centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1633

Procedimiento de Empleo Seguro
IRONCHIP Location-Based Identity Platform

Febrero de 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-075-1.
Fecha de Edición: febrero de 2024

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.19 09:31:16 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. La solución de *Ironchip Location-Based Identity Platform* es una plataforma de gestión de accesos y protección de identidades, basada en Inteligencia Artificial de localización. Permite la configuración de innovadoras políticas de seguridad, evitando la suplantación de identidades y los accesos no autorizados a los servicios protegidos.
2. Incluye integraciones preconfiguradas que el administrador puede completar siguiendo sencillos pasos, protegiendo todos los servicios IT de la empresa.
3. Los usuarios son integrados en la plataforma mediante la sincronización con el AD, permitiendo gestionar todos los permisos, individuales y grupales, aplicando distintos métodos de accesos y políticas de seguridad, garantizando la protección robusta a los servicios más críticos.

    - Gestión de privilegios basada en roles. Establece diferentes privilegios de usuario para prevenir el acceso no autorizado al resto del sistema.
    - Restringe el acceso desde lugares no autorizados. Genera acceso habilitado desde áreas autorizadas.
    - Monitorización de accesos en tiempo real. Documenta la actividad de los usuarios, visualiza el acceso en una línea de tiempo, genera informes, que pueden ser descargados para un control completo.

2. OBJETO Y ALCANCE

4. En esta guía se proporciona una descripción detallada de la instalación segura del servicio de Location-Based Identity platform, tanto como su configuración.

5. También proporcionaremos detalles para el correcto uso de nuestra plataforma. Esta guía facilita el manejo de las funciones permitiendo el dominio de las características que ofrece nuestro servicio, además mostraremos los pasos a seguir en las tareas que se deben realizar con el fin de proporcionar al usuario una herramienta que garantice la seguridad de accesos y empresas a través de una buena y fácil experiencia diaria.

6. Para la aplicación móvil, los dispositivos compatibles son:

    - Desde **Android** 8.0.
    - Desde **iOS** 10.0.

7. Para la aplicación de escritorio, los sistemas operativos compatibles son:

    - Desde Microsoft Windows 7.
    - Para **Linux**, en las distribuciones basadas en .deb o .rpm o en distribuciones compatibles.
    - Desde **Mac OS** Sierra.

8. **Este servicio ha sido cualificado e incluido en el Catálogo de Productos y Servicios de seguridad (CPSTIC) del Centro Criptológico Nacional para categoría ALTA.**

3. ORGANIZACIÓN DEL DOCUMENTO

9. El presente documento se divide en los siguientes apartados:

   a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

   b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

   c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   d) Apartado **7**. En este apartado se recogen las referencias usadas en el presente documento.

   e) Apartado **8**. En este apartado se recogen a modo de glosario las abreviaturas utilizadas a lo largo de este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Existen dos (2) tipos de distribuciones: pública y privada.
11. La distribución pública:
    a) Aplicación móvil:

       Ironchip proporciona una aplicación móvil generalmente mediante tiendas oficiales. La aplicación está disponible tanto para Android como iOS. La utilización en ambos sistemas es igual. La descarga de la aplicación se efectuará por lo general mediante las tiendas oficiales; Google Play o App Store.

    b) Aplicación de escritorio:

       Windows: La descarga de la aplicación en estos sistemas operativos se hará mediante el repositorio interno de Ironchip, este enlace a la aplicación lo proporcionará Ironchip. Para la descarga será suficiente con pulsar sobre el enlace.

12. Para la distribución privada, se disponemos de un repositorio de aplicaciones privado en caso de que se requiera este tipo de distribución. Es un proceso bajo demanda.

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado disponga de autorización para la configuración, despliegue y mantenimiento del producto.
14. Para garantizar una implementación segura del producto, es esencial que el entorno de instalación esté debidamente plataformado, abarcando tanto dispositivos móviles como equipos de sobremesa.
15. Además, al considerar dispositivos móviles de uso privado, es crucial tener en cuenta la seguridad de la información. Se requiere que estos dispositivos estén protegidos mediante la activación de patrones, contraseñas o biometría. Esto no solo salvaguarda la privacidad del usuario, sino que también añade un nivel adicional de protección a los datos sensibles que puedan estar asociados con el producto. La implementación de estas medidas de seguridad refuerza la integridad del entorno de instalación, asegurando que solo usuarios autorizados tengan acceso al producto y protegiendo así la confidencialidad de la información almacenada o procesada.
16. Asimismo, en lo que respecta a la seguridad en los sistemas de escritorio donde se implementa nuestro producto, es esencial restringir el número de usuarios con privilegios de administrador. Al acotar el acceso de los usuarios con privilegios de administrador, se refuerza la gestión de la seguridad y la cantidad de puntos potenciales de vulnerabilidad.

4.3 REGISTRO Y LICENCIAS

17. El registro es público y se puede hacer a través de la página web (https://www.ironchip.com/es/) en la esquina superior derecha al darle al botón “Prueba

gratuita" o directamente desde (https://www.ironchip.com/es/signup/) se abrirá un formulario que debemos completar para que podamos registrarnos en Ironchip.

18. Al contratar el producto, se incluyen las primeras cinco (5) licencias de forma gratuita. En caso de que requieras más licencias, ofrecemos la posibilidad de ampliarlas según tus necesidades, simplemente contactando con Ironchip. Es esencial destacar que nuestras licencias son no nominales y que protegen una identidad de usuario de manera independiente, sin importar el número de servicios utilizados o dispositivos protegidos.

4.4 CONSIDERACIONES PREVIAS

19. Antes de iniciar el proceso de instalación del producto en su versión de escritorio, es crucial tener en cuenta algunas consideraciones previas para garantizar la seguridad integral del sistema. Dado que el producto utiliza claves criptográficas para la identidad del usuario, es necesario que el proceso de instalación requiera permisos de administrador.

20. Estos privilegios adicionales aseguran que el sistema tenga la capacidad necesaria para gestionar de manera segura las operaciones criptográficas que sustentan la identidad del usuario, contribuyendo así a fortalecer la protección y confidencialidad de la información crítica. Al otorgar permisos de administrador durante la instalación, se habilita un entorno seguro que potencia la funcionalidad del producto y garantiza una experiencia de usuario robusta y fiable.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

21. En el entorno operativo del producto se encuentran, por una parte, el equipo cliente que será el encargado de ejecutar un navegador web, que, a su vez será el soporte final de ejecución del producto. El producto es compatible con los navegadores Edge, Chrome, Firefox y Safari cuyas versiones asociadas deben de soportar la versión 5 de HTML y además adecuarse a la norma ECMA-262 para el soporte de JavaScript.

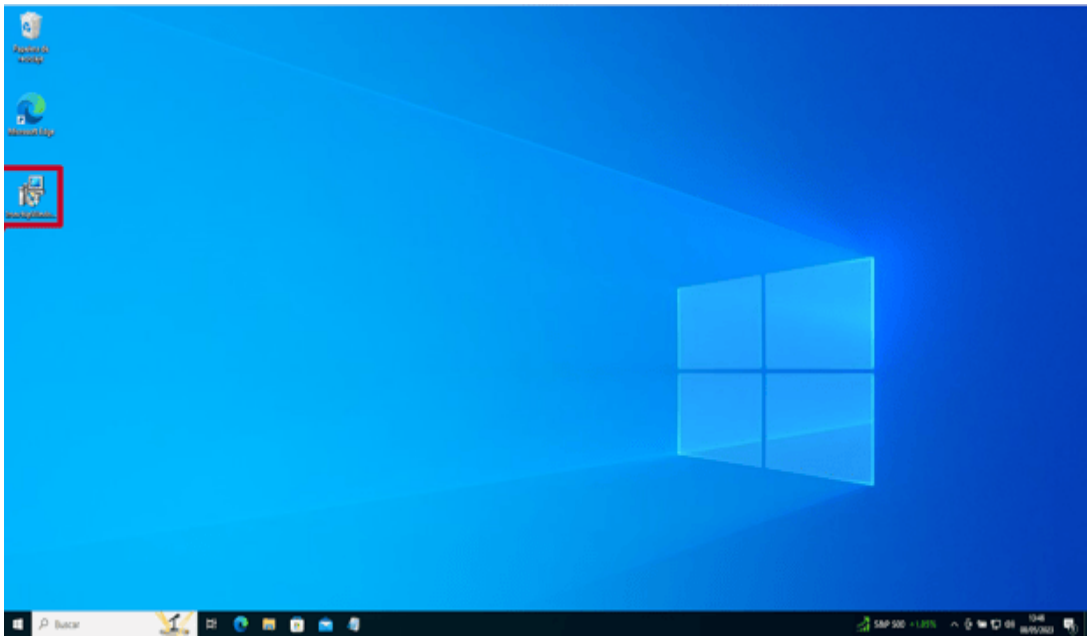
5. FASE DE INSTALACIÓN

5.1 INSTALACIÓN ESCRITORIO

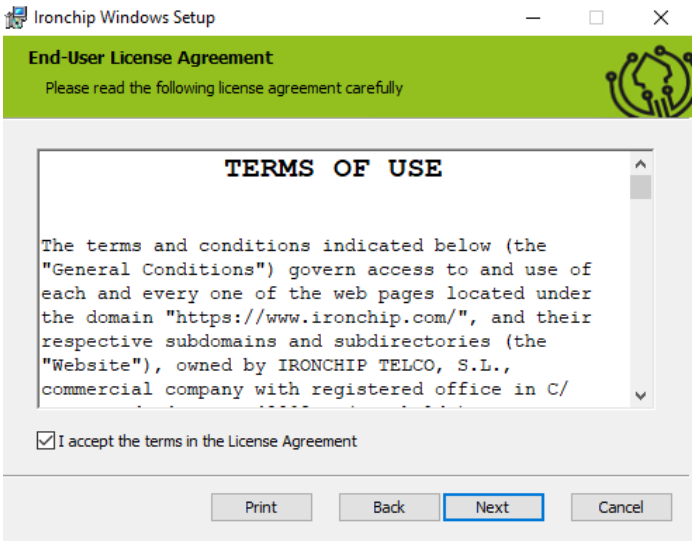
5.1.1 ESCRITORIO WINDOWS

22. La instalación de la aplicación de escritorio en Windows es segura por defecto, requiriendo medidas de seguridad mínimas adicionales más allá de las indicadas en la siguiente guía.

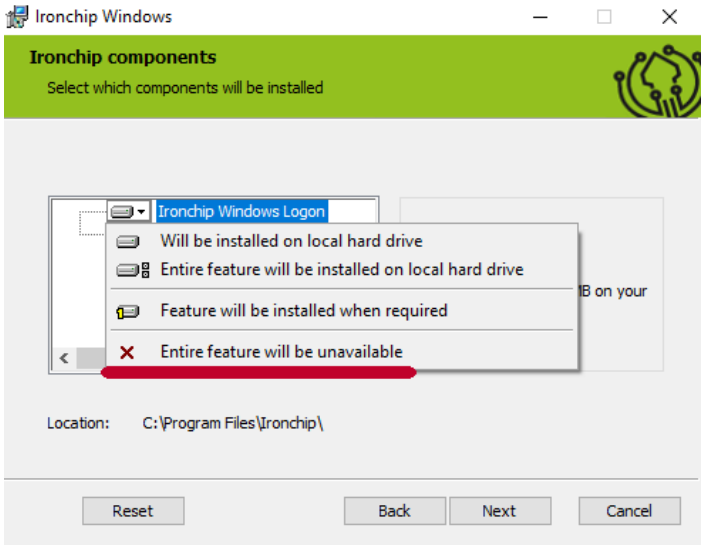
23. El instalador de la aplicación de escritorio de Windows ha de ser suministrado por un administrador técnico de su compañía. Una vez tenga a su disposición este instalador proceda a ejecutarlo haciendo doble clic en su icono:



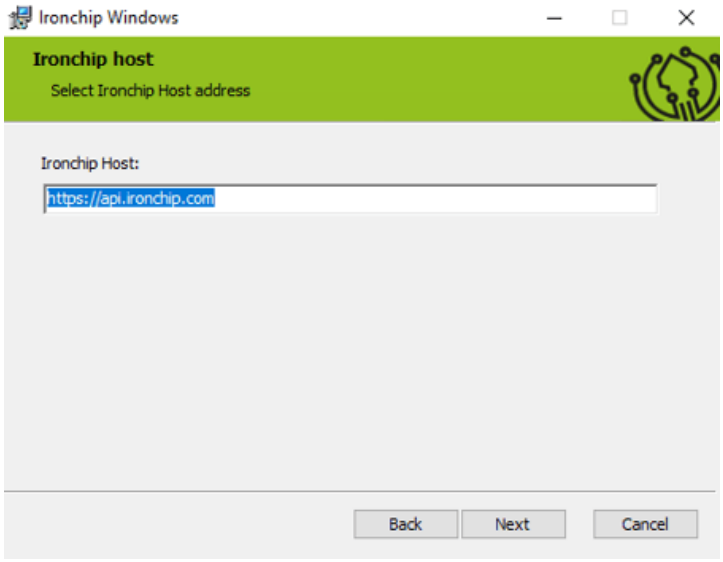
24. Primeramente, aparecerá la licencia de Ironchip, en donde se informan de los términos de uso. Se debe leer y marcar el campo "*I accept the terms in the License Agreement*" para poder proceder con la instalación, pulsar "*Next*" a continuación.



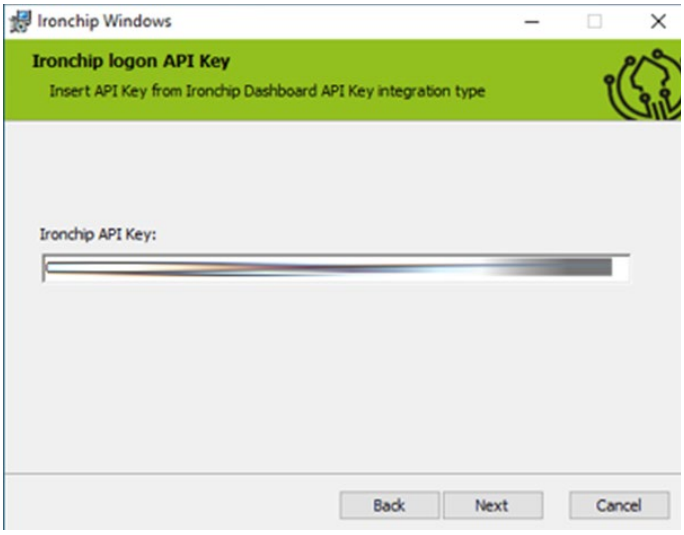
25. Seleccionar "*Ironchip Windows Logon*" y pulsar en "*Entire feature Will be unavailable*" para evitar la instalación del producto "*Windows Logon*".



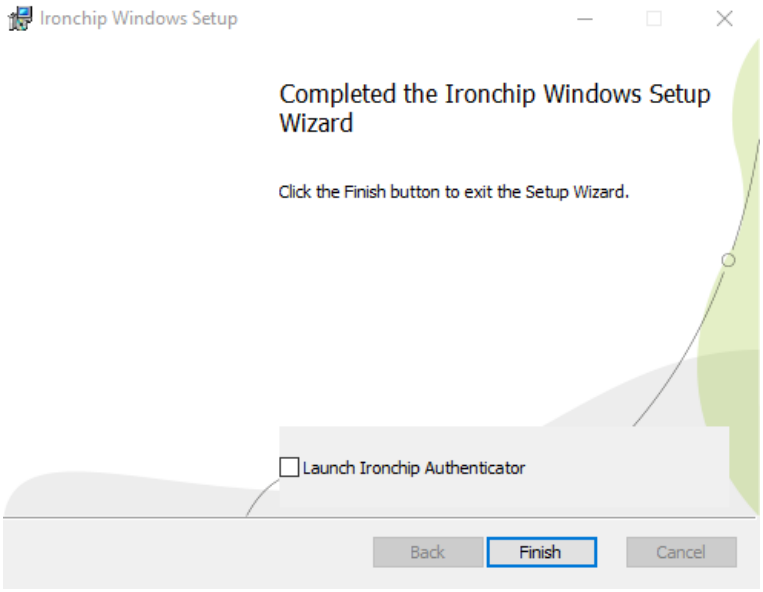
26. Pulsar "*Next*" para continuar y, en la siguiente pantalla del instalador mantenga el valor por defecto "https://api.ironchip.com":



27. Pulsar "*Next*" para proseguir, en la siguiente pantalla se debe introducir la API Key suministrada por el mismo programa. En el caso de que no disponerla, se debe contactar con el administrador técnico de la compañía.



28. Por último, pulsar en "*Next*" e "*Install*" en la siguiente pantalla para proceder con la instalación. Son necesarios permisos de administración sobre el equipo para poder realizar la instalación con éxito:



29. Pulsar en "*Finish*" para cerrar la instalación.

5.2 INSTALACIÓN MÓVIL

5.2.1 PLAY STORE

30. Los pasos para instalar la aplicación en un Sistema Operativo Android son los siguientes:

    a) Para descargar la aplicación de autenticación en un dispositivo móvil Android, debe acudir primero a la aplicación "Play Store".

    b) Una vez dentro, utilizar la barra superior de búsqueda e introducir "Ironchip" y buscar.

    c) Una vez realizada, seleccionar la aplicación "Ironchip Authenticator" y pulsar en instalar para comenzar la instalación.

d) Una vez pulsado el botón, el proceso de descarga e instalación dará comienzo. Cuando la aplicación haya finalizado, el botón de "Instalar" habrá cambiado a "Abrir" y la aplicación de autenticación se encontrará entre las que ya tenga instaladas.

5.2.2 APPLE STORE

31. Los pasos para instalar la aplicación en un Sistema Operativo IOS son los siguientes:

    a) Para descargar la aplicación de autenticación en un dispositivo móvil Apple acudir a la aplicación "*Apple Store*".

    b) A continuación, pulsar en la lupa inferior izquierda para realizar la búsqueda. Una vez realizada, seleccionar la aplicación "*Ironchip Authenticator*" y pulsar en Instalar para comenzar la instalación.

    c) Cuando la instalación haya finalizado, el botón de "Instalar" habrá cambiado a "Abrir" y la aplicación de autenticación se encontrará entre las que ya se tengan instaladas.

5.3 PROCESO DE ALTA

32. Dentro del *dashboard* en la pestaña de servicios se encuentran todos los servicios a los que se tienen acceso, incluyendo el de "Panel de gestión Ironchip", sí así se desea.

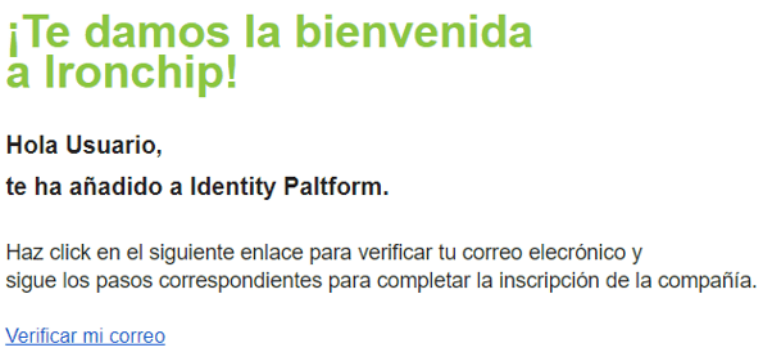
33. Se recuerda que el servicio "Panel de gestión Ironchip" es exclusivo para los administradores seleccionados, que serán los encargados de llevar la gestión de las autenticaciones y accesos a los servicios.

5.3.1 ALTA MEDIANTE APLICACIÓN MÓVIL

34. Para proceder a registrar la aplicación de autenticación primero es necesario haberla descargado (Sección 4.1) e instalado (Sección 5.2).

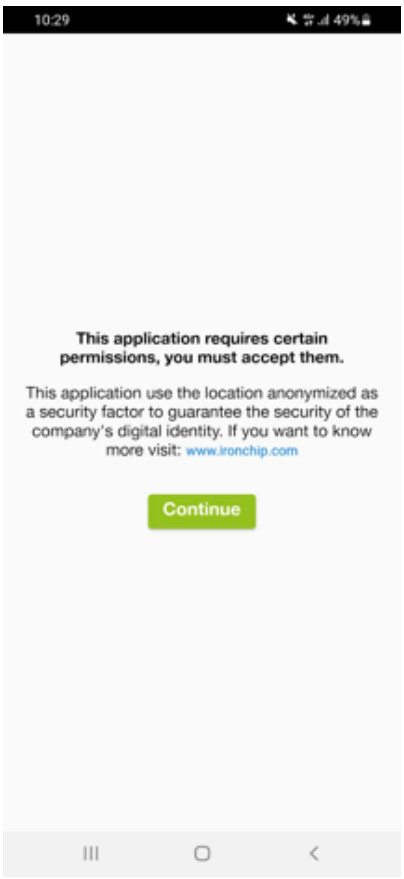
35. Para registrarse, un Administrador habrá dado de alta al usuario mediante el panel de control, "Panel de gestión". En ese momento, se enviará un correo electrónico para verificar y se seguirán los siguientes pasos:

    a) En el correo se pulsará el botón "Verificar mi correo".

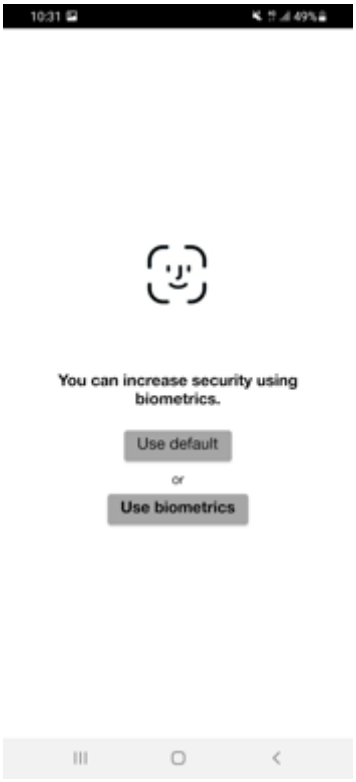


    b) Si ya se ha descargado la aplicación se pulsará "*Continuar*". Si no, se podrá descargar pulsando en la imagen correspondiente.

c) Se abrirá la aplicación y se aceptarán los permisos pertinentes.



36. Se podrá elegir si usar biometría en la aplicación.

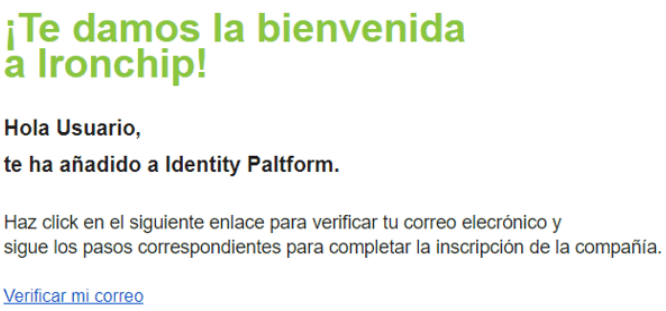


37. El QR que aparece en la pantalla del ordenador será escaneado con la aplicación de Ironchip.

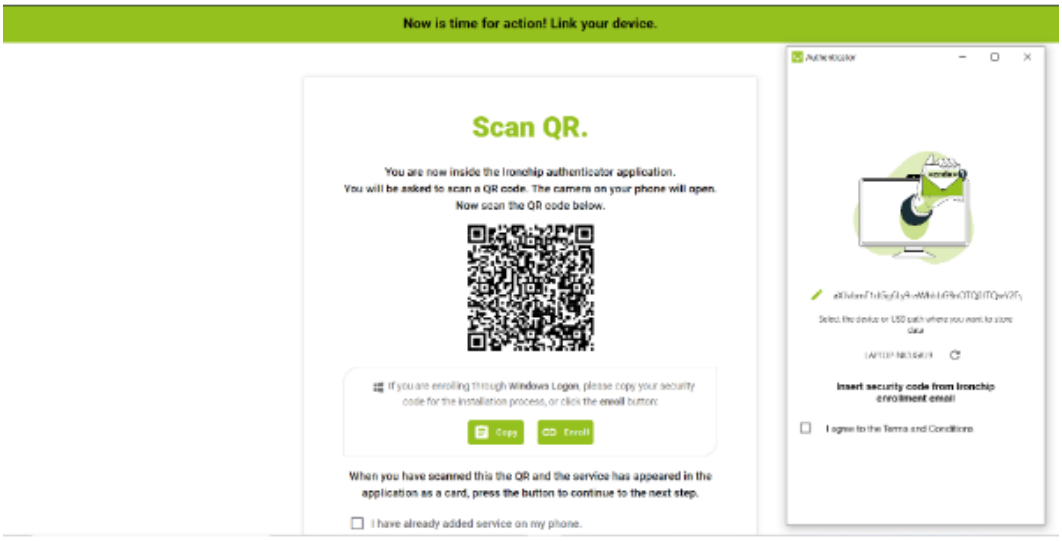
38. Con esto, se habrá acabado el proceso de registro. Se tendrá la confirmación cuando en el ordenador aparezca la siguiente imagen y en el móvil la aplicación se haya abierto.

5.3.2 ALTA MEDIANTE ESCRITORIO

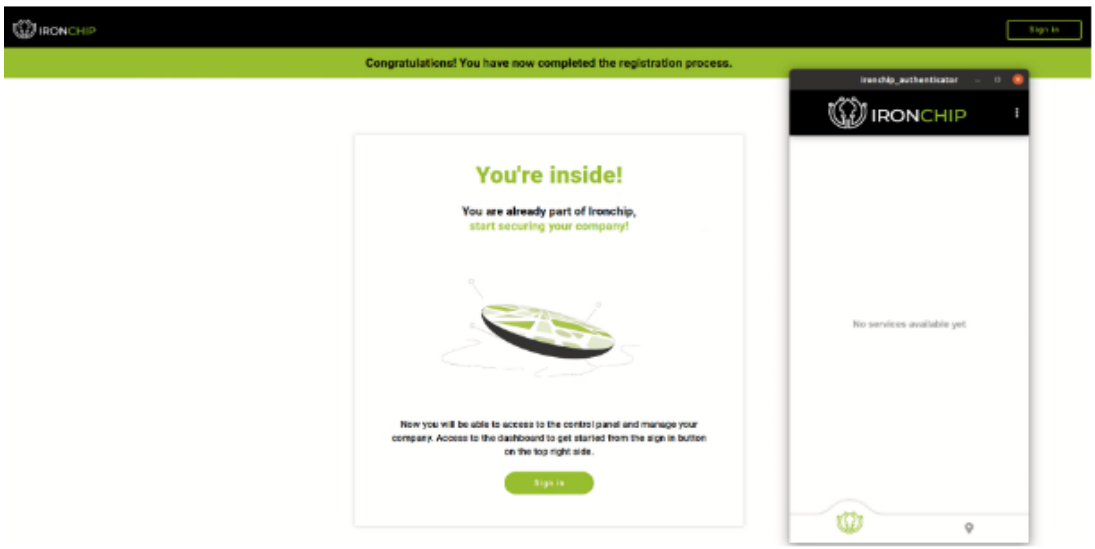
39. Para proceder a registrar la aplicación de autenticación primero es necesario haberla descargado (Sección **4.1**) e instalado (Sección **5.1**).
40. Para registrarse mediante un escritorio, un Administrador habrá dado de alta al usuario en la plataforma mediante el panel de control, “Panel de gestión”. En ese momento, se enviará un correo electrónico para la verificación y se seguirán los siguientes pasos:
41. En el correo se pulsará el botón de “Verificar mi correo”.



42. La aplicación de escritorio estará descargada; por lo tanto, se debe pulsar en “Continuar”.
43. El código de seguridad que aparece en la pantalla del ordenador será copiado e introducido en la aplicación de escritorio de Ironchip.



44. Con esto habrá acabado el proceso de registro. Se tendrá confirmación de ello cuando en el ordenador aparezca la siguiente imagen y la aplicación se haya abierto.



5.3.3 ALTA MEDIANTE USB

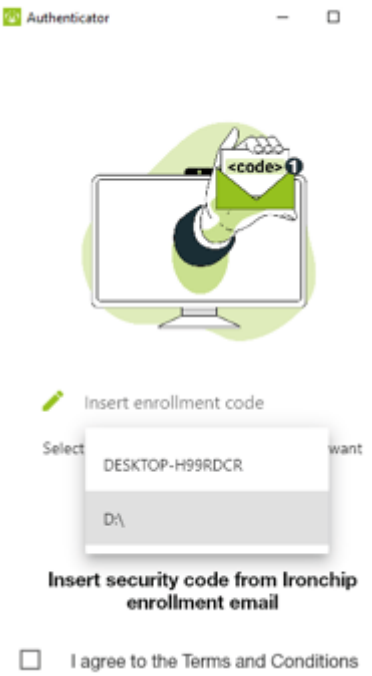
45. Esta opción permite llevar las credenciales de identificación a cualquier aviación. Una vez se haya registrado utilizando un dispositivo de memoria externo, puede usarlo como mecanismo de autenticación en cualquier dispositivo compatible con Ironchip que tenga instalado los servicios de escritorio de Ironchip.

46. Para realizar el registro de un nuevo dispositivo como proveedor de identidad, se necesitará seleccionar el dispositivo en el que se desea realizar la instalación durante el proceso de registro al ejecutar la Aplicación de escritorio de Ironchip:

    a) Introducir el dispositivo externo de almacenamiento.

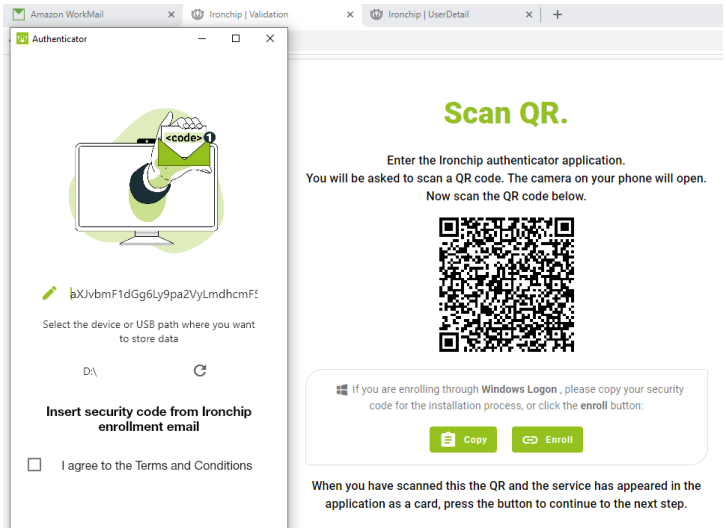
    b) Presionar el botón de Refrescar para escanear su dispositivo externo.

    c) Clic en el nombre del dispositivo a la izquierda del botón de refrescar y elegir el dispositivo externo deseado de la lista desplegable.



47. El dispositivo externo debe permanecer conectado para poder hacer uso de la aplicación de escritorio.

48. El administrador habrá mandado un email de alta y habrá que copiar el código recibido en el email y pegarlo en la ventana.



49. Y ya estaría dado de alta.

6. FASE DE CONFIGURACIÓN

50. El producto cuenta con una exhaustiva guía de uso general que proporciona información detallada sobre el funcionamiento operativo de cada uno de sus componentes. Sin embargo, esta guía tiene como objetivo orientar a los usuarios en la correcta utilización del producto, brindando instrucciones claras y paso a paso para configurar de forma segura el servicio.

51. Adicionalmente, la documentación proporcionada no sólo abarca aspectos técnicos, sino que también incluye recomendaciones y buenas prácticas para maximizar la seguridad y el rendimiento del producto en diferentes escenarios de aplicación. De este modo, se busca ofrecer a los usuarios una comprensión completa y detallada que les permita aprovechar al máximo las capacidades del producto de manera segura y efectiva.

6.1 MODO DE OPERACIÓN SEGURO

52. El diseño del producto se ha concebido con un enfoque centrado en la seguridad. Se han implementado medidas y protocolos específicos para garantizar un desempeño seguro en todas las posibles configuraciones del producto. Los valores por defecto han sido cuidadosamente seleccionados y configurados de manera que, en la mayoría de los casos, sean apropiados para un uso seguro y eficiente.

53. El producto no cuenta con distintos modos de operación. La configuración inicial del producto es segura por defecto.

6.2 AUTENTICACIÓN

6.2.1 AUTENTICACIÓN DEL SERVICIO

54. Los accesos a la herramienta de administración están protegidos por defecto mediante el propio producto quedando excluido cualquier mecanismo de autenticación no seguro.

55. Se ha restringido el acceso a la herramienta de administración únicamente a usuarios con privilegios de administrador. Esta limitación asegura que solo aquellos con los niveles adecuados de autorización puedan llevar a cabo funciones administrativas, proporcionando una capa de control adicional y mitigando posibles amenazas internas.

6.2.2 AUTENTICACIÓN DE APLICACIONES

56. En el caso de la aplicación autenticadora, esta queda bajo control de los administradores teniendo estos la potestad de eliminar o añadir nuevas aplicaciones a voluntad.

57. La autenticación en estas aplicaciones se realiza mediante un intercambio de claves seguras reflejándose en el intercambio de claves de TLS como el certificado cliente y servidor.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN REMOTA

58. El producto en cuestión es una solución remota que facilita la administración a través de una interfaz centralizada conocida como *dashboard* o panel de control. Para garantizar la

seguridad durante la comunicación, se utiliza el protocolo HTTPS, lo que asegura el cifrado de los datos transmitidos entre el usuario y el servidor, protegiendo así la confidencialidad e integridad de la información.

59. Además, se implementa una capa adicional de seguridad mediante la aplicación autenticadora Ironchip para MFA. Este método añade una capa adicional de protección al requerir que los usuarios verifiquen su identidad mediante algo que poseen (como un dispositivo móvil con la aplicación Ironchip instalada).

60. En resumen, la combinación de HTTPS y la autenticación MFA con Ironchip contribuye a garantizar un acceso seguro y controlado al dashboard, asegurando la integridad y privacidad de los datos gestionados a través de la plataforma remota.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

61. El usuario de administrador será proporcionado por Ironchip.

62. Para agregar un nuevo administrador a la plataforma es necesario que exista como usuario. Si existe como usuario, dentro de la herramienta de administración (dashboard), se debe acceder a la pestaña "*Users*" en la carpeta "*Directory*". Una vez verificado el usuario, seleccione "*Options*" y en el desplegable clique en "*Promote user*".

6.4 ACTUALIZACIONES

63. Las actualizaciones de la aplicación móvil se deberán hacer desde las tiendas oficiales *Google Play* o *App Store* según el dispositivo.

64. Las actualizaciones del *dashboard* se realizan automáticamente.

65. La aplicación de escritorio debe ser actualizada manualmente. Para ejecutar esta actualización se debe acudir al *dashboard* del producto donde, en la sección "*Plugins*" se encontrará siempre la última versión del aplicativo de escritorio.

66. Para proceder a la actualización, primero se debe descargar desde "*Windows Logon*" la última versión. Las actualizaciones están en formato "*msi*"; por lo que se ejecutará el programa descargado, a través de un *wizard* visual, y se procederá a la actualización.

67. Si el instalador detecta que la versión actualmente en ejecución es la misma o posterior a la descargada, el mismo instalador impedirá la actualización.

68. En cambio, cuando la versión sea anterior la ejecución de la actualización únicamente solicitará al usuario la autorización para proceder manteniéndose la configuración igual que en las instalaciones anteriores.

6.5 ALTA DISPONIBILIDAD

69. En relación a la Alta Disponibilidad, es relevante señalar que el SaaS ya ha sido implementado con un enfoque de Alta Disponibilidad. Este componente esencial del sistema asegura que el servicio permanezca accesible y funcional en todo momento.

6.6 AUDITORÍA

6.6.1 REGISTRO DE EVENTOS

70. Se generan eventos de seguridad cuando se realiza cualquier acción sobre el sistema y estos pueden ser solicitados por el usuario.

71. Se dispone de un sistema integral que registra de manera detallada cada acción llevada a cabo en la plataforma. Esta capacidad de seguimiento permite la generación de registros de todas las interacciones y operaciones realizadas, proporcionando así una trazabilidad completa de la actividad del sistema.

72. Estos datos pueden ser solicitados por el usuario si le es necesario. En el caso de solicitarlos, Ironchip se encargará de proveer los registros que requiera el usuario.

6.6.2 ALMACENAMIENTO REMOTO

73. En la operativa de almacenamiento remoto, se utiliza MongoDB Atlas para gestionar de manera eficiente los datos en la nube. Este servicio no solo simplifica la gestión de datos, sino que también destaca por su enfoque proactivo en la seguridad de la información.

74. Un aspecto fundamental que garantiza la integridad y confidencialidad de los datos es el cifrado en reposo proporcionado por MongoDB Atlas. Esta función asegura que, incluso en situaciones hipotéticas de acceso no autorizado a los dispositivos de almacenamiento, la información permanezca inaccesible sin la clave de cifrado correspondiente.

6.7 *BACKUP*

75. Las bases de datos del producto se encuentran en MongoDB Atlas, totalmente gestionados en la nube.

76. En MongoDB Atlas se realizan las copias de seguridad, con la siguiente periodicidad:

    - Diaria: Cada 6 horas.
    - Semanal: Cada sábado.
    - Mensual: Último día del mes.

77. Las copias de seguridad incrementales se realizan cada 6 horas, 4 veces al día con una retención de siete días. Además, cada sábado se realiza una copia de seguridad incremental con un tiempo de retención de 4 semanas. Y finalmente, la copia completa de la base de datos se ejecuta el último día de cada mes y su tiempo de retención es de 12 meses.

7. REFERENCIAS

78. La documentación de producto está disponible en el siguiente enlace:
https://knowledge.ironchip.com/es/plataforma-de-identidad

8. ABREVIATURAS

AD	Active Directory
API	Application Programming Interface
ENS	Esquema Nacional de Seguridad.
HTTPS	Hypertext Transfer Protocol Secure
MFA	Multi Factor Authenticator
mTLS	Mutual Transport Layer Security
SaaS	Software as a Service

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL