UCR
UNIVERSIDAD DE COSTA RICA

TCU-652 Migrantes como Sujetos Políticos

Análisis de Seguridad Observatorio de Migración

Autores: Andrey Elizondo, Stephanie Leitón

Tabla de contenido

1. Identificación componentes de la app

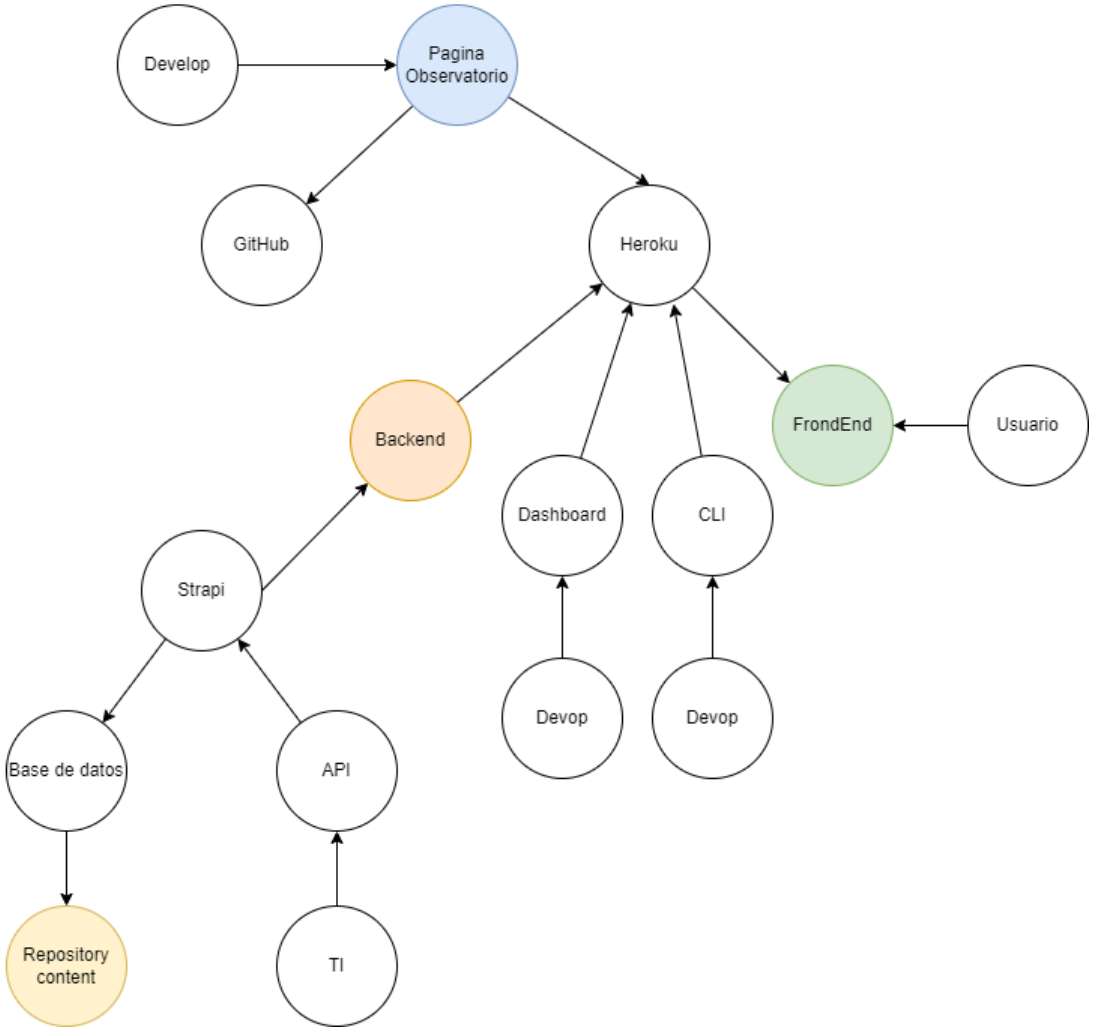
1.1. Componentes

- **Página Observatorio de Migración:** El Observatorio de Migración es un proyecto que trata de ayudar a las personas migrantes en la búsqueda de soluciones al gran reto que es la incorporación social y gubernamental al país, ya sea en el mercado laboral, la inclusión social y el trato igualitario entre hombres y mujeres. Por medio de talleres, charlas y post informativos. El Observatorio espera ser un centro de ayuda accesible y gratuito para las personas migrantes.
- **GitHub:** Git es un software de control de versiones distribuido. El control de versiones es una forma de guardar los cambios a lo largo del tiempo sin sobrescribir las versiones anteriores. Ser distribuido significa que cada desarrollador que trabaja con un repositorio de Git tiene una copia de ese repositorio completo: cada confirmación, cada rama, cada archivo. (GitHub, n.d.)
- **Heroku:** Un servicio de plataforma (PaaS) en la nube donde los desarrolladores no se tienen que preocupar por la infraestructura, sino que solamente se hay que centrar en el desarrollo del código de la aplicación. (Romero, n.d.) En Heroku el código corre siempre dentro de un dyno que es el que proporciona a la plataforma la capacidad de cómputo, es un proceso que puede usarse para ejecutar contenido web, para ejecutar procesos batch. Es necesario contratar un servicio de base de datos externa y un hosting. (Heroku, n.d.)
- **Frontend:** El front-end es una combinación de dos elementos diferentes: el diseño gráfico (la apariencia) y la interfaz de usuario (la sensación) . Cada uno de estos se crea de forma independiente, y la mayor parte del trabajo técnico se realiza en la interfaz de usuario utilizando lenguajes web como HTML, CSS y JavaScript. (Airfocus, n.d.)
- **Backend:** El back-end de un sitio web es todo lo que el usuario no ve, es quien responde a las solicitudes realizadas por el usuario mediante el envío de información desde el back-end al front-end para que se muestre.
    - El back-end de un sitio web comprende cosas como servidores, bases de datos, sistemas operativos, API y más, todos los cuales se unen para garantizar que el

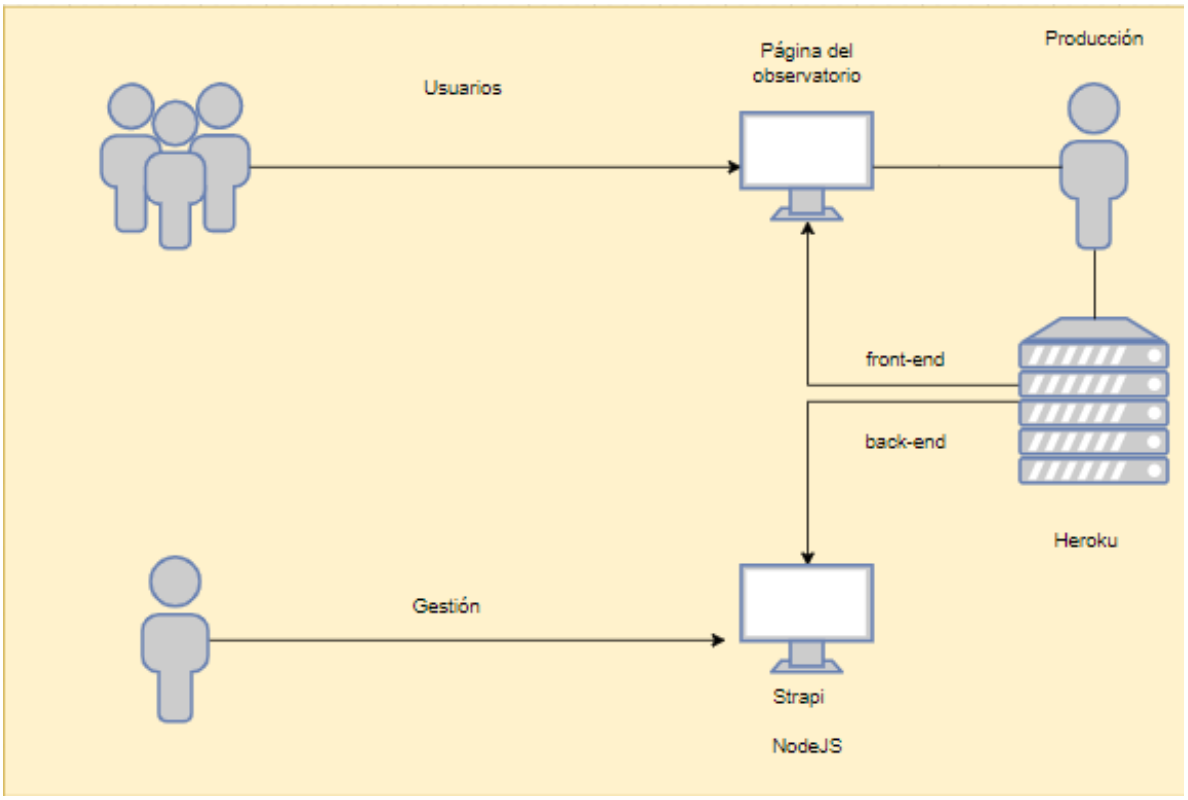
usuario reciba la información correcta lo más rápido posible. (Airfocus, n.d.)

- **Strapi:** Strapi es un CMS Headless de código abierto basado en Node.js que ahorra a los desarrolladores mucho tiempo de desarrollo y les da la libertad de usar sus herramientas y marcos favoritos. Strapi también permite a los editores de contenido optimizar la entrega de contenido (texto, imágenes, video, etc.) en cualquier dispositivo. (Strapi, n.d.)
- **API:** Una API, o interfaz de programación de aplicaciones, permite la interacción entre aplicaciones de software, sistemas o plataformas para enviar y recibir datos. Una API es el mensajero que entrega su solicitud de datos a una fuente externa y luego le devuelve su respuesta. (Airfocus, n.d.)
- **Usuarios**
    - Cliente
    - Tecnologías de la información
    - Desarrollo de software
    - Desarrollo Operativo
    - Publicación

1.2. Árbol del todo y las partes del sistema



2. Diagramas de interacción de los componentes



Los usuarios interaccionan con la página web.

Dentro del equipo de producción están los desarrolladores del código, los que realizan las pruebas de código, los encargados del diseño y los encargados de publicar la página en la plataforma del servicio, en este caso es Heroku.

Dentro del equipo de gestión están los encargados de tecnologías de la información, como por ejemplo seguridad, base de datos, arquitectura, entre otros. También se encuentran los encargados de publicar la información de los eventos, directorios de contactos y publicaciones mediante el administrador de la base de datos Strapi.

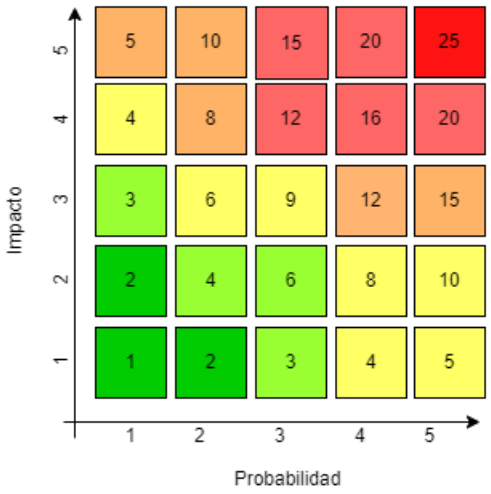
3. Definir objetivos de seguridad

1. Requerir autenticación para el ingreso a la base de datos del servicio.
2. Requerir autenticación para el ingreso a la plataforma de servicio.
3. Mantener una disponibilidad para el ingreso al servicio web por parte de los usuarios.
4. Mantener una disponibilidad para la administración del servicio web para el equipo de DevOps.
5. Mantener una disponibilidad para la administración de la base de datos para el equipo de TI.
6. Mantener la integridad de la información almacenada en la base de datos.
7. Mantener la integridad de la aplicación cargada en la plataforma del servicio.
8. Mantener confidencialidad en la información sobre controles de acceso a los servicios.
9. Mantener responsablemente la documentación para el funcionamiento de los servicios.
10. Requerir autorización para los accesos de la administración de la base de datos.

4. Definir políticas de seguridad

1. Utilizar autenticación para el ingreso a la base de datos del servicio.
2. Utilizar autenticación para el ingreso a la plataforma de servicio.
3. Implementar mecanismos para proporcionar una alta disponibilidad en el servicio web.
4. Definir una estrategia oportuna para proporcionar una alta disponibilidad en el servicio web.
5. Implementar mecanismos para mantener la disponibilidad para la administración del servicio web para el equipo de DevOp y desarrollo.
6. Implementar mecanismos para mantener la disponibilidad para la administración de la base de datos para el equipo de TI.
7. Definir estrategias de recuperación y respaldo para mantener la integridad de la información almacenada en la base de datos.
8. Realizar pruebas para verificar la integridad de la aplicación para cargarla en la plataforma del servicio.
9. Utilizar un mecanismo que permita mantener la confidencialidad de la información de los controles de acceso.
10. Definir una estrategia para mantener la confidencialidad de la información de los controles de acceso.
11. Definir pautas para que haya un desarrollo responsable de la documentación para el funcionamiento de los servicios.
12. Definir roles y permisos para los accesos de la base de datos.

5. Criterios para la evaluación y tratamiento los riesgo



Impacto	Descripción Impacto
1	Las perdidas de confidencialidad, disponibilidad o integridad no afectan la funcionalidad de los servicios.
2	Las perdidas de confidencialidad, disponibilidad o integridad afectan levemente los servicios , poco se percibe en el servicio.
3	Son perdidas de confidencialidad, disponibilidad o integridad bajas y por corto tiempo, el funcionamiento del servicio.
4	Son perdidas considerables de confidencialidad, disponibilidad o integridad en la estructura e información del servicio.
5	Son perdidas importantes e inmediatas de confidencialidad, disponibilidad o integridad de servicio operativo, obligaciones y prestigio

Probabilidad	Descripción Probabilidad
1	Lo controles existentes son seguros y brindan el nivel adecuado de protección. No se esperan incidentes de este tipo en el futuro.
2	Lo controles existentes son seguros y brindan el nivel adecuado de protección. Son muy poco probables los incidentes de este tipo en el futuro.
3	Los controles ofrecen un moderado nivel de seguridad y generalmente dan una adecuada protección. Si hay pero ocurren pocos incidentes
4	Los controles actuales son bajos o no muy efectivos. Si suceden pero ocasionalmente.
5	Los controles actuales muy pocos o ineficaces ante los incidente. Si suceden muy seguido.

Riesgo	Valoración	Aceptado
Bajo	Riesgos que son muy poco probables y de impacto muy bajo, no afectan la funcionalidad del servicio	Si
Medio-Bajo	Riesgos que son poco probables que pueden pasar, pero afectan muy poco la funcionalidad del servicio.	Si
Medio	Riesgos probables que aunque si su impacto es considerable, son remedables fácilmente	No
Medio-Alto	Riesgos probables y de alto impacto pero que su prevención es más compleja que su solución.	No
Alto	Riesgos casi críticos del servicio que son complejos.	No
Muy-Alto	Riesgo críticos, con impacto alto que provoquen graves daños en el servicio y que hacer grandes cambios para resolver o remover	No

6. Definición y evaluación de riesgos

Con la información del punto anterior, se hace una identificación de riesgos de los elementos seleccionados y tomando como referencia los objetivos establecidos.

Objetivo 1: Requerir autenticación para el ingreso a la base de datos del servicio.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Base de datos (strapi)	● Nulo mecanismo de autenticación. ● Débil mecanismo de autenticación ● Que no se limite la cantidad de intentos. ● Débil o nulo mecanismo de recuperación. ● Débil o nulo mecanismo de guardado de contraseñas anteriores.	- Que alguien malintencionado descifre el mecanismo de autenticación. - Que alguien malintencionado cambie fácilmente los mecanismos de autenticación.	- Que alguien malintencionado descifre el mecanismo de autenticación de la base de datos y borre o modifique los datos de la base de datos. Nivel de impacto: 5 Probabilidad: 1 - Que alguien malintencionado descifre el mecanismo de autenticación y cambie los mecanismos de ingreso e impida el acceso a la base de datos. Nivel de impacto: 5 Probabilidad: 1 - Que alguien malintencionado descifre el mecanismo de autenticación y cambie el mecanismo de recuperación e impida el ingreso a la base de datos. Nivel de impacto: 5 Probabilidad: 1

Objetivo 2: Requerir autenticación para el ingreso a la plataforma de servicio			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Plataforma del servicio (heroku)	● Nulo mecanismo de autenticación. ● Débil mecanismo de autenticación ● Que no se limite la cantidad de intentos. ● Débil o nulo mecanismo de recuperación.	- Que alguien malintencionado descifre el mecanismo de autenticación. - Que alguien malintencionado cambie fácilmente los mecanismos de autenticación.	- Que alguien malintencionado descifre el mecanismo de autenticación y borre o modifique los datos de la plataforma de servicio. Nivel de impacto: 5 Probabilidad: 1 - Que alguien malintencionado descifre el mecanismo de autenticación y cambie los mecanismos de ingreso e impida el acceso a la

	● Débil o nulo mecanismo de guardado de contraseñas anteriores.		plataforma de servicio. Nivel de impacto: 5 Probabilidad: 1 - Que alguien malintencionado descifre el mecanismo de autenticación y cambie el mecanismo de recuperación e impida el ingreso a la plataforma del servicio. Nivel de impacto: 5 Probabilidad: 1

Objetivo 3: Implementar mecanismos para proporcionar una alta disponibilidad en el servicio web.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Servidor web (heroku)	● Que el servidor no tenga un respaldo ante una eventualidad. ● Que no se tenga un WAF (web application firewall) Para controlar - límite de solicitudes - IP en listas negras - entre otros ● Ejecución de código remoto	- Que alguien malintencionado sature el servidor con muchas solicitudes - Que alguien malintencionado ataque el servidor. - Que se produzca y una falla en el servidor	- Que alguien malintencionado sature el servidor con muchas solicitudes y se caiga el servidor web. Nivel de impacto: 4 Probabilidad: 1 - Que ante una falla en el servidor no haya respaldo y se pierda la información. Nivel de impacto: 5 Probabilidad: 2 - Que no se pueda detectar o impedir un ataque y que se caiga el servidor. Nivel de impacto: 4 Probabilidad: 1
Aplicación web	● Input no sanitizados ● SQL Injection ● XXS ● Buffer overflow	- Que alguien malintencionado ataque la aplicación.	- Que alguien haga un ataque a la aplicación web, el servidor web se caiga y no se pueda acceder. Nivel de impacto: 3 Probabilidad: 2 - Que alguien haga un ataque a la aplicación web y que se modifique la información o la presentación de la página. Nivel de impacto: 4 Probabilidad: 2

Objetivo 4: Mantener una disponibilidad para la administración del servicio web para el equipo de DevOps y desarrollo.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Servidor web (heroku)	● Que si hay una falla no se pueda acceder a la administración	- Que alguien malintencionado ataque el servidor. - Que haya una falla en el servidor.	- Que alguien malintencionado ataque al servidor web y no se pueda ingresar a administrar. Nivel de impacto: 3 Probabilidad: 1 - Que haya una falla en el servidor web y no se pueda ingresar a administrar. Nivel de impacto: 3 Probabilidad: 1

Objetivo 5: Mantener una disponibilidad para la administración de la base de datos para el equipo de TI.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Administrador de Base de datos (strapi)	● Que si hay una falla no se pueda acceder a la administración	- Que alguien malintencionado ataque en la administración de la DB. - Que haya una falla en la administración de la BD.	- Que alguien malintencionado ataque al servidor de la base de datos y no se pueda ingresar a administrar. Nivel de impacto: 3 Probabilidad: 1 - Que haya una falla en el servidor de base de datos y no se pueda ingresar a administrar. Nivel de impacto: 3 Probabilidad: 1

Objetivo 6: Mantener la integridad de la información almacenada en la base de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Base de datos (strapi)	● Fallas a la hora de guardar la información. ● No tener respaldo de la información. ● Que se corrompa la información almacenada.	- Que alguien malintencionado acceda a la información - Que haya un fallo en el servidor de la base de datos - Que se corrompan archivos	- Que alguien malintencionado acceda a la información e ingrese código malicioso en la base de datos, altere la información y no haya un respaldo o no sea el óptimo. Nivel de impacto: 5 Probabilidad: 1 - Que haya un fallo en el servidor de la base de datos

	● Que no cuente con mecanismos para evitar inyección de código. ● Errores al cargar la información. ● Que no haya sincronización con el respaldo.		y no haya respaldo de la información o no sea óptimo. Nivel de impacto: 5 Probabilidad: 1 - Que se corrompan archivos de la base de datos y no haya respaldo en la información o no sea óptimo. Nivel de impacto: 5 Probabilidad: 1

Objetivo 7: Mantener la integridad de la aplicación cargada en la plataforma del servicio.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Aplicación web (Observatorio)	● Fallo en de despliegue de aplicación ● Aparición de errores en la ejecución ● Que no haya un buen respaldo	- Que alguien malintencionado altere los repositorios de código de la aplicación - Que se corrompan archivos - Que no se haya probado la aplicación	- Que alguien malintencionado altere los repositorios de código de la aplicación y se pierda la integridad. Nivel de impacto: 2 Probabilidad: 1 - Que se corrompan archivos los repositorios de código de la aplicación por algún fallo y la versión no esté estable. Nivel de impacto: 5 Probabilidad: 1 - Que no se haya probado la aplicación lo suficiente y aparecen errores en la ejecución. Nivel de impacto: 4 Probabilidad: 3
Plataforma del servicio y la base de datos.	● No actualizar la aplicación y tener vulnerabilidades de seguridad.	- Que alguien malintencionado encuentre las vulnerabilidades sin parchear.	- Que la plataforma del servicio y/o la base de datos estén desactualizados y con parches que puedan ser aprovechados por alguien malintencionado. - Nivel de impacto: 5 - Probabilidad: 3

Objetivo 8: Mantener confidencialidad en la información sobre controles de acceso a los servicios.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**

Información para el acceso	● Que la información de acceso no tenga un acceso restringido	- Que alguien malintencionado tenga los accesos	- Que alguien malintencionado modifique los accesos a los servicios del proyecto. Nivel de impacto: 5 Probabilidad: 1
Información almacenada en los repositorios	● Que la información de almacenada no tenga un acceso restringido	- Que alguien malintencionado tenga a acceso a la información de los repositorios	- Que alguien malintencionado pueda alterar los repositorios de información del proyecto. Nivel de impacto: 5 Probabilidad: 1 - Que alguien malintencionado elimine información de los repositorios del proyecto. Nivel de impacto: 5 Probabilidad: 1 - Que alguien malintencionado agregue información de los repositorios del proyecto. Nivel de impacto: 5 Probabilidad: 1
Información transmitida de la página a un usuario.	● Que la información de la página sea legible en texto plano mientras está siendo transmitida	- Que alguien malintencionado pueda cambiar la información que de la página mientras está siendo transmitida - Que alguien malintencionado vea la información de la página que mientras está siendo transmitida	- Que alguien malintencionado espie la información de la página que está transmitida. Nivel de impacto: 1 Probabilidad: 1 - Que alguien malintencionado cambie la información de la página mientras está siendo transmitida. Nivel de impacto: 1 Probabilidad: 1

Objetivo 9: Mantener responsablemente la documentación para el funcionamiento de los servicios.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Documentación	● Que la documentación no esté actualizada. ● Que la documentación sea nula, escasa. ● Que la documentación	- Que el equipo no comprenda la documentación - Que se den problemas en los servicios	- Que la documentación sea nula, escasa haría que el equipo no comprenda y el desarrollo de la aplicación sea más lento y complejo. Nivel de impacto: 1 Probabilidad: 4 - Que la documentación

	sea errónea.		no esté actualizada haría que el equipo no comprenda y el desarrollo de la aplicación sea más lento y complejo. Nivel de impacto: 1 Probabilidad: 4 - Si el equipo no comprende el funcionamiento y la documentación es nula, esto haría que no se puedan operar los servicios, hasta que se logre comprender. Nivel de impacto: 2 Probabilidad: 2 - Si la documentación es errónea, se dan problemas en los servicios, y resolverlos tomaría tiempo de desarrollo. Nivel de impacto: 1 Probabilidad: 4

Objetivo 10: Requerir autorización para los accesos de la administración de la base de datos.			
Componente	**Vulnerabilidades**	**Amenazas**	**Riesgos**
Accesos de la administración de la base de datos (Strapi)	● Que no existan roles para poder alterar la información de las bases de datos ● Que se pueda alterar los permisos de autorización de acceso	- Que alguien malintencionado tenga permiso para cambiar la base de datos - Que una cuenta tenga acceso a funciones que no les corresponden - Que alguien malintencionado tenga permiso para cambiar permiso	- Que una persona de forma malintencionada altere los permisos propios de los demás accesos de administración Nivel de impacto: 2 Probabilidad: 2 - Que una persona de forma malintencionada cree, modifique o elimine datos a los cuales no debería tener permiso acceder. Nivel de impacto: 1 Probabilidad: 2 - Que una persona accidentalmente modifique datos que no le corresponden cambiar. Nivel de impacto: 1 Probabilidad: 1 - Que una persona

			accidentalmente modifique permisos que no le corresponden cambiar. Nivel de impacto: 2 Probabilidad: 1

7. Análisis y tratamiento de los riesgos

Esta sección de la seguridad, posterior a la identificación del elemento analizado y los objetivos de seguridad, presenta los riesgos identificados y el análisis de seguridad con base en los riesgos donde se describen las políticas y controles a implementar.

Obj	Riesgo	Impacto	Proba	Nivel de Riesgo	Herramienta de control
1	Que alguien malintencionado descifre el mecanismo de autenticación de la base de datos y borre o modifique los datos de la base de datos.	5	1	Medio-Alto	Hardening de las credenciales de acceso a la base de datos
	Que alguien malintencionado descifre el mecanismo de autenticación y cambie los mecanismos de ingreso e impida el acceso a la base de datos	5	1	Medio-Alto	
	Que alguien malintencionado descifre el mecanismo de autenticación y cambie el mecanismo de recuperación e impida el ingreso a la base de datos.	5	1	Medio-Alto	
2	Que alguien malintencionado descifre el mecanismo de autenticación y borre o modifique los datos de la plataforma de servicio.	5	1	Medio-Alto	Hardening de las credenciales de acceso a la plataforma del servicio
	Que alguien malintencionado descifre el mecanismo de autenticación y cambie los mecanismos de ingreso e impida el acceso a la plataforma de servicio.	5	1	Medio-Alto	
	Que alguien malintencionado descifre el mecanismo de autenticación y cambie el	5	1	Medio-Alto	

	mecanismo de recuperación e impida el ingreso a la plataforma del servicio.				
3	Que alguien malintencionado sature el servidor con muchas solicitudes y se caiga el servidor web.	4	1	Medio	Actualmente este caso es responsabilidad de heroku Se recomienda tener un WAF (Web application firewall), filtrado de paquetes y limitar un máximo de las solicitudes al servidor.
	Que ante una falla en el servidor web no haya respaldo y se pierda la información.	2	5	Medio-Alto	Realizar respaldo.
	Que no se pueda detectar o impedir un ataque y que se caiga el servidor web.	4	1	Medio	Actualmente este caso es responsabilidad de heroku
	Que alguien haga un ataque a la aplicación web, el servidor web se caiga y no se pueda acceder.	3	2	Medio	Tener un respaldo. Sanitizar entradas de datos de la aplicación web.
	Que alguien haga un ataque a la aplicación web y que se modifique la información o la presentación de la página.	4	2	Medio-Alto	
4	Que alguien malintencionado ataque al servidor web y no se pueda ingresar a administrar.	3	1	Medio-Bajo	Riesgo aceptado
	Que haya una falla en el servidor web y no se pueda ingresar a administrar.	3	1	Medio-Bajo	
5	Que alguien malintencionado ataque al servidor de la base de datos y no se pueda ingresar a administrar.	3	1	Medio-Bajo	
	Que haya una falla en el servidor de base de datos y no se pueda ingresar a administrar.	3	1	Medio-Bajo	
6	Que alguien malintencionado acceda a la información e ingrese código malicioso en la base de datos, altere la información y no haya un respaldo o no sea el óptimo.	5	1	Medio-Alto	Tener respaldo.

	Que haya un fallo en el servidor de la base de datos y no haya respaldo de la información o no sea óptimo.	5	1	Medio-Alto	
	Que se corrompan archivos de la base de datos y no haya respaldo en la información o no sea óptimo.	5	1	Medio-Alto	
7	Que alguien malintencionado altere los repositorios de código de la aplicación y se pierda la integridad.	2	1	Bajo	Riesgo aceptado.
	Que se corrompan archivos los repositorios de código de la aplicación por algún fallo y la versión no esté estable.	5	1	Medio-Alto	Actualizar periódicamente las versiones de la página. Tener los respaldos actualizados y estables.
	Que la plataforma del servicio y/o la base de datos están desactualizados y con parches que puedan ser aprovechados por alguien malintencionado.	5	3	Medio	Tener actualizados la plataforma del servicio de la página y la base de datos.
	Que no se haya probado el código de la aplicación lo suficiente y aparecen errores en la ejecución.	4	3	Alto	Realizar un testing exhaustivo de la aplicación. Tener los respaldos actualizados y estables.
8	Que alguien malintencionado modifique los accesos a los servicios del proyecto.	5	1	Medio-Alto	Hardening de las credenciales de acceso a los servicios del proyecto. Cambiar las credenciales de acceso cada cierto tiempo a los servicios del proyecto.
	Que alguien malintencionado pueda alterar los repositorios de información del proyecto	5	1	Medio-Alto	Respaldos de la información del proyecto. Hardening de las credenciales de acceso a los servicios del proyecto. Cambiar las credenciales de acceso cada cierto tiempo a los servicios del proyecto.
	Que alguien malintencionado elimine información de los repositorios del proyecto.	5	1	Medio-Alto	
	Que alguien malintencionado agregue información de los repositorios del proyecto.	5	1	Medio-Alto	
	Que alguien malintencionado espie la información de la página que está transmitida.	1	1	Bajo	Riesgo aceptado.

	Que alguien malintencionado cambie la información de la página mientras está siendo transmitida.	1	1	Bajo	
9	Que la documentación sea nula o escasa haría que el equipo no comprenda y el desarrollo de la aplicación sea más lento y complejo.	4	1	Medio	Realizar y mantener la documentación actualizada.
	Que la documentación no esté actualizada haría que el equipo no comprenda y el desarrollo de la aplicación sea más lento y complejo.	4	1	Medio	
	Si el equipo no comprende el funcionamiento y la documentación es nula, esto haría que no se puedan operar los servicios, hasta que se logre comprender.	2	2	Medio-Bajo	Riesgo aceptado.
	Si la documentación es errónea, se dan problemas en los servicios, y resolverlos tomaría tiempo de desarrollo.	4	1	Medio	Mantener la documentación actualizada a lo implementado en el proyecto.
10	Que una persona de forma malintencionada altere los permisos propios de los demás accesos de administración	2	2	Medio-Bajo	Riesgo aceptado.
	Que una persona de forma malintencionada cree, modifique o elimine datos a los cuales no debería tener permiso acceder.	2	1	Bajo	
	Que una persona accidentalmente modifique datos que no le corresponden cambiar.	1	1	Bajo	
	Que una persona accidentalmente modifique permisos que no le corresponden cambiar.	1	2	Bajo	

8. Controles de seguridad

1. Hardening de las credenciales de acceso a la plataforma del servicio.
    - Heroku.
2. Hardening de las credenciales de acceso a la base de datos.
    - Strapi.
3. Hardening de las credenciales de acceso a los servicios del proyecto.
    - GitHub : respaldos del código.
    - Google Drive : para respaldos de información y documentación.
    - Gestor de contraseñas : para tener guardadas las contraseñas.
4. Cambiar las credenciales de acceso cada cierto tiempo a los servicios del proyecto.
    - Actualizarlas cada vez que se cambia el equipo de informática del TCU.
5. Sanitizar entradas de datos de la aplicación web.
    - Revisar que no se puedan hacer inyecciones de código en las entradas de datos de la aplicación. (inputs, URL, …)
6. Actualizar periódicamente las versiones de la página.

- Cada vez que se cumplan ciertos criterios, se debería hacer una actualización de la página de desarrollo y del respaldo.

7. Tener actualizados la plataforma del servicio de la página y la base de datos.
    - Actualizar Heroku, Strapi, Angular para que se puedan tener los parches de seguridad definidos por los desarrolladores.
8. Respaldos de la información del proyecto.
    - Respaldo de las contraseñas.
9. Tener mecanismos de recuperación eficaces y válidos. Realizar respaldo de la información de la base de datos.
10. Realizar un respaldo del código de la página web.
11. Tener los respaldos actualizados y estables de la base de datos.
12. Tener los respaldos actualizados y estables de la página web.
13. Realizar un testing exhaustivo de la página.
    - Realizar un testing exhaustivo de la aplicación web antes de cargarla a la plataforma del servicio y ponerla en producción.
14. Realizar y mantener la documentación actualizada.
15. Mantener la documentación actualizada a lo implementado en el proyecto.
16. Actualmente hay controles que son responsabilidad de cómo está desarrollado y cómo es la arquitectura de Heroku y Strapi.
17. Tener un lugar de respaldo para montar el proyecto para tener alta disponibilidad ante una eventualidad.

- GitHub Pages

9. Bibliografía

Airfocus. (n.d.). *What Is a Back End (In a Website)? Definition & FAQs*. Airfocus. Retrieved January 14, 2022, from https://airfocus.com/glossary/what-is-a-back-end/

Airfocus. (n.d.). *What is a Front End (In a Website) - Definition & Development*. Airfocus. Retrieved January 14, 2022, from https://airfocus.com/glossary/what-is-a-front-end/

Airfocus. (n.d.). *What Is an API? API Definition, Examples, Benefits, Challenges & FAQ*. Airfocus. Retrieved January 14, 2022, from https://airfocus.com/glossary/what-is-an-api/

GitHub. (n.d.). *Git Guides*. GitHub. Retrieved January 14, 2022, from https://github.com/git-guides

Heroku. (n.d.). *Heroku*. Heroku: Cloud Application Platform. Retrieved January 14, 2022, from https://www.heroku.com/

Romero, E. (n.d.). *Heroku - Una plataforma para la creación de aplicaciones - Esteban Romero*. Esteban Romero Frías. Retrieved January 14, 2022, from https://estebanromero.com/herramientas-emprender-desarrollar-proyectos/heroku-una-plataforma-para-la-creacion-de-aplicaciones/

Strapi. (n.d.). *FAQ*. Strapi. Retrieved January 14, 2022, from https://strapi.io/faq