GI.0901 Creación y Mantenimiento de Páginas Web

CONTROL DE CAMBIOS

PROPIEDAD DEL DOCUMENTO Y PARTICIPANTES

Nombre del documento:	**Creación y Mantenimiento de Páginas Web**		
Nombre del Fichero	**GI.0901 - Creación y Mantenimiento de Páginas Web _v1.0**		
		Fecha de creación	Firmas/Acta
Elaborado por Área de Seguridad / Dpto. Corporativo de Sistemas y Tecnología	José Ángel Cerviño, Gerente de Seguridad	19/05/2021	
	Luis Ramos, Técnico Experto en Seguridad	19/05/2021	
		Fecha de Aprobación	
Revisado por:	Subcomité de Ciberseguridad de Ilunion y Fundacion ONCE	15/01/2022	
Aprobado por:	Subcomité de Ciberseguridad de Ilunion y Fundacion ONCE	15/01/2022	

VERSIONES

Versión	Fecha	Capítulo afectado	Detalles de la versión
1.0	19/05/2021	Todo	Nueva versión

VIGENCIA

La aprobación y publicación de la versión 1.0 o posteriores de este documento expresa el respaldo de la Organización a su contenido. Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento. En cualquier caso, todas las referencias documentales, con información referente a versiones, modificaciones, etc., aparecen descritas en esta ficha de versiones.
En el caso de conflicto con otras normas o procedimientos de seguridad vigentes, será la opción más restrictiva la que prevalezca.

ÍNDICE

CONTROL DE CAMBIOS 2
1 INTRODUCCIÓN 4
1.1. Objetivo 4
1.2. Alcance 4
2 REFERENCIAS Y NORMAS PARA CONSULTA 4
3 DEFINICIONES 4
4 RESPONSABILIDADES 5
5 MÉTODO OPERATIVO 6
5.1. Normas Generales para Creación y Diseño 6
5.2. Medidas de Seguridad 7
5.3. Ubicación de la Página Web dentro de la Red Interna 11
5.4. Monitorización del Tráfico 11
5.5. Auditoría Técnica 12
5.6. Métodos de Pago Online 13
6 PROCESO DE ACTUACIÓN 13
7 REGISTRO/INVENTARIO WEBS 14
8 DIAGRAMA DE FLUJO 16
9 REVISIÓN DEL DOCUMENTO Y GESTIÓN DE EXCEPCIONES 17

1 INTRODUCCIÓN

1.1. Objetivo

El objeto de este procedimiento es definir las normas a seguir, en materia de seguridad y privacidad, para la creación y administración de las páginas web de cualquiera de las empresas del Grupo ILUNION y Fundación ONCE.

1.2. Alcance

Este documento es de aplicación a todos los empleados y colaboradores externos de las empresas del Grupo ILUNION y la Fundación ONCE, en adelante "el Grupo", que traten webs y aplicaciones web que sean responsabilidad del Grupo. Las directrices y objetivos de control definidos son de obligado cumplimiento para todo el personal del Grupo.

2 REFERENCIAS Y NORMAS PARA CONSULTA

A continuación, se listan las diferentes normas y/o estándares de referencia que se han tenido en cuenta para elaborar este documento.

Nota: Para los documentos en las que no se especifique la fecha, aplicará la última edición de este. Mientras que, para los documentos con fecha, aplicará únicamente la edición indicada.

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- GDPR

3 DEFINICIONES

DSSI: Departamento de Seguridad de Sistemas de Información.

DPD: Delegado de Protección de Datos.

LSSI: Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.

LPI: Ley de Propiedad Intelectual.

DMZ: (Demilitarized Zone) red local que se ubica entre la red interna de una organización y una red externa.

OWASP: Open Web Application Security Project (Proyecto abierto de seguridad de aplicaciones web).

PCI DSS: estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard).

CMS: (Content Management System) gestor de contenidos para páginas web.

CAPTCHA: (Completely Automated Public Turing test to tell Computers and Humans Apart) es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta.

IDS/IPS: sistema de prevención de intrusos.

WAF: (Web Aplication Firewall) es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web.

TLS: (Transport Layer Security) seguridad de la capa de transporte.

4 RESPONSABILIDADES

ÁREA	CARGO	RESPONSABILIDADES
Empresa o área responsable de la web.		Elaborar un documento de toma de requerimientos y hacer seguir las instrucciones sugeridas por el Dpto. de Seguridad, Dpto de Marketing y el DPD.
Dpto. de Seguridad Ilunion y F. O,		Revisar los requerimientos de seguridad de la web y su cumplimiento. Realizar el análisis de riesgos en colaboración con el DPD.
Dpto. de Marketing Ilunion / F. O.		Revisar y aprobar que la web cumple con los requerimientos de marcas y signos distintivos de Ilunion o F.O.
DPD Ilunion DPD F. O.		Apoyar al Dpto. de Seguridad en la elaboración del análisis de riesgos y evaluaciones de impacto, así como de cualquier

		duda sobre los requerimientos legales de la web en materia de protección de datos.

5 MÉTODO OPERATIVO

Las empresas que desean crear una web, microsite, una app, o modificar cualquiera de ellos, debe de proceder a elaborar un documento de toma de requerimientos y el presupuesto a Ilunion Tecnología y Accesibilidad o a la empresa tercera que vaya a suministrarles los servicios de diseño, desarrollo y alojamiento.

5.1. Normas Generales para Creación y Diseño

A la hora de contratar o diseñar una página web del Grupo, debemos tener en cuenta, y exigir a nuestros proveedores en su caso, los siguientes aspectos de seguridad:

- Garantías de seguridad, auditorías, sellos, etc.
- Utilizar metodologías de desarrollo seguro a la hora de construir la web, como por ejemplo la metodología OWASP.
- Garantizar un acceso seguro al panel de control del sitio web.
- Si se trata de una web de venta online tendremos que contratar medios de pago seguros y que cumplan estándares como PCI DSS.
- Se deberán de realizar copias de seguridad periódicas de todos los elementos que conforman nuestro servicio web;
- Mantener el gestor de contenidos (CMS) siempre actualizado;
- Guardar registros de la actividad generada en el servidor;
- Cumplir con la legislación marcada por el GDPR, LSSI y la LPI.
    - Incluir la política de privacidad del grupo, así como las cláusulas informativas de recogida del consentimiento aprobadas en el grupo.
    - Guardar un log del consentimiento otorgado por cada usuario que dé sus datos personales en la web.
    - Como regla general los datos recogidos en las webs no podrán salir de la Unión Europea o Espacio Económico Europeo. En el caso en que deba producirse la salida, esta contingencia deberá indicarse expresamente

al Área de Seguridad Informática y al Delegado de Protección de Datos, quienes proporcionarán el debido asesoramiento en la materia.

  - Se deberán realizar los análisis de riesgos y evaluaciones de impacto previas a la puesta en producción de una web que recoja datos de carácter personal. A tal efecto, el Dept. de Seguridad Informática, con el apoyo el DPD, procederá a realizar dichos exámenes.
- Disponer de un certificado digital que garantice la seguridad del sitio web.
- Respetar y utilizar las marcas y signos distintivos del grupo.

5.2. Medidas de Seguridad

Las medidas de seguridad a tener en cuenta a la hora de la creación de una web son las siguientes:

- **Certificado web**. Si la web contiene usuarios que hacen login en la página o pueden interactuar con ella de alguna forma (formularios, comentarios, etc.), es necesario proteger los canales por los que se transmite información mediante el cifrado de las comunicaciones, adquiriendo un certificado web de confianza.
- **Información del usuario (RGPD)**. Si la web recoge información del cliente, el RGPD [6 y 7] obliga a tomar estas medidas de seguridad:
  - No recabar más datos de los necesarios.
  - Tomar las medidas de seguridad adecuadas a los datos (autenticación, control de accesos, control de incidencias, gestión de soportes, copias de seguridad, etc).
  - Solicitar el consentimiento explícito del usuario, en un lenguaje claro y conciso, para tratar sus datos personales.
  - Contar con una política de cookies.
  - Garantizar, indicando cómo ejecutarlos en el Aviso Legal, los derechos:
    - ARCO: acceso, rectificación, cancelación y oposición;
    - Otros derechos: limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas, incluida la elaboración de perfiles.
- **Desarrollo de terceros**. Si contratamos el desarrollo de la web a un tercero, al

solicitar el desarrollo debemos incluir requisitos de seguridad como: autenticación y cifrado de credenciales, cumplimiento legal, copias de seguridad, privacidad por diseño y por defecto, y solicitar que se utilicen metodologías de desarrollo seguro.

- **Cumplimiento legal**. La página web debe cumplir, además de con el RGPD, con otra legislación vigente:
  - Si la utilizamos con fines lucrativos, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), indicando con claridad:
    - Las condiciones de contratación o las condiciones de uso
    - Lo relativo a las comunicaciones comerciales
  - Si utilizamos contenidos de terceros, la Ley de Propiedad Intelectual (LPI)
- **Alojamiento en servidor propio**. Si tenemos un servidor web para la página web en nuestras instalaciones, comprobaremos que:
  - Se encuentran en la DMZ corporativa.
  - Dispone de medidas de seguridad perimetrales: cortafuegos y sistemas de prevención y detección de intrusiones (IDS/IPS).
  - Dispone de medidas de seguridad contra malware.
  - Se han deshabilitado los servicios innecesarios (transferencia de ficheros, mantenimiento remoto, etc.);
  - El/los administradores utilizan dispositivos y canales seguros para administrar los servidores.
- **Alojamiento en servidor externo**. Si la web está alojada en un proveedor revisaremos que el contrato:
  - Incluye cláusulas de confidencialidad.
  - Estipula quién es el encargado del tratamiento de datos si fuera necesario.
  - Incluye acuerdos de nivel de servicio con responsabilidades de seguridad (copias de respaldo, actualizaciones, auditorías, etc.).
  - Establece la propiedad del código fuente.
- **Administración por terceros**. Si la web la administra un tercero, debe existir un registro de la actividad de los administradores que podamos consultar y obtener en caso de fraude o de incidentes de seguridad.

- **Configuración del CMS**. Tanto si lo administramos nosotros como si lo hace un proveedor para proteger el gestor de contenidos se deben aplicar y verificar las siguientes medidas de seguridad:
  - Deshabilitar los módulos que no se utilicen.
  - Eliminar el directorio de instalación.
  - Cambiar el nombre del usuario «admin» y el prefijo de la base de datos.
  - Utilizar CAPTCHA (accesible) en los formularios para evitar SPAM.
  - Eliminar metadatos de los documentos e imágenes.
  - Vigilar los cambios en los contenidos y los accesos al panel de control.
- **Acceso al panel de control**. Independientemente del gestor de contenidos utilizado, debemos asegurar que las claves de acceso al panel de control se generan cumpliendo los criterios de seguridad. Se debe:
  - Cambiar los nombres y las contraseñas de todos los usuarios por defecto y deshabilitarlos si no se van a utilizar;
  - Proteger al administrador (contraseñas fuertes y cambios frecuentes de contraseña, doble factor de autenticación…).
  - Utilizar comunicaciones seguras para administradores y usuarios.
- **Limitación de accesos**. Los servidores web se deben configurar (tanto en nuestras instalaciones como en las del proveedor) con un límite de accesos concurrentes para evitar ataques de denegación de servicio.
- **Usuarios por defecto**. Tendremos que eliminar o comprobar que se han eliminado los usuarios por defecto de las herramientas y software que soporta la web (servidores web, gestores de contenidos, etc.).
- **Guardado de registros**. Para poder investigar cualquier incidente relacionado con nuestra web o incluso poner los registros a disposición judicial (si se diera el caso), es necesario guardar un registro de cualquier interacción con la página. Si la gestión del servidor la lleva el técnico de la empresa será él quien guarde esos registros durante un período de tiempo conveniente. Si la gestión del servidor es externa, este aspecto deberá estar reflejado en el contrato con el proveedor, especificando el tipo de registros que se guardan, durante cuánto tiempo y la forma de acceso a dichos registros.
- **Comercio electrónico**. Si la web se utiliza para tener una tienda online se debe

elaborar y cumplir una normativa específica de seguridad para prevenir el fraude y proteger a los clientes online con las pautas indicadas en la política de comercio electrónico.

- **Sellos de confianza**. Si la web es una tienda online, es recomendable que este acreditada con un sello que garantice la seguridad del sitio. Los mejores sellos son los que auditan nuestra web periódicamente.
- **Copias de seguridad**. Tendremos que realizar copias periódicas de la web, incluida la base de datos, tanto si está alojada en un servidor propiedad de la empresa como si está en un servidor externo.
- **Auditorias**. Se deberán de realizar auditorías externas para verificar la seguridad de la web. Sobre todo en webs de comercio electrónico o con contenidos sensibles, como las que almacenan datos de carácter personal.
- **Software actualizado**. La actualización del gestor de contenidos y sus complementos, además de la actualización del software del servidor deben ser algunas de las tareas periódicas o puntuales a realizar tanto si la gestión de la página web se desarrolla en la empresa como si la realiza un tercero. Por otra parte, se considera conveniente estar suscrito a los servicios de avisos o alertas de seguridad del propio fabricante del gestor de contenidos, así como de cualquier otro software que utilicemos que nos indicará de la existencia de actualizaciones puntuales.
- **Protección frente al malware**. Instalaremos un antivirus en todos los equipos y servidores de la empresa, que sirva tanto para el correo electrónico como para la navegación web. Se deberá actualizar periódicamente o puntualmente cuando sea necesario, configurándolo y comprobando que está activo.
- **Eliminación de metadatos**. Si vamos a publicar documentos descargables como folletos, manuales u otra documentación en formatos ofimáticos, es importante que se utilice alguna herramienta para eliminar los metadatos que estos documentos guardan, ya que pueden proporcionar información a un posible atacante sobre nombres de usuarios, equipos, directorios, etc. Actualmente los principales productos de ofimática incorporan funcionalidades para realizar esta tarea.
- **Contraseñas robustas**. Independientemente del gestor, debemos asegurarnos de que las claves que dan acceso al panel de control de la página web mediante el que creamos y actualizamos los contenidos se generan cumpliendo unos criterios

mínimos de seguridad (al menos 8 caracteres y mayúsculas, minúsculas, números o símbolos). También es importante que estas contraseñas sean cambiadas regularmente. Además de las contraseñas es recomendable también modificar los nombres de los usuarios que vienen por defecto, como por ejemplo el caso de los administradores.

- **Entornos de producción y pruebas**. Si tenemos página web con una alta complejidad (páginas de comercio electrónico, con datos sensibles, etc.), si es posible, se debe de disponer de dos entornos diferenciados de producción y pruebas o preproducción. Se trata de dos entornos iguales, con los mismos contenidos y la misma configuración. Esto nos permitirá aplicar parches (en el entorno de pruebas) y comprobar el correcto funcionamiento de las nuevas modificaciones y funcionalidades antes de aplicar los cambios sobre la página web visible para los usuarios (el entorno de producción).

5.3. Ubicación de la Página Web dentro de la Red Interna

Si el alojamiento de la página web es interno, en instalaciones bajo nuestro control, debemos ubicar el servidor web en una subred aislada del resto de servidores internos de nuestra empresa (DMZ). Para esto necesitamos crear una subred accesible desde el exterior y separada de nuestra red interna mediante segmentación de red.

Desde la DMZ no se debe haber visibilidad de la red interna de nuestra organización. Es decir, si nos conectamos físicamente a un servidor alojado en la DMZ no podremos acceder a un sistema de la red interna de la empresa.

Para conseguirlo el tráfico entre la DMZ y la red interna de la empresa deberá haber un filtrado mediante cortafuegos.

5.4. Monitorización del Tráfico

Para la detección de cualquier tipo de ataque que nuestra web pueda sufrir, es una buena práctica la monitorización tanto del tráfico recibido como del tráfico generado. Si la página web la gestionamos nosotros mismos, se deberá instalar en nuestra red herramientas de detección de intrusos o IDS. Además, es muy recomendable instalar un cortafuegos de aplicación web o Web Application Firewall (WAF).

Si la página web es gestionada por un tercero, debemos incluir esta monitorización y supervisión del tráfico de red de nuestra página como parte del contrato de nivel de servicio con el proveedor.

5.5. Auditoría Técnica

Es recomendable que antes de publicar una página web se lleve a cabo un análisis técnico de seguridad o auditoría técnica, tanto de la página web como del servidor que la contiene. Esto es especialmente importante si la web no es meramente informativa, sino que va a gestionar datos de cualquier tipo.

Como parte de esta auditoría técnica, se deben llevar a cabo una serie de pruebas que incluyen, entre otras:

- **Análisis de visibilidad externa:** Se comprueban las funcionalidades accesibles desde el exterior a nivel de servidor, el gestor de contenidos usado y los complementos utilizados. Se evalúa si es necesario que dichos complementos y funcionalidades estén habilitados y si no lo es, se deshabilitan para evitar que posibles atacantes puedan aprovecharlas en su beneficio.
- **Contenido del directorio web:** Cualquier archivo o información almacenados en el directorio de nuestra web, es susceptible de ser accedido desde Internet, aunque no esté directamente enlazado desde nuestra página web. Es recomendable que el contenido del directorio donde se aloja nuestra página web, ya sea propio o de un tercero, sea revisado frecuentemente y que se evite almacenar en él cualquier información sensible.
- **Búsqueda de vulnerabilidades** propias de los entornos y lenguajes de programación utilizados para crear la página web. A la hora de realizar esta búsqueda de vulnerabilidades, se puede utilizar la metodología OWASP [1] entre otras. Entre las posibles vulnerabilidades que puede tener un portal, las más típicas son:
  - Cross-Site Scripting o XSS: La ejecución de un ataque de XSS, consiste en el envío de un código malicioso como parte de una petición aparentemente legítima. Los puntos de entrada más habituales son los formularios en línea. Una vez ejecutado el XSS, el atacante puede ser capaz de cambiar configuraciones de usuarios, secuestrar cuentas,

envenenar cookies, exponer conexiones seguras, acceder a sitios restringidos y hasta instalar publicidad en la web víctima del ataque.

- Inyección de SQL: Un ataque de inyección de SQL consiste en la ejecución de un comando malicioso de acceso o modificación de una base de datos como parte de una petición a una página web. Una deficitaria validación de los datos de entrada en la web puede permitir la realización de consultas no autorizadas a la base de datos.

Este análisis técnico es recomendable que se lleve a cabo por una empresa independiente que no haya participado en los procesos de desarrollo y gestión de nuestro sitio web.

5.6. Métodos de Pago Online

En el caso de que nuestra página web incorpore la posibilidad de vender productos, es importante seleccionar un sistema de pago adecuado para que nuestros clientes se sientan cómodos y seguros con la compra y cumplir los estándares de seguridad de pagos.

Si se utiliza, como es habitual, el pago con tarjeta, es muy recomendable que se utilice la pasarela de pago de una entidad bancaria. De este modo, no se accederá, ni se almacenarán los datos de la tarjeta, sino que dicha información será proporcionada exclusivamente al banco.

Las comunicaciones de estos terminales de punto de venta o TPV virtuales deben ir siempre cifradas (a través del protocolo TLS) e incorporan medidas de seguridad adicionales proporcionadas por el banco, como tarjeta de coordenadas o código de confirmación por SMS al móvil.

6 PROCESO DE ACTUACIÓN

Las empresas que desean crear una web, microsite, una app, o reformar cualquiera de ellos, debe de proceder a confeccionar el documento de toma de requerimientos y el presupuesto a Ilunion T y A o a la empresa tercera que vaya a suministrarles los servicios de diseño, desarrollo y hosting.

La empresa responsable deberá enviar copia del documento de toma de requerimientos al Dept. Marketing y al Área de Seguridad de Sistemas de Información, quienes revisan dichos requerimientos. Si no indica nada en el plazo de 10 días hábiles, se entiende autorizada.

Se lleva a cabo el desarrollo de la web, y antes de la puesta en producción de la misma, la web se envía a:

- Dept. Marketing Ilunion (Marketing Corporativo Ilunion marketinggi@ilunion.com).
- Dept. Marketing Fundación ONCE.
- Seguridad de Sistemas (Área de Seguridad de Sistemas de Informacion ssi@ilunion.com).
- Delegado de Protección de Datos (DPD Ilunion dpd@ilunion.com, DPD Fundación ONCE dpd@fundacionONCE.es).

Si ninguno de dichos departamentos hace ninguna advertencia, la web pasa a producción.

Por otro lado, el Área de Seguridad Informática debe registrar la web en el Inventario de webs del grupo.

7 REGISTRO/INVENTARIO WEBS

Cuando se decida subir a producción la web, deberá registrarse en el formulario de inventario al efecto, para ello la compañía deberá remitir una ficha con la siguiente información:

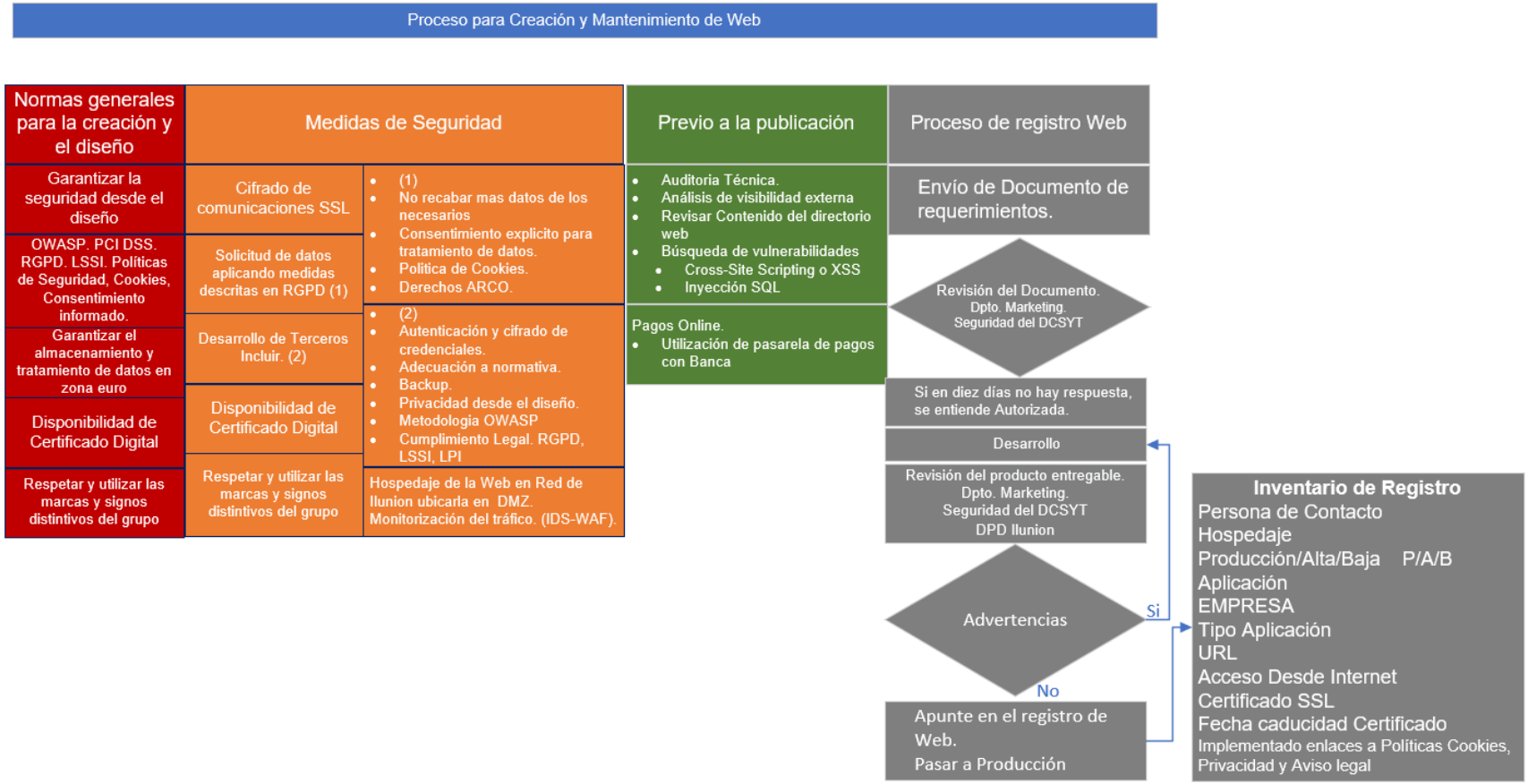
a. **Persona de Contacto.** Responsable en la compañía de la funcionalidad Web publicada.
b. **Ubicación Infraestructura**. Proveedor que ofrece el hosting.
c. **Aplicación**. Breve descripción de la función de la web que se va a publicar.
d. **Empresa**. Compañía responsable de la web a publicar.
e. **Acceso Desde Internet, URL**. Dirección web que se publica.
f. **Certificado SSL**. URL para la que se ha emitido el certificado.
g. **Certificado SSL**. Fecha de validez.

Los textos a los que hace referencia son los distribuidos por el Dpto. jurídico.

- Política de Cookies. Implementa el texto sobre cookies.
- Política de privacidad. Implementa el texto sobre privacidad.

- Aviso Legal. Implementa el texto sobre Aviso Legal.

8 DIAGRAMA DE FLUJO



9 REVISIÓN DEL DOCUMENTO Y GESTIÓN DE EXCEPCIONES

Toda la documentación del Marco Normativo se revisa y actualiza anualmente o cuando se produzcan cambios significativos. La revisión de documentación se planificará en función de su antigüedad, grado de obsolescencia, acciones correctivas en curso y observaciones recibidas.

En cualquiera de los casos la derogación de un documento se comunica al Gerente de Seguridad a efectos de que este mantenga actualizado el repositorio de documentación.

Toda excepción al presente documento es registrada e informada en el Subcomité de Ciberseguridad. Asimismo, cualquier violación del mismo puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno del Grupo. Es responsabilidad de todos los miembros de la organización notificar cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas en el presente documento.