Muchas de nuestras aplicaciones o proyectos requieren de dependencias para su correcto funcionamiento, pero cuando estas dependencias no están actualizadas, podrían causar muchos problemas con la seguridad, adicional la actualización manual de estas dependencias y la comprobación de actualizaciones pueden ser estresantes.

**Dependabot**

Dependabot es una herramienta ya totalmente integrada con github, que podemos utilizar para automatizar el análisis y las actualizaciones de dependencias de nuestros proyectos desarrollados.

Funciona analizando los archivos de dependencia de nuestros proyectos, verificando que no haya una versión más reciente en los repositorios oficiales, o de los proyectos (Github). Después del análisis, crea automáticamente pull request para las dependencias que no están al día. Normalmente, leerá el archivo correspondiente, en función del idioma que se especifique, como por ejemplo el package.json.

Dependabot aprovecha la api de **GitHub Security Advisory** para automatizar el proceso y crear solicitudes de extracción para corregir vulnerabilidades a medida que se encuentran.

**GitHub Security Advisory**: Detrás de las características de seguridad de GitHub hay una base de datos cuidadosamente seleccionada de vulnerabilidades de seguridad agregadas de toda la web. Estos datos ahora están disponibles para todos los desarrolladores con la API de asesoramiento de seguridad.

Al poder acceder a la api de **Security Advisory,** Dependabot puede:

* automatizar el proceso de monitoreo.
* ayudar a verificar los avisos de seguridad en los archivos de dependencia.
* crea solicitudes de extracción (pull requests) para corregir las vulnerabilidades a medida que se encuentran.

Cabe mencionar que Dependabot no solo crea solicitudes de extracción para vulnerabilidades de seguridad de forma predeterminada, sino que creará solicitudes de extracción siempre que haya una actualización disponible.

**Las alertas del dependabot**

GitHub puede crear Las alertas del dependabot cuando detecta dependencias vulnerables en tu repositorio. La alerta se muestra en la ficha Seguridad del repositorio. La alerta incluye un vínculo al archivo afectado en el proyecto e información sobre una versión fija. GitHub también notifica a los mantenedores del repositorio, de acuerdo con sus preferencias de notificación. Para obtener más información, consulte "Acerca de las alertas para dependencias vulnerables".

**Actualizaciones de seguridad del dependabot**

Cuando GitHub genera una alerta de Dependabot para una dependencia vulnerable en su repositorio, Dependabot puede intentar solucionarlo automáticamente por usted. Las actualizaciones de seguridad del dependabot son solicitudes de extracción generadas automáticamente que actualizan una dependencia vulnerable a una versión fija. Para obtener más información, consulte "Acerca de Actualizaciones de seguridad del dependabot".

**Gráfico de dependencias**

El gráfico de dependencias es un resumen de los archivos de manifiesto y bloqueo almacenados en un repositorio. Le muestra los ecosistemas y paquetes de los que depende su base de código (sus dependencias) y los repositorios y paquetes que dependen de su proyecto (sus dependientes). La información del gráfico de dependencias es utilizada por dependency review y Dependabot. Para obtener más información, consulte "Acerca del gráfico de dependencias".

**Acerca del archivo dependabot.yml**

El archivo de configuración de Dependabot, dependabot.yml, utiliza la sintaxis YAML. Si es nuevo en YAML y desea obtener más información, consulte "Aprender YAML en cinco minutos".

Debe almacenar este archivo en el directorio de su repositorio. Al agregar o actualizar el archivo dependabot.yml, esto desencadena una comprobación inmediata de las actualizaciones de versión.  
Cualquier opción que también afecte a las actualizaciones de seguridad se usará la próxima vez que una alerta de seguridad active una solicitud de extracción para una actualización de seguridad.  
El archivo dependabot.yml tiene dos claves de nivel superior obligatorias: , y . Opcionalmente, puede incluir una clave de nivel superior. El archivo debe comenzar con .versionupdatesregistriesversion: 2  


Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**package-ecosystem**

Obligatorio. Agregue un elemento para cada administrador de paquetes que desee que Dependabot supervise en busca de nuevas versiones. El repositorio también debe contener un manifiesto de dependencia o un archivo de bloqueo para cada uno de estos administradores de paquetes. Si desea habilitar la creación de proveedores para un administrador de paquetes que lo admita, las dependencias de proveedores deben estar ubicadas en el directorio requerido. Para obtener más información, consulte el proveedor a continuación. package-ecosystem

La siguiente tabla muestra, para cada administrador de paquetes:

* El valor YAML a utilizar en el archivo dependabot.yml
* Las versiones compatibles del administrador de paquetes
* Si las dependencias en los repositorios o registros privados de GitHub son compatibles
* Si las dependencias delegadas a proveedores son compatibles

**Directory**

‎Obligatorio‎‎. Debe definir la ubicación de los manifiestos de paquete para cada administrador de paquetes (por ejemplo, ‎‎package.json‎‎ o ‎‎Gemfile‎‎). El directorio se define en relación con la raíz del repositorio para todos los ecosistemas, excepto github Actions. Para Acciones de GitHub, establece el directorio en para buscar archivos de flujo de trabajo en .‎/.github/workflows

**schedule.interval**

Obligatorio. Debe definir con qué frecuencia buscar nuevas versiones para cada administrador de paquetes. De forma predeterminada, Dependabot asigna aleatoriamente una hora para aplicar todas las actualizaciones en el archivo de configuración. Para establecer una hora específica, puede usar schedule.time y schedule.timezone.

daily—funciona todos los días laborables, de lunes a viernes.

weekly—se ejecuta una vez por semana. De forma predeterminada, esto es el lunes. Para modificar esto, use schedule.day.

monthly— se ejecuta una vez al mes. Esto es el primer día del mes.

Imagen que contiene Tabla

Descripción generada automáticamente  
Pantalla de celular con imagen de la pantalla de un celular

Descripción generada automáticamente con confianza media

Captura de pantalla de un celular

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de computadora

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

[Dependabot : Como mantener las dependencias actualizadas y seguras – Davidson](https://www.davidson.es/blog/dependabot-como-mantener-las-dependencias-actualizadas-y-seguras)

[Acerca de la administración de dependencias vulnerables - GitHub Docs](https://docs.github.com/es/code-security/supply-chain-security/managing-vulnerabilities-in-your-projects-dependencies/about-managing-vulnerable-dependencies)

[Acerca de las actualizaciones de seguridad de Dependabot - GitHub Docs](https://docs.github.com/es/code-security/supply-chain-security/managing-vulnerabilities-in-your-projects-dependencies/about-dependabot-security-updates)

[Dependabot. Muchas de nuestras aplicaciones… | by Adonis Mendoza | Medium](https://medium.com/@adonis.mendoza/dependabot-c08d3ffae7d2)

[Opciones de configuración para actualizaciones de dependencias - GitHub Docs](https://docs.github.com/es/enterprise-server@3.4/code-security/supply-chain-security/keeping-your-dependencies-updated-automatically/configuration-options-for-dependency-updates)

[Administrar corredores autohospedados para actualizaciones de Dependabot en tu empresa - GitHub Docs](https://docs.github.com/es/enterprise-server@3.3/admin/github-actions/enabling-github-actions-for-github-enterprise-server/managing-self-hosted-runners-for-dependabot-updates)

[Administrar GitHub Connect - GitHub Docs](https://docs.github.com/es/enterprise-server@3.0/admin/configuration/configuring-github-connect/managing-github-connect)

[Habilitación de Dependabot para tu empresa - GitHub Docs](https://docs.github.com/es/enterprise-server@3.0/admin/configuration/configuring-github-connect/enabling-dependabot-for-your-enterprise)

## Las alertas del dependabot

GitHub puede crear Las alertas del dependabot cuando detecta dependencias vulnerables en tu repositorio. La alerta se muestra en la ficha Seguridad del repositorio. La alerta incluye un vínculo al archivo afectado en el proyecto e información sobre una versión fija. GitHub también notifica a los mantenedores del repositorio, de acuerdo con sus preferencias de notificación. Para obtener más información, consulte "[Acerca de las alertas para dependencias vulnerables](https://docs.github.com/es/code-security/supply-chain-security/about-alerts-for-vulnerable-dependencies)".

## Actualizaciones de seguridad del dependabot

Cuando GitHub genera una alerta de Dependabot para una dependencia vulnerable en su repositorio, Dependabot puede intentar solucionarlo automáticamente por usted. Las actualizaciones de seguridad del dependabot son solicitudes de extracción generadas automáticamente que actualizan una dependencia vulnerable a una versión fija. Para obtener más información, consulte "[Acerca de Actualizaciones de seguridad del dependabot](https://docs.github.com/es/github/managing-security-vulnerabilities/about-dependabot-security-updates)".

Por defecto genera 5