ANEXO 8 – SOLUCIÓN TÉCNICA Y DE SEGURIDAD

INTRODUCCIÓN:

El proponente deberá describir en su propuesta si proporciona cada funcionalidad solicitada en el presente anexo, para lo cual solicitamos que las respuestas sean diligenciadas como se indica en la tabla detallada al final con el nombre **FORMATO PARA CONSOLIDAR RESPUESTAS**. Si requiere dar más información sobre la respuesta, favor detallar el número de folio a que hace referencia.

Adicionalmente, la herramienta ofrecida debe ser comercial y se debe encontrar en el mercado funcionando de manera exitosa en otros clientes.

1. INFORMACIÓN ESPECÍFICA DE LA SOLUCIÓN TÉCNICA Y DE SEGURIDAD REQUERIDA

El Proponente debe incluir las licencias necesarias para la puesta en producción de la solución ofrecida y su actualización, aclarando que el Banco no incurrirá en costos de licenciamiento.

1.1 Características generales de la solución. El proponente deberá describir:

- Nombre del producto, versión del producto (si no es la última versión liberada, explique porque) y fecha de liberación de la versión presentada y Fecha de liberación de la próxima versión (si se conoce).
- Idiomas que maneja la solución (se requiere en español)
- Detallar los módulos que contempla la solución propuesta y hacer una descripción de su alcance.
- Indicar el proceso y las metodologías de actualización e instalación de una versión del software del gestor del contenido.
- Esquema para garantizar que las herramientas, componentes y demás piezas de software que integran la solución presentada, serán actualizadas con el fin de mantener el soporte por parte del fabricante
- Especificar los tiempos de respuesta o latencia que puede ofrecer para el despliegue de las páginas del portal dependiendo de las características de contenido y el número máximo de usuarios concurrentes. (Bancoldex estima 100 usuarios concurrentes).

1.2 Arquitectura Tecnológica. A continuación se pide que el proveedor de respuesta a la Arquitectura tecnológica que dispone la solución ofrecida, teniendo en cuenta que el Banco requiere contratar el servicio de Hosting, por lo que el dimensionamiento se debe dar en términos de licenciamiento y capacidad de TIC. Dar respuesta:

1.2.1 Arquitectura de la solución.

- **Diagrama.** Adjuntar el diagrama donde se muestre claramente la arquitectura de la solución propuesta. Hacer una descripción de todos los componentes que se utilizarán en las diferentes capas.
- **Arquitectura**. Detallar el tipo de arquitectura de la solución ofrecida: Monolítica, WEB, Cliente – Servidor, otra.
- **Disponibilidad**. Detallar el esquema de disponibilidad para la solución ofrecida, para lo cual el Banco requiere que esta sea 7*24, con un indicador de por lo menos el 99.8%
- **Rendimiento**. Como garantiza el Proponente que el sistema propuesto tenga un código optimizado para alto rendimiento y velocidad

1.2.2 Arquitectura del software:

- Sistema Operativo, bases de datos: Motor y versiones, Software base, Lenguaje de desarrollo utilizado, que soporta la solución ofrecida.
- Se presenta compatibilidad con los estándares html5 y css3. En caso de presentarse, el proponente deberá detallar con que otros estándares presenta compatibilidad.
- Indicar el grado de Portabilidad.
- **Presentación de interfaz gráfica.** Detallar para cada uno de los siguientes ítems el alcance:
  - ✓ Especificar los dispositivos y tecnologías compatibles con la solución presentada: dispositivos móviles, equipos de escritorio, portátiles, etc.
  - ✓ Como es el esquema de adaptación a los diferentes tamaños de salida
  - ✓ La interfaz gráfica debe presentar un diseño intuitivo.
- Indicar si presenta la facilidad de Streaming Distribución digital de contenido multimedia.

1.2.3 Arquitectura del Hardware.

- Detallar en un modelo, la arquitectura de hardware que se propone para la solución requerida.
- Cuáles son los requerimientos mínimos y óptimos en que trabaja la solución.
- Para servidores indicar: Tipo de servidores, procesador (características), memoria, capacidad de almacenamiento, asignación de servidores, tarjetas de Red, características de disponibilidad y escalabilidad

1.2.4 Arquitectura de redes y comunicaciones.

- Descripción de la arquitectura de red y comunicaciones.
- Características de disponibilidad y escalabilidad
- Velocidad del canal de comunicaciones
- Medición y registro de parámetros del uso del ancho de banda
- Evaluación y administración del reúso
- Sistema de administración de redes
- Disponibilidad del servicio del canal (Uptime requerido 99.9995%)

1.3 Servicio de HOSTING.

El proponente deberá proporcionar el servicio de hosting para alojar la página web. El hosting debe ser dimensionado de tal manera que la página web tenga un óptimo rendimiento y no presente desperdicio de recursos. Igualmente debe contar con los debidos mecanismos de seguridad física y lógica para evitar ataques o intrusiones maliciosas.

El servicio de hosting antes de ser puesto en producción debe acometer una prueba de vulnerabilidad que será realizada y acordada con el proponente seleccionado y evaluada por el Banco.

Se aclara que el Banco requiere para cumplimiento de lineamientos de entes de control, realizar pruebas de vulnerabilidad por lo menos dos veces al año. Adicionalmente, el sitio debe contar con certificados SSL, los cuales proveerá el Banco.

Favor dar respuesta a:

- Indicar el proveedor del servicio de hosting.
- Describa el esquema del servicio de hosting. Debe estar relacionado con la propuesta detallada en el ítem de arquitectura y se pide que esté en la nube.
- Especificar el esquema de seguridad que tendrá el servicio de hosting. Accesos no autorizados, ataque de negación de servicio y en general cualquier aspecto relacionado con la estabilidad y seguridad del sitio web en hosting.
- Describir el servicio de contingencia que tendrá la solución ofrecida a nivel de aplicación y servicio de hosting. Indicar si se cuenta con servicio de Data Center alterno.
- Permite fácil crecimiento en los recursos dependiendo de lo que se requiera en algún momento crítico? Como se gestiona este crecimiento.
- **Se** cuenta con WAF (Web Aplication Firewall) . Si se cuenta con un WAF este gestiona ataques de negación de servicio DDoS?
- Indique el tipo de FW ofrecido y describa sus características.
- Tiempo - ANS, para dar respuesta a las vulnerabilidades encontradas.
- Indicar estrategia para hardening “endurecer” el sistema operativo. Se recomienda demostrar que se acogen las buenas prácticas.
- Disponibilidad del servicio. Indicar los ANS’s, los indicadores asociados a continuidad, los cuales se esperan que estén en un porcentaje de disponibilidad del sitio WEB del 99.9%.
- Indicar cuál es el plan de Continuidad del servicio de soporte y mantenimiento para el sitio WEB y el HOSTING.
- Indicar las políticas de respaldo y recuperación del sistema: Aplicación, Datos.
- Indicar el proceso de contingencia para contar con la disponibilidad de los respaldos realizados.
- Indicar los ANS establecidos para contar con procesos de recuperación y disponibilidad de los datos y aplicación.
- Estrategia para actualizar o instalar parches: Hadware, software, redes y comunicaciones.

2. SOPORTE, MANTENIMIENTO Y CONTINUIDAD.

2.1. Generalidades soporte, mantenimiento correctivo y evolutivo. El proponente debe especificar:

- Describir el esquema del servicio de soporte y mantenimiento correctivo para la solución o para los componentes que presente en su propuesta (software base, aplicaciones, servicios, componentes, módulos, etc.).
- Describir el esquema del servicio a proponer para mantenimiento evolutivo (nuevos desarrollos, ya sean solicitados por el Banco o por el Proponente).
- Niveles de acuerdos de servicio para mantenimiento correctivo y evolutivo. Servicios, tiempos de respuesta, disponibilidad, prioridades, responsabilidades, documentación, garantías y penalizaciones.
- Informes que se usarán para el seguimiento y cuáles son los tiempos de entrega.
- Esquemas de monitoreo, seguimiento y control.
  - ✓ Incidencias
  - ✓ Problemas
  - ✓ Acuerdos de servicio (SLA). Niveles de acuerdos de servicio.
  - ✓ Acuerdos de Operación (OLA)
  - ✓ Niveles de atención
  - ✓ Controles de cambio
  - ✓ Manejo de versiones.
  - ✓ Configuraciones (aplicación, base de datos, servidores)
- Soporte sobre la funcionalidad de la solución 7x24x365.

3. PROCESO DE IMPLANTACIÓN

3.1. Esquema de Implantación y Adecuación.

- Describir el proceso de implantación y adecuación de la solución propuesta.
- Indicar el proceso para ajustar la solución propuesta de acuerdo con las adecuaciones o extensiones necesarias para que la solución ofrecida cumpla totalmente con los requerimientos definidos en estos términos.

- Cuál es el plan de cargue inicial y migración de datos para la operatividad de la solución indicando la participación del Banco y del proponente y qué condiciones se requieren para obtener una funcionalidad exitosa. Se espera que el porcentaje de migración del contenido actual frente a la nueva arquitectura esté entre un 30% a 40%.

3.3 Capacitación que brindará a la solución ofrecida.

El proponente deberá presentar las condiciones bajo las cuales brindará la capacitación respectiva en todos los componentes que integren la solución:

- Tipo de capacitación: Técnica, operación, administración y usuario.
- Contenido de cada curso, Duración e intensidad horaria.
- Grupo objetivo del curso y requisitos de grupo.
- Recursos necesarios para la capacitación u otras condiciones necesarias.
- En el capítulo de costos, detallar lo pertinente a este ítem

3.4. Pruebas de la solución ofrecida.

- Describir el proceso que se tiene para gestión de las pruebas del Desarrollador, Técnicas y de usuario.
  - ✓ Casos de prueba que contemplen múltiples escenarios de operación. Tener en cuenta escenarios para cargue manual y automática.
  - ✓ Pruebas integrales orientadas a verificar la integridad de operación y de los datos después de la ejecución de diferentes funcionalidades que los comparten.
  - ✓ Pruebas de rendimiento bajo carga
  - ✓ Pruebas de seguridad del software contra ataques
  - ✓ Pruebas de facilidad de uso con usuarios reales.
  - ✓ Pruebas modulares para verificar que la solución ofrecida funciona correctamente.
  - ✓ Pruebas de las interfaces (si se requieren).
  - ✓ Pruebas de funcionamiento del software en el hardware seleccionado
  - ✓ Pruebas para verificar que el servicio ofrecido funciona como se esperaba.
  - ✓ Pruebas de rendimiento (stress) orientada al acceso WEB.
- Indicar el procedimiento para gestión de incidentes o errores que ocurran en las pruebas y el procedimiento de atención. Cuáles son los ANS para su solución.
- Describir el proceso de aseguramiento de la calidad.
- Describir como la solución será probada en ambientes de máxima utilización simulando picos, volúmenes, números de usuarios y en general carga/sobrecarga del sistema.
- Establecer un procesos para hacer más rápidas las pruebas “Celeridad”, con el fin de evitar que se impacten los tiempos estimados para pasó a PRODUCCIÓN.
- El proveedor deberá prever la realización de una prueba de vulnerabilidad antes del paso a PRODUCCIÓN.

3.5. Documentación técnica y de usuario.

Los manuales deberán cumplen con los estándares especificados en el Manual de Identidad visual y corporativa de Bancóldex y se entregan en formato físico y digital y en idioma Español.

Indicar que documentación entrega el Proponente al Banco.

- Documentación técnica y de usuario.
- Manual de instalación.
- Documentación del proyecto o servicio ofrecido.

4 SEGURIDAD DE LA SOLUCIÓN OFRECIDA

El proponente debe describir los aspectos que la solución debe tener para evitar riesgos según el área o campo a la que haga referencia el riesgo. El proponente deberá presentar una matriz de riesgos y sus contingencias, con el fin de disminuir la incertidumbre de prórroga de las actividades detalladas en el cronograma del proyecto.

El proponente debe tener presente al menos los siguientes mecanismos de seguridad a implantar con la herramienta de software que se proponga:

- **Autenticación**
  El proponente deberá indicar lo siguiente
  :
  - ✓ El sistema se adapta para trabajar bajo un esquema Single Sign On.
  - ✓ Proceso de confirmación de la identidad del usuario. Antes de que una aplicación pueda autorizar el acceso a un recurso, debe confirmar su identidad. Esta es la primera capa de control de seguridad.
  - ✓ Roles de usuarios: La solución debe manejar un control de acceso a las opciones del sistema por roles. Un usuario puede tener asignado uno (1) o más roles.
  - ✓ Bloqueo intentos fallidos: Detallar si el sistema ofrecido cuenta con control de acceso al sistema a través de ingreso de usuario y contraseña y si controla los intentos fallidos de registro.
  - ✓ Parametrización de la contraseña. Se permite parametrizar la contraseña de acuerdo con políticas internas del Banco referente a número de caracteres, combinación de caracteres.
  - ✓ El sistema permite configurar los criterios de creación y cambio de clave del acceso al sistema: tiempo para cambio de clave, caracteres obligatorios, etc.

- **Autorización:**
  El proponente deberá indicar el proceso de verificación en caso que un usuario autenticado tenga permiso para obtener acceso a un recurso determinado. Siguiente capa de seguridad tras la autenticación.

- **Protección de datos:**
  El proponente deberá indicar el proceso consistente en proporcionar confidencialidad, integridad y no repudio a los datos.

- **Sistema de control interno (auditorias-logs):**

- Cuál es el proceso de registro y supervisión de los eventos que se producen en un sistema y que son importantes para la seguridad.
- Indicar que logs tiene implementados la solución ofrecida.
- Indicar el proceso de: Registro, consulta. Permite la consulta de logs a través de opciones de menú u opciones de perfil administrador y se puedan imprimir o exportar a un formato de fácil lectura las consultas.
- Que información contiene el log. El diseño de los logs debe contener por lo menos la siguiente información: fecha, hora, segundo, comentario.

- **Herramientas de seguridad:** El proponente deberá contar con por los menos las siguientes herramientas de seguridad: Antivirus, antispam, firewall, software para prevenir ataques o intrusiones, entre otros.

- **Cumplimiento políticas SEGURIDAD DE LA INFORMACIÓN.** El proponente deberá dar respuesta al cumplimiento de las políticas detalladas en el **anexo 10: Seguridad de la información**. **Políticas del SGSI, Habeas Data, Circular externa 042 de 2012, consideraciones Adicionales.**

6. Consolidación de respuestas

Se pide a los proponentes consolidar sus respuestas teniendo en cuenta el formato detallado en la tabla adjunta. Cada uno de los ítems, debe tener una respuesta asociada a sus sub-ítem:

Descripción	CUMPLE		Detallar la respuesta	Indicar si adjunta documentación adicional e indicar la identificación del documento anexo en la propuesta.
	SI	NO		
1- Características generales de la solución				
Nombre y versión del producto. Fecha de liberación de la versión presentada.				
Indicar el proceso y las metodologías de actualización e instalación de una versión del software del gestor del contenido.				
Esquema para garantizar que las herramientas, componentes y demás piezas de software que integran la solución presentada, serán actualizadas con el fin de mantener el soporte por parte del fabricante				
Especificar los tiempos de respuesta o latencia que puede ofrecer para el despliegue de las páginas del portal dependiendo de las características de contenido y el número máximo de usuarios				

concurrentes. (Bancoldex estima 100 usuarios concurrentes).				
1- ARQUITECTURA				
Arquitectura de la solución				
Diagrama. Adjuntar el diagrama donde se muestre claramente la arquitectura de la solución propuesta. Hacer una descripción de todos los componentes que se utilizarán en las diferentes capas. Que tipo Monolítica, WEB, Cliente – Servidor, otra.				
Disponibilidad. Detallar el esquema de disponibilidad para la solución ofrecida, para lo cual el Banco requiere que esta sea 7*24, con un indicador de por lo menos el 99.8%				
Rendimiento. Como garantiza el Proponente que el sistema propuesto tenga un código optimizado para alto rendimiento y velocidad				
3. Arquitectura del software				
Sistema Operativo que soporta la solución ofrecida, Bases de Datos: Motor y versiones.				
Presenta compatibilidad con los estándares html5 y css3. En caso de presentarse, el proponente deberá detallar con que otros estándares presenta compatibilidad.				
Indicar el grado de Portabilidad.				
Presentación de interfaz gráfica: • Presentación en diferentes tipos de dispositivos móviles • Indicar los diferentes tipos de navegadores que soporta. • Como es el esquema de adaptación a los diferentes tamaños de salida • La interfaz gráfica debe presentar un diseño intuitivo.				
Debe Presentar la facilidad de Streaming Distribución digital de contenido multimedia.				
4. Arquitectura del Hardware.				
Detallar en un modelo la arquitectura de hardware que se propone para la solución requerida. Se debe especificar los requerimientos mínimos y óptimos en que trabaja la solución.				
Cuáles son los requerimientos mínimos y óptimos en que trabaja la solución.				
Para servidores indicar: Tipo de servidores, procesador (características), memoria, capacidad de almacenamiento, asignación de servidores, tarjetas de Red, características de disponibilidad y escalabilidad				

5. Arquitectura de comunicaciones.				
Descripción de la arquitectura de red y comunicaciones.				
Características de disponibilidad y escalabilidad				
Velocidad del canal de comunicaciones				
Medición y registro de parámetros del uso del ancho de banda				
Evaluación y administración del reúso				
Infraestructura física				
Sistema de administración de redes				
Disponibilidad del servicio del canal (Uptime requerido 99.9995%)				
6. Generalidades soporte, mantenimiento correctivo y evolutivo				
Describir el esquema del servicio de soporte y mantenimiento correctivo para la solución o para los componentes que presente en su propuesta (software base, aplicaciones, servicios, componentes, módulos, etc.).				
Describir el esquema del servicio a proponer para mantenimiento evolutivo: nuevos desarrollos, ya sean solicitados por el Banco o por el Proponente.				
Niveles de acuerdos de servicio para mantenimiento correctivo y evolutivo. Servicios, tiempos de respuesta, disponibilidad, prioridades, responsabilidades, documentación, garantías y penalizaciones.				
Informes que se usarán para el seguimiento y cuáles son los tiempos de entrega.				
Soporte sobre la funcionalidad de la solución 7x24x365.				
Esquemas de monitoreo, seguimiento y control. ✓ Incidencias ✓ Problemas ✓ Acuerdos de servicio (SLA). Niveles de acuerdos de servicio. ✓ Acuerdos de Operación (OLA) ✓ Niveles de atención ✓ Controles de cambio ✓ Manejo de versiones. ✓ Configuraciones: Aplicación, base de datos, servidores.				
7. Esquema de Implantación y Adecuación.				

Describir el proceso de implantación y adecuación de la solución propuesta.				
Indicar el proceso para ajustar la solución propuesta de acuerdo con las adecuaciones o extensiones necesarias para que la solución ofrecida cumpla totalmente con los requerimientos definidos en estos términos.				
Cuál es el plan de cargue inicial y migración de datos para la operatividad de la solución indicando la participación del Banco y del proponente y qué condiciones se requieren para obtener una funcionalidad exitosa. Se espera que el porcentaje de migración del contenido actual frente a la nueva arquitectura esté entre un 30% a 40%.				
8. Capacitación que brindará a la solución ofrecida.				
Tipo de capacitación: Técnica, operación, administración y usuario.				
Contenido de cada curso.				
Grupo objetivo del curso y requisitos de grupo.				
Recursos necesarios para la capacitación u otras condiciones necesarias.				
En el capítulo de costos, detallar lo pertinente a este ítem				
9. Pruebas de la solución ofrecida. Indicar si el proceso de pruebas incluye:				
Describir el proceso que se tiene para gestión de las pruebas del Desarrollador, Técnicas y de usuario. ✓ Casos de prueba que contemplen múltiples escenarios de operación. Tener en cuenta escenarios para cargue manual y automática. ✓ Pruebas integrales orientadas a verificar la integridad de operación y de los datos después de la ejecución de diferentes funcionalidades que los comparten. ✓ Pruebas de rendimiento bajo carga ✓ Pruebas de seguridad del software contra ataques ✓ Pruebas de facilidad de uso con usuarios reales. ✓ Pruebas modulares para verificar que la solución ofrecida funciona correctamente. ✓ Pruebas de las interfaces (si se requieren). ✓ Pruebas de funcionamiento del software en el hardware seleccionado				

✓ Pruebas para verificar que el servicio ofrecido funciona como se esperaba. ✓ Pruebas de rendimiento (stress) orientada al acceso WEB.				
Indicar el procedimiento para gestión de incidentes o errores que ocurran en las pruebas y el procedimiento de atención. Cuáles son los ANS para su solución.				
Describir el proceso de aseguramiento de la calidad.				
Describir como la solución será probada en ambientes de máxima utilización simulando picos, volúmenes, números de usuarios y en general carga/sobrecarga del sistema.				
Establecer un procesos para hacer más rápidas las pruebas "Celeridad", con el fin de evitar que se impacten los tiempos estimados para pasó a PRODUCCIÓN.				
El proveedor deberá prever la realización de una prueba de vulnerabilidad antes del paso a PRODUCCIÓN.				
14. **Documentación técnica y de usuario**				
Documentación técnica y de usuario en español.				
Indicar que documentación entrega el Proponente al Banco y como la entrega (Medio). - Documentación técnica y de usuario. - Manual de instalación. - Documentación del proyecto o servicio ofrecido.				
10. **SEGURIDAD DE LA SOLUCIÓN OFRECIDA**				
• **Autenticación** • El sistema se adapta para trabajar bajo un esquema Single Sign On. • Proceso de confirmación de la identidad del usuario. Antes de que una aplicación pueda autorizar el acceso a un recurso, debe confirmar su identidad. Esta es la primera capa de control de seguridad. • Roles de usuarios: La solución debe manejar un control de acceso a las opciones del sistema por roles. Un usuario puede tener asignado uno (1) o más roles. • Bloqueo intentos fallidos: Detallar si el sistema ofrecido cuenta con control de acceso al sistema a través de ingreso de usuario y contraseña y si controla los intentos fallidos de registro.				

• Parametrización de la contraseña. Se permite parametrizar la contraseña de acuerdo con políticas internas del Banco referente a número de caracteres, combinación de caracteres. • El sistema permite configurar los criterios de creación y cambio de clave del acceso al sistema: tiempo para cambio de clave, caracteres obligatorios, etc.				
• **Autorización:** Indicar el proceso de verificación en caso que un usuario autenticado tenga permiso para obtener acceso a un recurso determinado. Siguiente capa de seguridad tras la autenticación.				
• **Protección de datos: I**ndicar el proceso consistente en proporcionar confidencialidad, integridad y no repudio a los datos.				
• **Sistema de control interno (auditorias-logs):** ✓ Indicar que logs tiene implementados la solución ofrecida. ✓ Indicar el proceso de: ▪ Registro. ▪ Consulta. Tiene implementadas consultas que permitan el acceso a estos logs. ▪ Permite la consulta de logs a través de opciones de menú u opciones de perfil administrador y se puedan imprimir o exportar a un formato de fácil lectura las consultas. ▪ Depuración. ▪ Respaldo. ✓ Genera y registra logs sobre las operaciones que un usuario realice en el sistema. ✓ Que información contiene el log. El diseño de los logs debe contener por lo menos la siguiente información: fecha, hora, segundo, comentario.				
Herramientas de seguridad: El proponente deberá contar con por los menos las siguientes herramientas de seguridad: Antivirus, antispam, firewall, software para prevenir ataques o intrusiones, entre otros.				
• **Cumplimiento.** Como cumple con: (**Anexo 15 SEGURIDAD DE LA INFORMACIÓN**) - CIR 42 - Protección de Datos Personales Ley 1581 de 2012.				

- Ley 1712 de 2014 de transparencia y del derecho de acceso a la información pública nacional. - Acuerdo Interbancario sobre Requerimientos mínimos de seguridad para los servicios transaccionales ofrecidos a entidades públicas, de noviembre 20 de 2009. - Ley de Habeas Data 1266 de 2008.				
16. **Servicio de HOSTING.**				
Indicar el proveedor del servicio de hosting, incluyendo el de la contingencia.				
Describa el esquema del servicio de hosting. Debe estar relacionado con la propuesta detallada en el ítem de arquitectura y se pide que esté en la nube.				
Especificar el esquema de seguridad que tendrá el servicio de hosting. Accesos no autorizados, ataque de negación de servicio y en general cualquier aspecto relacionado con la estabilidad y seguridad del sitio web en hosting.				
Describir el servicio de CONTINGENCIA que tendrá la solución ofrecida a nivel de aplicación y servicio de hosting. Indicar si se cuenta con servicio de Data Center alterno.				
Permite fácil crecimiento en los recursos dependiendo de lo que se requiera en algún momento crítico? Como se gestiona este crecimiento.				
Se cuenta con WAF (Web Aplication Firewall). Si se cuenta con un WAF este gestiona ataques de negación de servicio DDoS?				
Indique el tipo de FW ofrecido y describa sus características.				
Tiempo - ANS, para dar respuesta a las vulnerabilidades encontradas.				
Indicar estrategia para hardening “endurecer” el sistema operativo. Se recomienda demostrar que se acogen las buenas prácticas.				
Disponibilidad del servicio. Indicar los ANS’s, los indicadores asociados a continuidad, los cuales se esperan que estén en un porcentaje de disponibilidad del sitio WEB del 99.9%.				
Indicar cuál es el plan de Continuidad del servicio de soporte y mantenimiento para el sitio WEB y el HOSTING.				
Indicar las políticas de respaldo y recuperación del sistema: Aplicación, Datos.				
Indicar el proceso de contingencia para contar con la disponibilidad de los respaldos realizados.				

Indicar los ANS establecidos para contar con procesos de recuperación y disponibilidad de los datos y aplicación.				
Estrategia para actualizar o instalar parches: Hadware, software, redes y comunicaciones.				