STOCKHOLM

GUÍA DEL USUARIO

SEGURIDAD

STOCKHOLM es una plataforma de la Estrategia de Preposicionamiento de Suministros de Emergencia (ESUPS).

ESUPS está auspiciado por Welthungerhilfe (WHH) y dirigido por un Grupo Directivo de actores humanitarios clave.

STOCKHOLM ha sido desarrollado por Tonkin + Taylor, una empresa registrada especializada en el desarrollo ágil de sitios web tras catástrofes. Está gestionado por WHH y alojado en dos servidores situados en Europa.

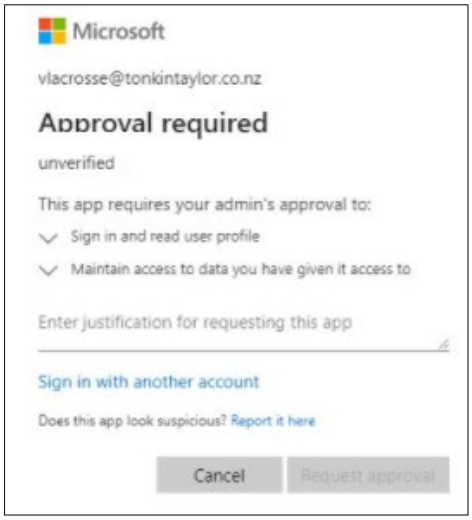
STOCKHOLM se adhiere a los requisitos del Reglamento General de Protección de Datos (RGPD).

AUTENTICACIÓN DE ANUNCIOS DE MICROSOFT AZURE

STOCKHOLM utiliza el inicio de sesión de Microsoft Azure AD como uno de los métodos de autenticación. Se trata de un servicio de gestión de identidades y accesos basado en la nube y gestionado por Microsoft.

Esta aplicación requiere la aprobación de su administrador de TI interno para utilizarla como método de inicio de sesión y para leer el perfil del usuario (por ejemplo, correo electrónico y nombre de usuario).

A continuación se muestra una captura de pantalla de la ventana emergente de aprobación requerida por Microsoft que aparece:



Una vez que el administrador de TI interno haya concedido la aprobación a todo el sistema, cualquier persona de ese mismo organismo podrá acceder a STOCKHOLM.

No es necesaria la aprobación individual para diferentes usuarios dentro de la misma agencia.

La aplicación requiere la aprobación del administrador de TI para:

1. Inicia sesión y leer el perfil de usuario

2. Mantener el acceso a los datos a los que usted le ha dado permiso para acceder.

En el siguiente cuadro se explica con más detalle.

Admin Consent display Name	Admin consent description	User consent display name	User consent description	Related MS Graph Scope
Maintain access to data you have given it access to	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	**Maintain access to data you have given it access to**	Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.	*offline_access*
Inspire Usage: This permission scope is required for single sign on (SSO) and allows a refresh token to be returned from the authentication flow so that the Inspire application can perform task and calendar synchronizations without user involvement and not prompt the user every time their primary authentication token times out.				
Admin Consent display Name	**Admin consent description**	**User consent display name**	**User consent description**	**Related MS Graph Scope**
Sign in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	**Sign you in and read your profile**	Allows you to sign in to the app with your organizational account and let the app read your profile. It also allows the app to read basic company information.	*User.Read*
Inspire Usage: This permission scope is required for single sign on (SSO).				

CÓMO DAR EL VISTO BUENO

1. **Inicie sesión en el portal de Azure** utilizando una cuenta de usuario de Azure AD con uno de los siguientes roles:
   a) Administrador global o administrador con funciones privilegiadas, para conceder el consentimiento a las aplicaciones que soliciten cualquier permiso, para cualquier API.

b) Administrador de aplicaciones en la nube o administrador de aplicaciones, para conceder el consentimiento a las aplicaciones que soliciten cualquier permiso para cualquier API, excepto Azure AD Graph o los roles de aplicación de Microsoft Graph (permisos de aplicación).
c) Un rol de directorio personalizado que incluye el permiso para conceder permisos a las aplicaciones, para los permisos requeridos por la aplicación.

2. Seleccione **Azure Active Directory** y, a continuación, seleccione **Aplicaciones empresariales**.

3. Seleccione la **aplicación** a la que desea conceder el consentimiento de administrador para todo el inquilino y, a continuación, seleccione **Permisos**.

4. Revise cuidadosamente los **permisos** que requiere la aplicación.

5. Si está de acuerdo con los permisos que requiere la aplicación, seleccione **Conceder consentimiento de administrador**.

MÁS INFORMACIÓN
Conceder el consentimiento de administrador de todo el sistema a una aplicación - Microsoft Entra