
<b>Requerimientos no Funcionales</b> .....	16
<b>Lenguajes, <i>frameworks</i>, herramientas, bases de datos y servicios utilizados</b> .....	17
<b>Requerimientos de infraestructura y servicios en la nube</b> .....	17
<b>Requerimientos de Transferencia Tecnológica</b> .....	18
Trabajo en equipo .....	18
Código fuente, licencia para modificar el código y comentarios .....	18
Capacitación .....	18
Documentación .....	19
<b>Soporte y Mantenimiento Correctiva</b> .....	19
<b>Actividades y Pruebas de Aceptación</b> .....	20
<b>Prácticas de Seguridad en el desarrollo software de la empresa</b> .....	20
<b>Propiedad Intelectual</b> .....	20
<b>Anexo 1 - Formulario de Prácticas de Desarrollo Seguro de Software</b> .....	21

## Términos y definiciones

**Aplicación Web:** en el ámbito de esta licitación, se refiere a la aplicación o plataforma a construir por parte de la empresa desarrolladora. También se puede referir a ella como Plataforma o solamente Aplicación.

**Carnet de riesgo de pérdida de funcionalidad:** documento digital que reporta la cuantificación, puntaje o score de riesgo de pérdida de funcionalidad de una persona a una determinada fecha junto con los datos que permiten la identificación de dicha persona y el período de vigencia de dicho documento.

**Contraparte técnica:** persona o grupo de personas designadas por la contratante para la interacción en el ámbito técnico con la empresa proveedora.

**Contratante:** para el caso de esta licitación, se entenderá como contraparte a la Universidad del Desarrollo.

**Diseño web adaptable, adaptativo o responsivo:** es una filosofía de diseño y desarrollo cuyo objetivo es adaptar la apariencia de las páginas web al dispositivo que se esté utilizando para visitarlas.

**EMPAM:** Examen de Medicina Preventiva del Adulto Mayor.

**Empresa Oferente:** la empresa de desarrollo software que participará en esta licitación enviando una propuesta técnica y una oferta económica junto con los demás requisitos solicitados de acuerdo con los términos establecidos en estas bases de licitación.

**Empresa Proveedora o Proveedor:** la empresa de desarrollo software que se adjudique la presente licitación y que esté obligada por tanto a cumplir con los términos y condiciones presentados en su oferta y los indicados en estas bases de licitación.

**IRENE<sup>R</sup>** (*Integrated Risk Estimation for the New Elderly*) algoritmo relacionado con el modelo predictivo para la pérdida de funcionalidad de la persona mayor que será desarrollado por el equipo de investigación del proyecto IRENE FONDEF ID19I10319

**ISO/IEC 25010:** la norma o estándar internacional que describe un modelo y las métricas para la evaluación de la calidad del producto software.

**Plataforma web IRENESALUD.CL:** la plataforma web que incorporará el modelo predictivo IRENE<sup>R</sup> para volverlo accesible y permitir su uso por parte de los profesionales clínicos o de la salud, cuyo desarrollo es el objetivo de esta licitación.

**Runbook:** documento que contiene el conjunto de procedimientos y rutinas de operaciones para iniciar, detener, supervisar y depurar las componentes de sistema que sustentan la operación

de la plataforma web objeto de esta licitación. Incluye en particular también los procedimientos que se deben llevar a cabo para el manejo de contingencias del sistema.

**Secure Software Development Framework (SSDF):** el conjunto de prácticas de desarrollo de software seguro de alto nivel, denominadas “Marco de desarrollo de software seguro” desarrollado por el NIST (EE.UU.) (disponible en <https://doi.org/10.6028/NIST.CSWP.04232020>).

## Bases Administrativas

### Antecedentes

La Facultad de Medicina de la Universidad del Desarrollo se adjudicó a fines del año 2019 el proyecto FONDEF “Optimización de la capacidad predictiva del examen de medicina preventiva del adulto mayor (EMPAM) a través del desarrollo de una herramienta digital y el uso machine learning” código ID19I10319. Las instituciones asociadas para el desarrollo de este proyecto son: el Ministerio de Salud, el Servicio de Salud Metropolitano Occidente y la Fundación País Digital.

El objetivo del proyecto es desarrollar y poner a disposición de los equipos de salud el modelo predictivo IRENE<sup>R</sup> (*Integrated Risk Estimation for New Elderly*), i.e. un modelo predictivo optimizado del riesgo de pérdida de la capacidad funcional en personas de 65 y más años, basado en un subconjunto de las variables del EMPAM, seleccionadas a través del uso de herramientas de *machine learning*.

Para lograr dicho objetivo, el proyecto considera las siguientes tres componentes principales:

- i) La construcción de una base de datos validada con los resultados del examen de medicina preventiva del adulto mayor (EMPAM);
- ii) La generación de un modelo predictivo optimizado del riesgo de pérdida de funcionalidad denominado IRENE<sup>R</sup> (*Integrated Risk Estimation for the New Elderly*);  
y
- iii) El desarrollo e implementación de una plataforma web que responderá al dominio IRENESALUD.CL para incorporar y poner a disposición de los profesionales y equipos de salud el modelo predictivo IRENE<sup>R</sup>.

### Objetivo de la licitación

Desarrollar y desplegar una Plataforma web asociada al dominio IRENESALUD.CL que incorpora y pone a disposición de los profesionales y equipos de salud el modelo predictivo IRENE<sup>R</sup> proporcionando además el conjunto de funcionalidades relacionadas que emanan de las historias de usuario indicadas en las Bases Técnicas a continuación dentro de un marco de calidad y seguridad.

## Etapas y Plazos

Fecha de Publicación Bases:	Lunes 22 de marzo 2021.
Fecha Límite para recibir preguntas por escrito (exclusivamente por este canal):	Martes 30 de marzo 2021 a las 17:00 horas a la dirección de correo e-mail <a href="mailto:ci3@udd.cl">ci3@udd.cl</a> ; las respuestas serán publicadas el martes 06 de abril 2021.
Fecha de cierre de recepción de ofertas:	Martes 13 de abril 2021 a las 23:59 horas.
Fecha de notificación y publicación de resultados:	Viernes 23 de abril 2021, vía e-mail y en la página web de Investigación de la UDD

## Entrega de la Oferta

La empresa oferente deberá enviar su propuesta –en formato PDF– al correo e-mail de Carolina Mora, ([carolinamora@udd.cl](mailto:carolinamora@udd.cl)), con copia al equipo de contraparte técnica del Centro de Informática Biomédica ([ci3@udd.cl](mailto:ci3@udd.cl)), dentro de los plazos definidos. Solo se aceptarán propuestas de **personas jurídicas**, acorde a los lineamientos de FONDEF-ANID.

La propuesta deberá incluir en sus contenidos, al menos los siguientes elementos:

1. **Propuesta técnica** que detalle el desarrollo y despliegue en operación de la plataforma, las características de los servicios de soporte y mantención correctiva, junto con los demás entregables y aspectos indicados explícitamente o que emanan de lo especificado en estas Bases Administrativas y Técnicas en particular.
2. **Plan de trabajo** para el desarrollo y puesta en marcha de la plataforma a partir de lo indicado o lo que emana de estas Bases Administrativas y Técnicas, incluyendo las Horas Humanas (HH) estimadas en cada etapa y actividad.
3. **Portafolio** de la empresa, proporcionando antecedentes, documentación y referencias verificables en relación con las plataformas, aplicaciones o proyectos software desarrollados en el rubro de la salud con anterioridad, y antecedentes adicionales que puedan dar cuenta de la experiencia a nivel país y a nivel internacional en el rubro del desarrollo software y la capacidad profesional y técnica de la empresa.
4. **Formulario de Prácticas de Desarrollo Seguro de Software** (llenado) que lleva a cabo actualmente la empresa en el ámbito de sus procesos de desarrollo software, respecto del *Secure Software Development Framework (SSDF)* (Anexo 1).
5. **Currículum** completo de los miembros del equipo de trabajo que trabajarán directamente en el desarrollo de esta plataforma web.
6. **Propuesta económica valorizada**, expresada en pesos chilenos, con IVA incluido, sin reajustes ni intereses. En caso de ser una prestación exenta de IVA, especificar. La propuesta económica tendrá que incluir tanto las actividades y servicios de **desarrollo y despliegue de la Plataforma web IRENESALUD.CL** como el servicio de **Soporte Técnico y Mantención Correctiva** según la duración, términos y condiciones indicadas en las Bases Técnicas.

## Contactos y consultas

Exclusivamente por escrito a los correos e-mail de Carolina Mora, *contraparte administrativa* ([carolinamora@udd.cl](mailto:carolinamora@udd.cl)) y del equipo de *contraparte técnica* del Centro de Informática Biomédica ([ci3@udd.cl](mailto:ci3@udd.cl)), dentro de los plazos definidos, indicando en el asunto del correo: “**consulta licitación plataforma web IRENESALUD**”.

## Criterios de admisibilidad y evaluación

No se aceptarán ni pasarán a la etapa de evaluación aquellas propuestas que no abarquen o entreguen todos los elementos mínimos indicados en estas bases (ver “Entrega de la Oferta”).

Para esta licitación se han contemplado los siguientes criterios y ponderaciones:

Criterios de Evaluación		
1.	Calidad Propuesta Técnica	85%
2.	Oferta Económica	15%

Se hace presente que la contratante se reserva el derecho de declarar desierta la licitación en caso de que la Comisión Evaluadora determine que ninguna de las propuestas y ofertas recibidas resulte suficiente, adecuada o dentro del presupuesto disponible.

### 1. Calidad de la propuesta técnica

Factores por evaluar	Descripción	Puntaje*	Ponderación
<b>F1. Cumplimiento de características, funcionalidades, aspectos y requisitos de la Plataforma, infraestructura en la nube, transferencia tecnológica, servicio de soporte técnico y mantención correctiva</b>	La propuesta considera las características y funcionalidades que emanan de las historias de usuario, aborda y propone adecuadamente los aspectos y requisitos no funcionales, considera los requerimientos de infraestructura, transferencia tecnológica y las características del servicio de soporte técnico y mantención correctiva según solicitado en las bases	0 = La propuesta no cumple con lo requerido 50 = La propuesta no considera todo lo requerido 100 = La propuesta cumple con todo lo requerido	50%

<b>F2. Plan de trabajo</b>	Definición del plan de trabajo de forma coherente a los plazos del proyecto, incluyendo hitos y entregas de avance	0 = Plan de trabajo no es coherente a los plazos del proyecto 50 = Plan de trabajo es coherente a los plazos del proyecto 100 = Plan de trabajo coherente a los plazos del proyecto, con hitos y entregas de avance plausibles	20%
<b>F3. Experiencia y capacidad técnica de la empresa</b>	Experiencia en la ejecución de proyectos de características similares o del rubro salud nacionales como internacionales, y pericia en los procesos de desarrollo y en el manejo de herramientas de tecnología requerida por parte de los miembros del equipo de trabajo	0 = No se evidencia experiencia y capacidad técnica 50 = No se evidencia suficiente experiencia y capacidad técnica 100 = Se evidencia suficiente experiencia y capacidad técnica	30%

\*Si bien en la tabla se indican los criterios de los factores en relación a los puntajes: 0, 50 y 100, la calificación del puntaje de cada factor podrá tener valores intermedios.

Cálculo de puntaje Propuesta Técnica (**PPT**):

$$(F1 \times 0,5) + (F2 \times 0,2) + (F3 \times 0,3) = PPT$$

## 2. Oferta Económica

Cálculo de puntaje Oferta Económica (**POE**):

$$\frac{(\text{Precio más bajo ofertado})}{(\text{Precio de la oferta analizada})} \times 100 = POE$$

## 3. Puntaje Final

El puntaje final se calculará de la siguiente forma:

$$(PPT \times 0,85\%) + (POE \times 0,15) = \text{Puntaje Final}$$



La propuesta con mayor puntaje será la adjudicada. En caso de empate entre una o más ofertas, se tomará en especial consideración la experiencia y capacidad técnica de la empresa oferente respecto de la cantidad de productos software desarrollados para el rubro de la salud nacional e internacionalmente.

### Formalización de la licitación y contrato de servicios de desarrollo software

Se realizará mediante la firma de un Acta de Adjudicación y un Contrato de Servicios de desarrollo, soporte y mantención software entre la empresa oferente y la contratante, de acuerdo con lo estipulado en el *Manual de Declaración de Gastos y Rendición de Cuentas de Proyectos FONDEF-ANID*.

Los pagos se realizarán contra entrega de hitos y/o reportes de avance, en fechas específicas que quedarán definidas en el contrato de servicios. Cada pago se realiza mediante Orden de Compra, y la factura se pagará a 30 días, desde que se encuentre conforme la entrega o reporte según corresponda.

## Bases Técnicas

### Objetivo de la Plataforma web

La plataforma web asociada al dominio **IRENESALUD.CL** tendrá como principal objetivo poner a disposición de la comunidad y en particular de los profesionales de la salud el algoritmo relacionado con el modelo predictivo **IRENE<sup>R</sup>** (*Integrated Risk Estimation for New Elderly*) desarrollado por el equipo de investigación del proyecto IRENE FONDEF ID19I10319. La plataforma deberá incorporar, implementar y poner a disposición dicho algoritmo de la forma más usable posible, accesible tanto a los usuarios registrados como a los usuarios no registrados que quisieran utilizar o probar el modelo predictivo **IRENE<sup>R</sup>** proporcionando además un conjunto de funcionalidades que habiliten las historias de usuario descritas a continuación dentro de un marco de calidad y seguridad.

### Supuestos e insumos proporcionados por la contratante

1. El modelo predictivo **IRENE<sup>R</sup>** es el principal resultado esperado del trabajo de investigación del equipo del proyecto IRENE FONDEF ID19I10319, correspondiente al modelo optimizado del riesgo de pérdida de la capacidad funcional en personas de 65 y más años, basado en un subconjunto de las variables del EMPAM (Examen de Medicina Preventivo del Adulto Mayor), seleccionadas a través del uso de herramientas de *machine learning* durante el trabajo de investigación.
2. El modelo predictivo **IRENE<sup>R</sup>** es además el principal insumo que será requerido por la Empresa Provedora o Proveedor de la **Plataforma web IRENESALUD.CL** para que pueda incorporarlo en ella como funcionalidad para estimar un “*score*” de riesgo de pérdida de la capacidad funcional.
3. Para efectos de poder disponer oportunamente de la **Plataforma web IRENESALUD.CL**, se ha estimado adecuado iniciar el trabajo de desarrollo software de la plataforma antes de contar con el algoritmo relacionado con el modelo predictivo **IRENE<sup>R</sup>**, ya sea omitiendo inicialmente la incorporación a la plataforma de la funcionalidad “calculadora de riesgo de pérdida de capacidad funcional” (historia de usuario n.º1 detallada más adelante) -o en alternativa- se podrá proceder con la utilización de un algoritmo o modelo predictivo “*dummy*” para simular dicha funcionalidad en la plataforma hasta que esté efectivamente disponible el algoritmo relacionado con el modelo predictivo **IRENE<sup>R</sup>**.
4. Se espera que el algoritmo del modelo predictivo **IRENE<sup>R</sup>** estará disponible a más tardar a finales de agosto para que la Empresa Provedora o Proveedor de la **Plataforma web IRENESALUD.CL** pueda incorporarlo a tiempo para finalizar el desarrollo de la plataforma.
5. Se entiende que la **Plataforma web IRENESALUD.CL** en cuanto tal y su desarrollo son independientes de la calidad que podrá alcanzar (o no) el algoritmo que implementa el modelo predictivo **IRENE<sup>R</sup>**, puesto que el propósito de la plataforma es volver disponible dicho modelo predictivo. Aun así, la plataforma deberá proporcionar la interfase, entorno, aspectos y las funcionalidades adecuadas que faciliten el uso dicho modelo.

6. La **Plataforma web IRENESALUD.CL** permitirá a los usuarios no solamente manejar su propia información personal (ej. perfil de usuario) sino que también cargar y manejar información personal y de salud de otras personas (pacientes), es decir la plataforma manejará **información sensible** por lo que es de primaria importancia una adecuada gestión del riesgo y de la seguridad de la información, **en los términos establecidos en el D.S. N° 41 de 2012 del Ministerio de Salud (Reglamento de Fichas Clínicas)**.
7. La entrega y despliegue de la **Plataforma web IRENESALUD.CL** tendrá que realizarse sobre una infraestructura y servicios en la nube que tendrán que ser concordados con la contratante y según especificado más adelante en estas bases.
8. Las cuentas de servicios relacionadas con la infraestructura y servicios en la nube de la plataforma web IRENESALUD.CL de producción estarán bajo el control de la contratante la que se hará cargo de los correspondientes costos. Los costos de infraestructura y servicios en la nube relacionados con los ambientes de desarrollo, *testing* o certificación son de cargo de la empresa oferente, así como también los costos de cualquier herramienta, equipo, dispositivo, software, *framework* o cualquier otro producto o servicio utilizados para el desarrollo y testeo de la plataforma web IRENESALUD.CL por parte de la Empresa Provedora serán de cargo de esta última.
9. El dominio **IRENESALUD.CL** es de propiedad de la Universidad del Desarrollo y será proveído por ésta para la ejecución e implementación del contrato.

## Plan de trabajo, metodología, duración, hitos y entregables de desarrollo

La empresa oferente deberá presentar un plan o cronograma de trabajo relacionado con el desarrollo hasta la puesta en marcha de la **Plataforma web IRENESALUD.CL** que permita implementar todas las funcionalidades y requisitos no funcionales que emanan directa o indirectamente de las historias de usuario y de los requisitos formulados explícita o implícitamente más adelante en estas bases técnicas, poniendo en clara evidencia los hitos más relevantes en correspondencia de los cuales deberá señalar explícitamente cuáles serían los entregables relacionados, incorporando una holgura que permita abordar eventuales imprevistos dentro de ciertos límites, considerando por otra parte que el modelo predictivo **IRENE<sup>R</sup>** estará disponible para que pueda incorporarse a la plataforma a más tardar a finales de agosto 2021 y que la plataforma tendrá necesariamente que activarse en producción y estar disponible a más tardar la primera semana del mes de **noviembre 2021**. Dicho cronograma o plan de trabajo deberá considerar además las actividades de pruebas, *Quality Assurance* (QA) y transferencia tecnológica hacia la contratante como descrito a continuación en estas bases.

En particular, se señala además que el desarrollo de la **Plataforma web IRENESALUD.CL** deberá realizarse utilizando metodologías ágiles que consideren como mínimo tres ciclos, iteraciones o *sprint* de desarrollo. Cada una de las iteraciones deberá considerar tanto instancias de levantamiento de detalle como validación de los requerimientos por parte de la contratante y representantes de los usuarios finales, así como también instancias de verificación y certificación del efectivo avance y calidad del desarrollo por parte del equipo de profesionales de TI de la contratante. La empresa oferente deberá considerar los recursos y las HH necesarias para poder llevar a cabo razonablemente las actividades mencionadas que deberán reflejarse explícitamente en el plan de trabajo.

## Requerimientos Funcionales

A continuación, se presentan los requerimientos expresados bajo forma de historias de usuario (alto nivel) a partir de los cuales se pueden determinar las funcionalidades requeridas. Se asume que algunas de ellas podrían tener algunos ajustes y que de todas formas durante los ciclos o iteraciones de desarrollo se determinarán con mayor detalle las funcionalidades y características requeridas producto de las actividades de levantamiento y validación con los profesionales de la contratante y los representantes de los usuarios finales.

Cabe destacar que los principales destinatarios y *usuarios* de la plataforma corresponderán a profesionales y equipos de la salud relacionados directa o indirectamente con el cuidado de las personas mayores. Dichos profesionales podrán utilizar y actuar en la plataforma como profesionales individuales y/o también podrían actuar, formar parte o estar vinculados a uno o más establecimientos, centros o prestadores institucionales de salud, en cuyo caso existe además la figura del *administrador de centros* de salud con privilegios para configurar dicha vinculación. Se requerirá además la figura o rol de *super administrador* que será ejercido por uno o más profesionales de la contratante, tal como descrito a continuación.

	Requisito	Historia de usuario Formato: “Como [perfil], [quiero] [para]”
1	Usuario: Calculadora de riesgo de pérdida de capacidad funcional	Como usuario (ya sea anónimo o registrado), quiero ingresar los datos (provenientes de resultados de exámenes o mediciones realizadas) para así poder calcular y obtener (visualizar) el <i>score</i> de riesgo de pérdida de capacidad funcional utilizando el modelo predictivo IRENE <sup>R</sup> .
2	Usuario: Registro usuario	Como usuario no registrado, quiero solicitar registrarme en la plataforma para tener acceso a las funcionalidades adicionales disponibles para una cuenta usuario registrado (ej. mantención historial cálculos <i>score</i> pacientes, emisión <i>carne</i> de riesgo de pérdida de capacidad funcional etc.) proporcionando el conjunto de datos requerido para mi registro como usuario.
3	Administrador de un centro: gestión cuentas usuarios del centro	Como usuario administrador, quiero crear yo mismo/a cuentas para usuarios nuevos y administrar cuentas de los usuarios registrados asociados a mi establecimiento de salud.
4	Administrador de un centro: auditoría	Como usuario administrador de un establecimiento, quiero acceder al registro de auditoría de accesos y uso de la plataforma IRENE por parte de los usuarios asociados al establecimiento que administro, con oportunas funcionalidades de búsqueda y filtro (por fechas, períodos, usuarios, acciones realizadas, etc.).
5	Administrador de un centro: estadísticas	Como usuario administrador de un establecimiento, quiero acceder a las estadísticas de acceso y uso de la plataforma por parte de los usuarios registrados de mi establecimiento.

6	Usuario registrado: gestión perfil	Como usuario registrado, quiero editar los datos de usuario (perfil) de mi cuenta en la plataforma, por ejemplo, para mantener los datos de contacto actualizados o cambiar mi contraseña.
7	Usuario registrado: gestión de sus pacientes	Como usuario registrado, quiero gestionar (visualizar, crear, modificar o borrar según el caso) los registros de información, datos demográficos y cálculos de <i>score</i> de riesgo de mis pacientes en la plataforma*.
8	Usuario registrado: gráficos de perfiles de trayectorias de la capacidad funcional	Como usuario registrado, quiero ver los datos relacionados con la capacidad funcional (variables de <i>input</i> , <i>score</i> de riesgo e historial) de mis pacientes para poder realizar alguna intervención (por ejemplo, alguna acción preventiva).
9	Usuario registrado: búsqueda	Como usuario registrado, quiero realizar una búsqueda en los datos de mis pacientes de acuerdo a cualquiera de sus datos y filtrar los resultados para, por ejemplo, realizar comparaciones o notificar pacientes que pertenecen a determinados grupos o corresponden a ciertos criterios para eventuales acciones de salud.
10	Usuario registrado: información adicional	Como usuario registrado, en correspondencia de la realización de un cálculo de <i>score</i> de riesgo, quiero ingresar información adicional, por ejemplo, relacionada con el contexto de la toma de exámenes y/o de la captura de datos (variables) utilizados o necesarios para el cálculo del <i>score</i> de riesgo para mi paciente (ej. fecha de toma exámenes o mediciones ingresadas, que podría no corresponder a la fecha actual en que el usuario registrado realiza el cálculo del <i>score</i> de riesgo).
11	Usuario registrado: carnet de riesgo de pérdida de capacidad funcional	Como usuario registrado, quiero generar y emitir el carnet de riesgo de pérdida de capacidad funcional (como documento digital) de un paciente mío para que pueda enviárselo en formato digital o entregarlo físicamente impreso a mi paciente.
12	Usuario registrado: carga masiva	Como usuario registrado, quiero hacer una carga masiva de datos (variables utilizadas o necesarias para el cálculo del <i>score</i> de riesgo) de múltiples pacientes a la plataforma para que puedan ser utilizados para calcular sus <i>scores de pérdida de funcionalidad</i> de forma masiva, junto con sus datos de identificación.

13	Super administrador: gestión de establecimientos	Como usuario super administrador, quiero gestionar (crear, editar y deshabilitar) establecimientos o centros de salud en la plataforma y asociarle usuarios, los que podré eventualmente designarle o asignarles (o revocarles si ya lo tuvieran) el rol de administrador de ese determinado establecimiento o de más de un establecimiento (los que serán luego los que gestionarán los usuarios registrados asociados a su correspondiente establecimiento, centro de salud o prestador de salud institucional).
14	Super administrador: gestión de cuentas de usuario	Como usuario super administrador, quiero revisar y aprobar (o no) solicitudes de registro de usuarios individuales no asociados a establecimientos, centros o prestadores de salud institucionales y quiero también poder gestionar (crear, editar y deshabilitar) cuentas de usuario registrado, ya sea asociados a cualquier establecimiento de salud o que corresponden a profesionales prestadores de salud individuales no asociados a un establecimiento o centro de salud o prestador institucional (i.e. personas naturales, profesionales independientes o de todas formas prestadores de salud individuales).
15	Super administrador: auditoría	Como usuario super administrador, quiero acceder al registro completo de auditoría de accesos y uso de la plataforma web IRENESALUD.CL por parte de todos los usuarios de la plataforma con oportunas funcionalidades de búsqueda y filtro (ej. por fechas, períodos, usuarios/establecimientos, acciones realizadas, etc.).
16	Super administrador: estadísticas	Como usuario super administrador, quiero acceder estadísticas agregadas de acceso y uso de la plataforma web IRENESALUD.CL por parte de grupos o perfiles de usuarios de la plataforma (ya sea registrados o no, individuales o asociados a establecimientos o centros de salud) con oportunas funcionalidades de búsqueda y filtro (ej. por grupos, fechas, períodos, usuarios/establecimientos, etc.), sobre todo en relación al uso de la principal funcionalidad ofrecida por la plataforma: la calculadora para el <i>score</i> de riesgo de pérdida de capacidad funcional de las personas basada en el modelo predictivo IRENE <sup>R</sup> .
17	Usuario: verificación validez y vigencia del carnet de riesgo	Como usuario (ya sea anónimo que accede a la plataforma web o registrado), quiero poder verificar en línea (a través de la misma plataforma web IRENESALUD.CL) la autenticidad y vigencia de un carnet de riesgo de pérdida de funcionalidad (documento digital) que ha sido emitido por parte de un usuario registrado de la plataforma web.

(\*) Las funcionalidades de borrado o eliminación de datos o registros de todo tipo, en particular y sobre todo también de datos de pacientes que están a disposición de los usuarios registrados

de la plataforma deberán habilitarse de tal forma que desaparezcan a la vista de los usuarios pero en ningún caso podrán eliminarse realmente de la base de datos (por ej. manejando oportunamente los estados de la información “vigente”, “borrado” etc. y las fechas y usuarios que realizan dichos cambios de estado, cfr. Registros de auditoría). Esto para efectos de poder establecer siempre y en todo momento todo el historial de la información que fue o es manejada en la plataforma en un dado momento.

## Requerimientos no Funcionales

A continuación, el conjunto de requerimientos no funcionales previstos para la Plataforma web IRENESALUD.CL. La empresa oferente, proveedora o proveedor podrá eventualmente proponer también otros adicionales o alternativos, toda vez que el resultado final resulte en una mejora de los correspondientes aspectos o atributos indicados a continuación o de aquellos atributos considerados en el ámbito de la Calidad del Software (ver estándar ISO 25010).

Requerimiento	Formulación de una propuesta relacionada
Seguridad  Privacidad (cumplimiento de las leyes de privacidad, Ley 19.628, Ley 20.584 y sus reglamentos)  Confidencialidad de la información  Integridad de los datos  Disponibilidad de los datos y de la plataforma  Estabilidad	<p>En relación a estos aspectos se espera que la empresa proveedora indique en su propuesta de qué forma abordaría estos requerimientos no funcionales teniendo en cuenta que la plataforma manejará información personal y sensible. Partiendo desde el diseño y desarrollo del software, hasta la arquitectura, infraestructura y servicios en la nube y -de cara a los usuarios- se espera que la propuesta indique un adecuado equilibrio (“<i>trade-off</i>”) entre aspectos de seguridad vs. usabilidad (e.g. “<i>usable security</i>”). Más en general se espera que la propuesta permita evidenciar que la empresa proveedora tiene una visión de conjunto y aplicará políticas, principios y controles relacionados con la Seguridad de la Información en todos los estados en los que esta pueda encontrarse (en tránsito o almacenada).</p>
Rendimiento ( <i>performance</i> ): tiempo de respuesta  1. <i>Page load time</i> 2. Cálculo del <i>score</i> 3. Visualización 4. Escalabilidad (elasticidad)	<p>Se espera que la empresa proveedora proponga indicadores-objetivo relacionados con estos aspectos.</p>
Aplicación/Accesibilidad  Compatibilidad  Portabilidad	<p>Se espera que la empresa utilizará un diseño y desarrollo web adaptable, adaptativo o responsivo, para que la plataforma web IRENESALUD.CL pueda resultar accesible de forma adecuada a través de un <i>browser</i> desde casi cualquier dispositivo, computador, <i>tablet</i>, <i>smartphone</i> o características de la pantalla que tuviera a disposición el usuario.</p>



Usabilidad (aprendizaje, eficiencia, memorabilidad, errores y satisfacción)	Se espera que la empresa proveedora proponga criterios y/o métricas-objetivo relacionados con estos aspectos.
Interoperabilidad Integrabilidad	A pesar de que en esta fase del proyecto no se contempla la integración con sistemas de terceros, se privilegiará de todas formas una propuesta que incorpore el uso de estándares orientados a la interoperabilidad.
Documentación	Se solicita un conjunto de documentación que está descrita más adelante en la sección “Requerimientos de Transferencia Tecnológica”.

### Lenguajes, *frameworks*, herramientas, bases de datos y servicios utilizados

La empresa oferente deberá indicar dentro de su propuesta técnica los lenguajes, *frameworks*, herramientas y servicios que utiliza habitualmente para el desarrollo software y en particular cuáles propone utilizar en particular para el desarrollo y mantención de la Plataforma web IRENESALUD.CL. indicando también las eventuales dependencias que podrían darse producto de su utilización respecto del ciclo de vida del software de la plataforma web IRENESALUD.CL.

### Requerimientos de infraestructura y servicios en la nube

De preferencia, para la puesta en marcha y operación de la plataforma web IRENESALUD.CL la propuesta deberá considerar la utilización de los servicios en la nube provistos por Amazon Web Services (AWS), sin embargo, la empresa oferente podrá proponer otras tecnologías, soluciones o proveedores de servicios alternativos, siempre y cuando las acompañe de una justificación fundada de la mejor oportunidad respecto de AWS a su juicio, y esta tecnología ser aprobada por la Contratante, por cumplir las exigencias técnicas para dar cumplimiento a los fines del Proyecto IRENE FONDEF ID19I10319.

En particular, la empresa oferente deberá incluir en su oferta técnica las descripciones y diagramas arquitecturales (de alto nivel) de los servicios en la nube que propone preliminarmente utilizar para el desarrollo, despliegue y operación de la Plataforma web IRENESALUD.CL en la que se pueda además apreciar la aplicación de los principios o pilares básicos de seguridad en el diseño o arquitectura de servicios en la nube.

Se señala de todas formas, que tanto el proveedor de servicios en la nube a elegir como las decisiones del diseño y la determinación de la arquitectura, infraestructura y servicios en la nube sobre la cual funcionará finalmente la Plataforma web IRENESALUD.CL deberá contar con la aprobación de la contratante puesto que será esta la que por un lado asumirá el control de la cuenta y arquitectura de despliegue en operación o producción de la plataforma. La contratante también asumirá los costos de los servicios en la nube relacionados con el entorno y/o la/s instancias e infraestructura de producción y será además la que asumirá gran parte de la responsabilidad hacia los usuarios finales, por lo que ésta velará con particular énfasis por la Seguridad de la Información, partiendo desde el diseño mismo de la infraestructura y servicios

entre otros aspectos, sin perjuicio de la noción de que la seguridad es una responsabilidad compartida.

Se hace especial hincapié además que toda intervención que se hiciera necesaria por razones de soporte técnico, investigación de incidentes, monitoreo, auditorías, mantención correctiva o cualquier otra causal que hiciera necesario realizar un acceso a la instancia, infraestructura, servicios y bases de datos de la instancia de producción y/o las de respaldo o contingencia de la Plataforma web IRENESALUD.CL por parte de la empresa desarrolladora de la misma sólo podrá realizarse de forma segura, con la autorización explícita escrita y bajo la supervisión directa de la contratante con el fin de poder dar cumplimiento a las Políticas de Privacidad y de Protección de los Datos vigentes relacionadas con la plataforma, tal como señalado también en la sección Requerimientos de infraestructura y servicios en la nube de estas bases.

## Requerimientos de Transferencia Tecnológica

### Trabajo en equipo

Se requerirá que al menos un miembro del equipo de TI de la contratante se incorpore en algunas de las instancias de trabajo con el equipo de desarrollo de la empresa proveedora en calidad de analista observador por parte de la contratante. Dicha incorporación tendrá que ocurrir desde el inicio del trabajo de desarrollo no solamente como parte de una estrategia de transferencia tecnológica, sino que también para que dicho profesional conozca, aporte y participe activamente de las decisiones relacionadas con la arquitectura, infraestructura y servicios en la nube del ambiente de producción que estará bajo el control de la contratante (ver Requerimientos de Infraestructura y Servicios en la Nube).

### Código fuente, licencia para modificar el código y comentarios

La empresa proveedora deberá considerar la entrega a la contratante de los códigos fuente de los programas informáticos desarrollados en relación con la Plataforma web IRENESALUD.CL El código fuente deberá contar con comentarios de bloque y de línea según corresponda, para facilitar la comprensión y la mantenibilidad del software. La contratante será la dueña exclusiva de la propiedad intelectual sobre todo el material, código fuente y demás artefactos desarrollados por la proponente en el marco de la presente licitación y durante la ejecución del contrato, así como sobre los manuales de usuario, bases de datos, “runbook”, presentaciones explicativas, material de capacitación sobre la arquitectura del software, y demás entregables desarrollados por la contraparte en el marco de la ejecución del presente encargo (ver también la sección “Propiedad Intelectual” más adelante).

### Capacitación

Se requiere que la empresa proveedora considere y proporcione una o más instancias de capacitación dirigidas a los equipos profesionales de TI de la contratante sobre la descripción de la arquitectura y las actividades más relevantes de gestión de la infraestructura y servicios en la

nube relacionados con la plataforma en producción. En dichas instancias se podrán además utilizar los *runbook* señalados más adelante en estas bases.

## Documentación

Se deberá entregar la documentación relevante que describa la estructura y las componentes software desarrolladas y aquellas componentes, dependencias, paquetes, librerías o equivalente ya sea propias o de terceros utilizadas para el desarrollo y funcionamiento de la Plataforma web IRENESALUD.CL indicando además la referencia al tipo de licencia de terceros relacionada. Dentro de la documentación relevante deberá estar incluida la entrega del Diccionario de Datos de la o de las bases de datos relacionadas con la Plataforma web IRENESALUD.CL.

Adicionalmente, se deberá confeccionar un *runbook* con la descripción del conjunto de las principales rutinas y procedimientos de administración de las componentes de sistema que permiten el funcionamiento y operación de la Plataforma web IRENESALUD.CL, incluidas las rutinas o procedimientos de levantamiento, inicio, detención, supervisión y administración de los servicios, componentes, bases de datos, eventuales servidores e infraestructura en la nube. En particular deberán incluir también las rutinas para hacer frente a incidentes o contingencias operacionales que pudieran afectar cualquiera de las componentes de sistema. La contratante podrá poner a prueba la ejecución de las rutinas y procedimientos documentados en el *runbook* previo a su aceptación. Materialmente el *runbook* tendrá que corresponder a un documento digital fechado y versionado, incluida una versión del mismo en formato editable para facilitar su mantención y actualización en el tiempo.

Todos estos elementos deberán estar explícitamente indicados en la oferta técnica y formarán parte del conjunto de los entregables esperados, es decir también deberán explicitarse en correspondencia al cronograma o plan de trabajo.

No se requiere el desarrollo de manuales de usuario propiamente tales, porque se espera que el nivel de UI/UX alcanzado por la Plataforma web IRENESALUD.CL permita un suficiente y adecuado uso de la misma por parte de la gran mayoría de los usuarios, y de llegar a ser necesario, será desarrollado por la contratante.

## Soporte y Mantención Correctiva

La empresa oferente deberá incluir y detallar en su oferta la entrega de un servicio de soporte técnico y mantención software correctiva de la plataforma que abarque un período desde la puesta en marcha (“producción”) de la **Plataforma web IRENESALUD.CL** hasta el **31 de diciembre 2022**, detallando los canales de comunicación disponibles para notificar o informar sobre incidentes, los tiempos de primera respuesta y los tiempos de resolución máximos comprometidos. Los eventuales accesos a la instancia, infraestructura, servicios y bases de datos de la instancia de producción y/o las de respaldo o contingencia de la Plataforma web IRENESALUD.CL que fueran necesarios por parte del desarrollador de la misma para los efectos de actividades soporte técnico, investigación de incidentes, monitoreo, auditorías o mantención

correctiva, sólo podrán realizarse con la autorización explícita escrita y bajo la supervisión directa de la contratante con el fin de poder dar cumplimiento a las Políticas de Privacidad y de Protección de los Datos relacionados con dicha plataforma.

## Actividades y Pruebas de Aceptación

Sin perjuicio de lo ya señalado en estas bases sobre la metodología, cronograma de trabajo, y en particular sobre los aspectos de calidad y seguridad del software, la contratante se reserva el derecho de realizar actividades de aseguramiento de la calidad, seguridad y certificación de la plataforma y sus componentes cuyos resultados someterá oportunamente a la atención de la empresa proveedora y que serán parte además del conjunto de pruebas de aceptación-entrega. La empresa proveedora deberá insertarlas adecuada y oportunamente en el Plan de Trabajo que presentará en su oferta.

## Prácticas de Seguridad en el desarrollo software de la empresa

La empresa oferente deberá llenar y enviar junto con los demás elementos de su oferta el **Formulario de Prácticas de Desarrollo Seguro de Software** (Anexo 1) que está basado en las recomendaciones que emanan del white paper del NIST “*Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*” del 23 de Abril 2020 (disponible <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf>)

La información proporcionada a través de dicho formulario concurrirá a determinar (en parte) la capacidad técnica de la empresa en relación a las prácticas de seguridad que tiene actualmente implementadas en su desarrollo software habitual.

## Propiedad Intelectual

La empresa oferente reconoce que el modelo predictivo **IRENE<sup>R</sup>** corresponde a una tecnología de propiedad exclusiva de la contratante por lo que sobre dicho modelo acepta y reconoce que no tiene ningún título de propiedad, derecho o licencia ni de uso ni menos de cesión o licenciamiento a terceros sin la autorización previa escrita de parte de la contratante.

Por otra parte, la empresa proveedora reconoce, acepta y declara explícitamente que la propiedad intelectual sobre el código fuente, programas, diseños, elementos gráficos o audiovisuales y todo artefacto o creación que la empresa proveedora desarrollará para la **Plataforma web IRENESALUD.CL** será de la Universidad del Desarrollo, la que podrá administrarlos y gestionarlos a su total arbitrio y sin restricciones de ninguna especie. Dicha materia será de todas formas explicitada con mayor detalle en el ámbito del contrato de servicios correspondiente.

*\*end of file\**

## Anexo 1 - Formulario de Prácticas de Desarrollo Seguro de Software

Completar este formulario sobre las prácticas de desarrollo seguro de software que lleva a cabo actualmente la empresa oferente en el ámbito de sus procesos de desarrollo software. La información proporcionada a través de dicho formulario será parte de los insumos que se utilizarán para determinar la capacidad y pericia técnica de la empresa. Este formulario se basa y considera las recomendaciones que emanan del *white paper* del NIST “*Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*” edición del 23 de Abril 2020 que está disponible al siguiente enlace: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf>. Revisar dicho documento para más detalles, ejemplos e información sobre las prácticas o tareas que aparecen en este formulario.

### **Términos y acrónimos utilizados**

**Cadena de herramientas:** del inglés *toolchain*, la cadena de herramientas o el conjunto de programas informáticos que se usan para crear un programa o un sistema informático.

**NIST** – *National Institute of Standards and Technology* : el Instituto Nacional de Estándares y Tecnologías de los EE.UU.

**SDLC** – *Software development life cycle* : el ciclo de vida del desarrollo de software.

**SSDF** – *Secure Software Development Framework* : el Marco de Desarrollo Seguro de Software del NIST (cfr. “*Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*” del NIST, edición del 23 de Abril 2020).

### **Instrucciones para llenar el formulario**

En la tabla denominada “Prácticas de Desarrollo Seguro de Software” (páginas a continuación), llenar los campos de “*Nombre Empresa / Razón Social*” y “*Fecha*”, luego llenar cada una de las celdas de la columna “*Código Grado Implementación Empresa Oferente*” para indicar el grado de implementación de cada una de las prácticas de desarrollo software seguro que allí aparecen indicadas en cada línea. Para indicar el grado de implementación utilizar exclusivamente uno de los códigos (3, 2, 1 o N/A) para expresar lo descrito en la leyenda a continuación.

### **Leyenda códigos para llenar el formulario**

Códigos para el llenado de la columna “*Código Grado Implementación Empresa Oferente*”.

<b>3 (siempre)</b>	Para indicar que la empresa oferente <b>realiza esta práctica-tarea en todos sus desarrollos</b>
<b>2 (frecuentemente)</b>	Para indicar que la empresa oferente <b>realiza esta práctica-tarea en la gran mayoría de sus desarrollos</b>
<b>1 (ocasionalmente)</b>	Para indicar que la empresa oferente <b>realiza esta práctica-tarea sólo en algunos desarrollos</b>
<b>0 (nunca)</b>	Para indicar que la empresa oferente <b>no realiza esta práctica en sus desarrollos</b>

N/A	Para indicar que la <b>práctica-tarea no aplica para el tipo de desarrollos, herramientas o tecnologías que utiliza o realiza la empresa oferente</b>
-----	---

Formulario Prácticas NIST-SSDF 23.4.2020 de Desarrollo Seguro de Software			
<b>Nombre Empresa / Razón Social:</b>			
<b>Fecha:</b>			
Código-Práctica NIST-SSDF	Código y Descripción Tarea NIST-SSDF (modificado el tiempo verbal en presente de indicativo respecto de la formulación original en infinitivo del NIST-SSDF)	Código del Grado Implementación Empresa Oferente [ver leyenda códigos]	
<b>PO.1</b> Definir los requisitos de seguridad para el desarrollo de software	<b>PO.1.1</b> Identifica todos los requisitos de seguridad aplicables para el desarrollo general de software de la organización, y mantiene los requisitos a lo largo del tiempo.	<i>Ejemplo:</i> 2 (frecuentemente)	
<b>PO.2</b> Implementar los roles y responsabilidades	<b>PO.2.1</b> Crea nuevos roles y modifica las responsabilidades de los roles existentes para abarcar todas las partes del SSDF. Revisa periódicamente las funciones y responsabilidades definidas, y las actualiza cuando es necesario.	<i>Ejemplo:</i> 3 (siempre)	
	<b>PO.2.2</b> Proporciona formación específica para cada rol a todo el personal con responsabilidades que contribuyan al desarrollo seguro. Revisa periódicamente la formación específica de cada función y la actualiza según sea necesario.		
	<b>PO.2.3</b> Consigue el compromiso de la alta dirección para el desarrollo seguro, y transmite ese compromiso a todos los que tienen funciones y responsabilidades relacionadas con el SSDF		
<b>PO.3</b> Implementar una cadena de herramientas de apoyo	<b>PO.3.1</b> Especifica qué herramientas o tipos de herramientas deben incluirse en cada cadena de herramientas ( <i>toolchain</i> ) y cuáles son obligatorias, así como el modo en que los componentes de la cadena de herramientas deben integrarse entre sí.		
	<b>PO.3.2</b> Conforme a prácticas de seguridad sólidas, despliega y configura herramientas, las integra dentro de la cadena de herramientas y		

	<p>mantiene las herramientas individuales y la cadena de herramientas como un todo.</p> <p><b>PO.3.3</b> Configura las herramientas para recoger evidencia y artefactos de su soporte de las prácticas de desarrollo de software seguro.</p>	
<p><b>PO.4</b> Definir los criterios para las verificaciones de seguridad del software</p>	<p><b>PO.4.1</b> Define los criterios para las verificaciones de seguridad del software a lo largo del ciclo de vida del desarrollo de software (SDLC).</p>	
	<p><b>PO.4.2</b> Implementa procesos, mecanismos, etc. para reunir la información necesaria en apoyo de los criterios.</p>	
<p><b>PS.1</b> Proteger todas las formas de código contra el acceso no autorizado y la manipulación.</p>	<p><b>PS.1.1</b> Almacena todas las formas de código, incluido el código fuente y el código ejecutable, basándose en el principio de mínimo privilegio, de modo que sólo el personal autorizado tiene las modalidades o medios de acceso necesarios.</p>	
<p><b>PS.2</b> Proporcionar un mecanismo para verificar la integridad de la versión del software.</p>	<p><b>PS.2.1</b> Pone la información de verificación a disposición de los consumidores de software.</p>	
<p><b>PS.3</b> Archivar y proteger cada versión de software</p>	<p><b>PS.3.1</b> Archiva de forma segura una copia de cada versión y todos sus componentes (por ejemplo, código, archivos de paquetes, bibliotecas de terceros, documentación), así como la información de verificación de la integridad de la versión.</p>	
<p><b>PW.1</b> Diseñar el software para cumplir los requisitos de seguridad y mitigar los riesgos de seguridad</p>	<p><b>PW.1.1</b> Utiliza formas de modelado de riesgos, como el modelado de amenazas, el modelado de ataques o el mapeo de la superficie de ataque, para ayudar a evaluar el riesgo de seguridad para el software.</p>	
<p><b>PW.2</b> Revisar el diseño del software para verificar el cumplimiento de los requisitos de seguridad y la información sobre riesgos</p>	<p><b>PW.2.1</b> Hace que una persona cualificada que no haya participado en el diseño del software lo revise para confirmar que cumple todos los requisitos de seguridad y que aborda satisfactoriamente la información de riesgo identificado.</p>	
<p><b>PW.3</b> Verificar que el software de terceros cumple con los requisitos de seguridad</p>	<p><b>PW.3.1</b> Comunica los requisitos a terceros que pudieran proporcionar módulos y servicios de software a la organización para su reutilización por el propio software de la organización.</p>	
	<p><b>PW.3.2</b> Utiliza los medios adecuados para verificar que los módulos y servicios de software comerciales, de código abierto y todos los otros de terceras partes cumplen con los requisitos.</p>	

<p><b>PW.4</b> Reutilizar el software bien protegido ya existente cuando sea posible, en lugar de duplicar la funcionalidad</p>	<p><b>PW4.1</b> Adquiere componentes bien protegidos (por ejemplo, bibliotecas de software, módulos, middleware, <i>frameworks</i>) de terceros para ser utilizados por el software de la organización.</p>	
	<p><b>PW4.2</b> Crea componentes de software bien protegidos internamente siguiendo los procesos del SDLC para satisfacer las necesidades comunes de desarrollo de software interno que no pueden ser satisfechas mejor por software de terceros.</p>	
	<p><b>PW4.3</b> Cuando fuera apropiado, incorpora soporte para el uso de características y servicios de seguridad estandarizados (por ejemplo, integración con sistemas de gestión de bitácoras, gestión de identidades, control de acceso y gestión de vulnerabilidades) en lugar de crear implementaciones propietarias de características y servicios de seguridad.</p>	
<p><b>PW.5</b> Crear un Código Fuente que se adhiera a las prácticas de codificación segura</p>	<p><b>PW.5.1</b> Sigue todas las prácticas de programación seguras que sean apropiadas para los lenguajes y el entorno de desarrollo.</p>	
	<p><b>PW.5.2</b> Hace que el desarrollador revise su propio código legible por el ser humano, analice su propio código legible por el ser humano y/o pruebe su propio código ejecutable para complementar (no sustituir) la revisión, el análisis y/o la prueba del código realizada por otros.</p>	
<p><b>PW.6</b> Configurar los procesos de compilación y construcción (<i>build</i>) para mejorar la seguridad de los ejecutables</p>	<p><b>PW.6.1</b> Utiliza herramientas de compilación y construcción que ofrecen funciones para mejorar la seguridad de los ejecutables.</p>	
	<p><b>PW.6.2</b> Determina qué características del compilador y de la herramienta de compilación deben utilizarse y cómo debe configurarse cada una de ellas y, a continuación, aplica la configuración aprobada para las herramientas de compilación y construcción, los procesos, etc.</p>	
<p><b>PW.7</b> Revisar y/o analizar código legible por humanos para identificar vulnerabilidades y verificar el cumplimiento de los requisitos de seguridad</p>	<p><b>PW.7.2</b> Determina si se debiera utilizar una revisión del código (es decir, una persona revisa directamente el código para encontrar problemas) y/o el análisis de código (es decir, se utilizan herramientas para encontrar problemas en el código, ya sea de forma totalmente automatizada o junto con una persona).</p>	
	<p><b>PW.7.3</b> Realiza la revisión del código y/o el análisis del código basándose en las normas de programación segura de la organización, y</p>	



	documenta y prioriza/clasifica todos los problemas descubiertos y las soluciones recomendadas en el flujo de trabajo del equipo de desarrollo o en el sistema de seguimiento de incidentes.	
<b>PW.8</b> Prueba de código ejecutable para identificar vulnerabilidades y verificar el cumplimiento de los requisitos de seguridad	<b>PW.8.1</b> Determina si deben realizarse pruebas de código ejecutable y, en caso afirmativo, qué tipos deben utilizarse.	
	<b>PW.8.2</b> Diseña las pruebas, las realiza y documenta los resultados.	
<b>PW.9</b> Configurar el software para que tenga una configuración segura por defecto	<b>PW.9.1</b> Determina cómo configurar cada ajuste que tenga un efecto sobre la seguridad para que los ajustes por defecto sean seguros y no debiliten las funciones de seguridad proporcionadas por la plataforma, la infraestructura de red o los servicios.	
	<b>PW.9.2</b> Implementa las configuraciones por defecto (o grupos de configuraciones por defecto, si procede), y documenta cada configuración para los administradores de software.	
<b>RV.1</b> Identificar y confirmar las vulnerabilidades de forma continua	<b>RV.1.1</b> Recopila información de los consumidores y de fuentes públicas sobre las potenciales vulnerabilidades del software y de los componentes de terceros que utiliza el software, e investiga todos los informes creíbles.	
	<b>RV.1.2</b> Revisa, analiza y/o prueba el código del software para identificar o confirmar la presencia de vulnerabilidades no detectadas previamente.	
	<b>RV.1.3</b> Dispone de un equipo y procesos para gestionar las respuestas a los reportes de vulnerabilidad e incidentes.	
<b>RV.2</b> Evaluar, priorizar y remediar las vulnerabilidades	<b>RV.2.1</b> Analiza cada vulnerabilidad para reunir información suficiente para planificar su remediación.	
	<b>RV.2.2</b> Desarrolla y aplica un plan de remediación para cada vulnerabilidad.	
<b>RV.3</b> Analizar las vulnerabilidades para identificar sus causas - raíz (origen)	<b>RV.3.1</b> Analiza todas las vulnerabilidades identificadas para determinar la causa raíz de cada una de ellas.	
	<b>RV.3.2</b> Analiza las causas raíz a lo largo del tiempo para identificar patrones, como por ejemplo cuando no se sigue una práctica de programación segura en particular.	

	<b>RV.3.3</b> Revise el software en busca de otras instancias del problema reportado y corríjalo proactivamente en lugar de esperar los reportes externos.	
	<b>RV.3.4</b> Revisa el proceso SDLC y lo actualiza según corresponda para evitar (o reducir la probabilidad de) que la causa raíz se repita en las actualizaciones de este software o en el nuevo software que se cree.	

\*fin formulario\*