Anexo I Requisitos de Seguridad y Nivel de Servicio

Seguridad física:

La plataforma se encuentra alojada en varios servidores subcontratados tanto en digital ocean así como en amazon AWS. De manera que delegamos la seguridad física de los servidores en ellos y trabajamos con ambos proveedores para no depender exclusivamente de uno de ellos.

Infraestructura utilizada e implicación de subcontratistas.

Tanto en el caso de digital ocean como de amazon, los nodos se encuentran tras un balanceador de carga que decide que nodo debe atender las peticiones.

Los nodos se encuentran en distintas regiones físicas para evitar problemas o cortes en el servicio por zonas geográficas, trabajando así con las regiones: Amsterdam (AM2) y Londres (LON1).

Las responsabilidades sobre el mantenimiento del hardware y software:

Es responsabilidad directa de Gooveris Software la gestión y mantenimiento del software, copias de seguridad y actualización de sistema operativo así como servicios relacionados.

Así mismo, es responsabilidad de Gooveris Software el dimensionar los nodos y recursos de los mismos de acuerdo a la carga máxima de peticiones requeridas por el servicio.

Aislamiento de software y datos de otros clientes:

El software está desarrollado de manera íntegra por Gooveris Software utilizando el framework Laravel en su versión 5.5. Es por ello que el software, se basa en Laravel y sus depencias a través de composer, así como de servicios tales como Apache, MySQL y resto de componentes de un entorno LAMP, bajo sistema operativo Unix.

Además, el software se apoya de paquetes de tereceros que pueden encontrarse como software libre en la plataforma github.

Nivel de servicio (SLA), donde se establecen aspectos como el tiempo de respuesta y disponibilidad del servicio:

Desde Gooveris Software ofrecemos distintos tipos de nivel de servicio (SLA multinivel):

- Soporte estándar:
  - 12x6 L-S: 8h – 20h
    - Soporte telefónico

        - Soporte email
- Soporte Premium:
    - 24x7 sin tiempo de interrupción
        - Soporte presencial
        - Soporte telefónico
    - Sporte email

Política de copias de seguridad:

Cada uno de los nodos así como nodos locales que utilizamos para desarrollo, se encargan de realizar automáticamente una copia incremental diaria y completa cada 3 días, sincronizándolas además con nuestros servidores locales.

Las copias con más de 90 días de antigüedad se eliminan automáticamente.

Política de recuperación completa y el tiempo que podría tardar:

La restauración de servicio por completo no sólo de una APP sino del entorno al completo no llevaría más de 120 minutos para su restauración desde cero.

Monitorización de registros de auditoría:

Contamos con herramientas de tereceros para el registro de información en logs de diverso tipo. Desde logs técnicos tales como los propios de Laravel, Apache o sistema operativo así como logs desarrollados para la plataforma como historial de acciones sobre la plataforma, acciones sobre APPs, historial de acciones por usuario o logs durante el proceso de backup.

Proporcionar informes periódicos del servicio y registros sobre los problemas relacionados con la provisión del mismo:

En este sentido, enviamos distintos tipos de informes del servicio a los clientes:

1. Informe de funcionalidades: Donde describimos las nuevas mejoras y funciones añadidas recientemente a la plataforma. Es de carácter mensual.
2. Informe de sistemas: Informe de intervención, errores y actuaciones sobre los sistemas, a pesar de no tener impacto directo sobre el servicio.

Gestión de riesgos, de cambios e incidentes de seguridad de la información:

- Análisis: Realizamos el seguimiento de logs del sistema, componentes software y logs de la propia plataforma para la protección, detección de vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- Clasificación: En función de los tipos de riesgos, estos son clasificados como bugs, ataques o fallos de terceros, tomando distintas medidas en función de dicha clasificación.
- Reducción: De nuevo dependiendo de la clasificación, distinguimos distintas medidas de reducción del riesgo: En el caso de ataque o amenza por debilidad de software, pasará por actualizar y parchear el sistema o versión del componente software. En caso de tratarse de un bug o error en el software, se desplegará un nuevo commit para su resolución.
- Control: Durante todo el proceso, tomamos indicadores del funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Desarrollo de software seguro:

Desarrollamos el software bajo políticas de buenas prácticas así como la implementación de patrones de diseño enfocados al desarrollo seguro.

El hecho de utilizar un framework como Laravel ya lleva implícitas una serie de abstracciones y seguridad implementadas, tales como la validación de todos los datos, sanetización, control de ataques de pila, estructura y organización de la lógica de negocio y ficheros públicos, paradigma MVC, etc.

Entornos de desarrollo y producción diferenciados:

Como hemos comentado, nuestros sistemas en producción se encuentran distribuidos y balanceados entre digital ocean.

De manera paralela, contamos con servidores en entorno local que utilizamos tanto para copias de seguridad de los sistemas de producción como para el desarrollo local. Este entorno local es una copia exacta de los entornos de producción y se reparte en 2 servidores físicos ejecutando sistemas Unix con exactamente las mismas versiones y componentes software que los sistemas en producción.

Este entorno de desarrollo tan sólo es accesible desde la intranet de gooveris software. El desarrollo del software se realiza desde el puesto de trabajo de cada trabajador, utilizando sistemas MAC OS X y se sincronizan y testean en los servidores locales.

Protección contra malware e intrusiones:

En nuestros entornos de producción, evitamos intrusiones en el mismo utilizando tanto control de IP a través del firewall del sistema así como una autenticación por

clave pública y privada SSH , de manera que cualquier otro intento de conexión sea rechazada.
Por parte de malware, tan sólo confiamos en la instalación de paquetes de fuentes fiables de nuestra distribución Linux, evitando instalar cualquier software de orígenes desconocidos.
El utilizar sistemas UNIX nos garantiza en mayor medida aún la protección del sistema de cara a software de terceros que no cuentan con permisos como super-usuario.

Parcheado y corrección de vulnerabilidades:

Tanto sistema operativo como componentes software (servidor gestor de base de datos, servidor web, servicios ssh, git, lenguajes de programación y plugins) se mantienen actualizados y al día tras la revisión de compatibilidad necesaria para la plataforma.

Seguridad del código fuente y los archivos del sistema:

Para el control de nuestro código fuente, utilizamos el sistema de control de versiones GIT, trabajando además en distintas ramas según el versionado interno y alineado a nuestro roadmap.

La plataforma sigue la misma estructura de código recomendada por Laravel, separando toda la lógica de negocio de la parte pública del proyecto, que es la única ruta a la que puede acceder el servidor web, garantizando aún más la seguridad a través de posibles ataques a través de versiones obsoletas del servidor web.

Seguridad de las interfaces:

Para el acceso web desde la plataforma web, utilizamos captcha a través del servicio de Google para formularios de uso público, prescindiendo del mismo desde el panel una vez el usuario está autenticado.

Para el usuario final, a consumir los servicios de APPs nativas, prescindimos de captcha y simplemente desplegamos teclados virtuales propios del sistema operativo en uso.

Seguridad de los servicios de comercio electrónico:

En los módulos y funcionalidades de compra (tienda virtual, entradas, etc), delegamos el proceso de compra a TPV externo quien se encarga de la recogida de datos bancarios y proceso de cobro. En ningún caso almacenamos este tipo de información.

Una vez procesada la compra se devuelve el control del usuario a la APP.

Gestión de usuarios y contraseñas:

La gestión de usuarios y contraseñas se realiza por la propia plataforma, permitiéndose habilitar o no el registro público de usuarios de los mismos u obligando en otro caso a solicitar la cuenta de usuario.

Las cuentas de usuario se identifican por email válido que debe ser confirmado para la activación del usuario.

Del mismo modo, proporcionamos mecanismos de recuperación de credenciales mediante la introducción del email del usuario y a través de un sistema de tokens con una validez de tiempo máxima de 1 hora.

Los usuarios pueden crearse bien desde la propia plataforma o a través de servicios web, permitiendo integrar software de terceros con la plataforma y sincronizar tanto altas, bajas como cambio de credenciales de los mismos.

Autenticación y control de acceso:

La autenticación se puede realizar mediante usuario (email) y clave directamente contra la propia plataforma.

En cuanto a control de acceso, las cuentas pueden ser administradoras de las APPs o cuentas colaborativas con distintos permisos en la gestión de la APP. Además, el administrador puede decidir si las cuentas continúan activas o dejan de tener acceso a la plataforma, así como gestionar sus datos, credenciales de acceso, etc.

Protección de datos mediante el cifrado de los mismos:

Para todos los usuarios, sus contraseñas se almacenan de forma cifrada; no se almacena ningún tipo de dato bancario o pago de los usuarios y el resto de datos se guardan de forma legible en las bases de datos del sistema.

Custodia, recuperación y destrucción de los datos:

El sistema permite por defecto la exportación a formato Excel y csv de la información almacenada por la APP (pacientes, citas, leads, contactos, usuarios, acreditaciones, informes, etc)

Protección de datos de carácter personal (LOPD) y cumplimiento de la ley de servicios de la sociedad de la información y comercio electrónico (LSSI-CE):

Nuestra empresa está inscrita en el El Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

En cada formulario o punto de recogida de información así como en las condiciones de uso de cada APP, se informa al usuario del uso del tratamiento de la información mediante el siguiente epígrafe:

* En cumplimiento de lo previsto por el artículo 5 de la LOPD, se informa que los datos de carácter personal que se recaban directamente del usuario a través de esta APP, serán tratados de forma confidencial y quedarán incorporados a los respectivos ficheros de los que es responsable la AEPD, con las finalidades que se detallan en el Registro General de Protección de Datos no siendo utilizados para finalidades incompatibles con estas.

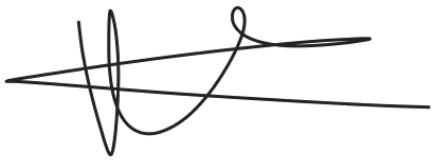
Por otro lado, siguiendo la certificación de APP saludable, en cada contenido médico así como en las condiciones de uso, se indica que tan sólo se tratan de informaciones y recomendaciones de carácter general que en ningún caso sustituyen o prevalecen sobre la información proporcionada por el ginecólogo o clínica respectivo.

Firma de un contrato de confidencialidad y/o de acceso a datos por cuenta de terceros si se tratan datos personales:

Facilitamos una copia de nuestro contrato tipo con el cliente, donde se definen alcances, responsabilidades, confidencialidad y permisos explícitos. Adjuntamos dicho documento anexo.

Gooveris
Software Solutions

CIF B56077100
GOOVERIS SOFTWARE SL
info@gooveris.com | www.gooveris.com



D. Víctor Téllez Lozano

DNI: 30978062Y
CEO Gooveris Software