Actualización de Seguridad de Microsoft - Enero 2022

BCSC-ACTUALIZACION-MICROSOFT-2022-ENERO

TLP:WHITE

www.basquecybersecurity.eus

Enero 2022

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

Microsoft ha publicado las actualizaciones de seguridad para el mes enero de 2022, en donde se corrigen 102 vulnerabilidades, 9 calificadas como críticas, 92 como importantes y 1 como moderada.

A estas hay que añadir 24 vulnerabilidades que corrigen diferentes problemas en el navegador Edge basado en Chromium, para las que Microsoft no ha establecido un nivel de su severidad.

Afectan a productos como Microsoft Teams, Word, Excel o Windows Defender, entre otros.

La clasificación de las vulnerabilidades según su descripción es la siguiente:

- 2 vulnerabilidades de suplantación (spoofing)
- 9 vulnerabilidades de denegación de servicio.
- 6 vulnerabilidades de divulgación de información.
- 31 vulnerabilidades de ejecución remota de código.
- 10 vulnerabilidades de bypass.
- 43 vulnerabilidades de elevación de privilegios.
- 1 vulnerabilidad de cross-site scripting.

Se recomienda la aplicación de estas actualizaciones en cuanto sea posible.

2. RECURSOS AFECTADOS

Los parches de seguridad de este mes están asociados a vulnerabilidades que afectan a los siguientes productos:

- .NET Framework
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Teams
- Microsoft Windows Codecs Library
- Open Source Software
- Role: Windows Hyper-V
- Tablet Windows User Interface
- Windows Account Control
- Windows Active Directory
- Windows AppContracts API Server
- Windows Application Model
- Windows BackupKey Remote Protocol
- Windows Bind Filter Driver
- Windows Certificates
- Windows Cleanup Manager
- Windows Clipboard User Service
- Windows Cluster Port Driver
- Windows Common Log File System Driver
- Windows Connected Devices Platform Service
- Windows Cryptographic Services
- Windows Defender
- Windows Devices Human Interface
- Windows Diagnostic Hub
- Windows DirectX
- Windows DWM Core Library
- Windows Event Tracing
- Windows Geolocation Service
- Windows HTTP Protocol Stack
- Windows IKE Extension
- Windows Installer
- Windows Kerberos
- Windows Kernel
- Windows Libarchive
- Windows Local Security Authority
- Windows Local Security Authority Subsystem Service
- Windows Modern Execution Server
- Windows Push Notifications

- Windows RDP
- Windows Remote Access Connection Manager
- Windows Remote Desktop
- Windows Remote Procedure Call Runtime
- Windows Resilient File System (ReFS)
- Windows Secure Boot
- Windows Security Center
- Windows StateRepository API
- Windows Storage
- Windows Storage Spaces Controller
- Windows System Launcher
- Windows Task Flow Data Engine
- Windows Tile Data Repository
- Windows UEFI
- Windows UI Immersive Server
- Windows User Profile Service
- Windows User-mode Driver Framework
- Windows Virtual Machine IDE Drive
- Windows Win32K
- Windows Workstation Service Remote Protocol

3. ANÁLISIS TÉCNICO

Las vulnerabilidades más destacables que han sido corregidas en esta actualización son las 6 que han sido divulgadas públicamente, pero no explotadas activamente. Son las siguientes:

- CVE 2022-21836: Consiste en una vulnerabilidad de suplantación sobre la verificación binaria de WPBT, que es una tabla de interfaz de energía y configuración de firmware que permite ejecutar programas cuando arranca un dispositivo, y permite a los fabricantes la ejecución de software crítico que no se pueda realizar de forma regular con Windows. Desde Microsoft se recomienda aplicar una política, desde el control de aplicaciones de Windows Defender, que sea lo más restrictiva posible para proteger el entorno del usuario.
- CVE 2022-21839: Es una vulnerabilidad de denegación de servicio de la lista de control de acceso de seguimiento de eventos de Windows. El vector de ataque se basa en capacidades de lectura/escritura/ejecución de forma local y tiene condiciones para poder ser aprovechada por un atacante.
- CVE 2022-21874: Vulnerabilidad de ejecución remota del código de la API del centro de seguridad de Windows. El vector de ataque, como en la vulnerabilidad anterior, se basa en capacidades de lectura/escritura/ejecución de forma local y tiene unas condiciones de poder ser aprovechada por un atacante.
- CVE 2022-21919: Vulnerabilidad de elevación de privilegios del servicio de perfil de usuario de Windows. La complejidad de un ataque es alta, lo que implica que el agente malicioso debe contar con un nivel de conocimientos técnicos elevados para conseguir explotarla. El vector de ataque se basa en capacidades de lectura/escritura/ejecución de forma local.
- CVE 2022-22947: Es una vulnerabilidad en Curl, la herramienta por línea de comandos que se utiliza para conectar con servidores y trabajar con ellos usando la sintaxis de Url. Desde Microsoft consideran que su explotación es poco probable.
- CVE 2022-36976: Es una vulnerabilidad de ejecución de código remoto de Libarchive, librería de código abierto para trabajar con archivos comprimidos en Windows. Al igual que la anterior, desde Microsoft consideran que su explotación es poco probable.

La lista con todas las vulnerabilidades identificadas se detalla a continuación:

CVE	Descripción	Severidad	CVSS
CVE-2022-21912	Vulnerabilidad de ejecución remota de código en el Kernel de Directx Graphics	**Crítica**	7.8

CVE-2022-21846	Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server	**Crítica**	9.0
CVE-2022-21857	Vulnerabilidad de elevación de privilegios en los Servicios de Dominio de Active Directory	**Crítica**	8.8
CVE-2022-21898	Vulnerabilidad de ejecución remota de código en el Kernel de Directx Graphics	**Crítica**	7.8
CVE-2022-21833	Vulnerabilidad de elevación de privilegios en la unidad IDE de Máquina Virtual	**Crítica**	7.8
CVE-2022-21907	Vulnerabilidad de ejecución remota de código en la pila de protocolos HTTP	**Crítica**	9.8
CVE-2022-21840	Vulnerabilidad de ejecución remota de código en Microsoft Office	**Crítica**	8.8
CVE-2021-22947	Vulnerabilidad de ejecución remota de código remoto de Open Source Curl	**Crítica**	7.8
CVE-2022-21917	Vulnerabilidad de ejecución remota de código en las extensiones de vídeo HEVC	**Crítica**	7.8
CVE-2022-21908	Vulnerabilidad de elevación de privilegios en Windows Installer	Importante	7.8
CVE-2022-21922	Vulnerabilidad de ejecución remota de código en tiempo de ejecución remota de llamadas a procedimientos remotos	Importante	8.8
CVE-2022-21847	Vulnerabilidad de denegación de servicio en Windows Hyper-V	Importante	6.5
CVE-2022-21964	Vulnerabilidad de divulgación de información en el diagnosticador de licencias de Escritorio Remoto	Importante	5.5
CVE-2022-21963	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.4

CVE-2022-21962	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.8
CVE-2022-21961	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.8
CVE-2022-21960	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.8
CVE-2022-21959	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.8
CVE-2022-21958	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.8
CVE-2022-21925	Vulnerabilidad de omisión de la característica de seguridad de protocolo remoto de Windows BackupKey	Importante	5.3
CVE-2022-21921	Vulnerabilidad de omisión de la característica de seguridad de Credential Guard de Windows Defender	Importante	4.4
CVE-2022-21924	Vulnerabilidad de bypass en característica de Workstation Service Remote Protocol Security Feature	Importante	5.3
CVE-2022-21913	Vulnerabilidad de bypass sobre característica de seguridad de protocolo remoto en la autoridad de seguridad local (política de dominio)	Importante	5.3
CVE-2022-21905	Vulnerabilidad de omisión de la característica de seguridad de Hyper-V en Windows	Importante	4.6
CVE-2022-21911	Vulnerabilidad de denegación de servicio en .NET Framework	Importante	7.5

CVE-2022-21910	Vulnerabilidad de elevación de privilegios en el controlador de puerto de Clúster de Microsoft	Importante	7.8
CVE-2022-21906	Vulnerabilidad de bypass en característica de seguridad en la aplicación de Windows Defender	Importante	5.5
CVE-2022-21904	Vulnerabilidad de divulgación de información de GDI en Windows	Importante	7.5
CVE-2022-21920	Vulnerabilidad de elevación de privilegios en Kerberos de Windows	Importante	8.8
CVE-2022-21850	Vulnerabilidad de ejecución remota de código en el cliente de Escritorio Remoto	Importante	8.8
CVE-2022-21849	Vulnerabilidad de ejecución remota de código en la extensión IKE de Windows	Importante	9.8
CVE-2022-21970	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Importante	6.1
CVE-2022-21969	Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server	Importante	9.0
CVE-2022-21954	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Importante	6.1
CVE-2022-21931	Vulnerabilidad de ejecución remota de código en Microsoft Edge (basado en Chromium)	Importante	4.2
CVE-2022-21930	Vulnerabilidad de ejecución remota de código en Microsoft Edge (basado en Chromium)	Importante	4.2
CVE-2022-21928	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.3
CVE-2022-21899	Vulnerabilidad de bypass en el Firmware de la Interfaz de seguridad de Windows Extensible	Importante	5.5

CVE-2022-21897	Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows	Importante	7.8
CVE-2022-21896	Vulnerabilidad de elevación de privilegios en la biblioteca principal de DWM de Windows	Importante	7.0
CVE-2022-21848	Vulnerabilidad de denegación de servicio en la extensión IKE de Windows	Importante	7.5
CVE-2022-21891	Vulnerabilidad de suplantación de identidad en Microsoft Dynamics 365 (local)	Importante	7.6
CVE-2022-21889	Vulnerabilidad de denegación de servicio en la extensión IKE de Windows	Importante	7.5
CVE-2022-21842	Vulnerabilidad de ejecución remota de código en Microsoft Word	Importante	7.8
CVE-2022-21837	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	Importante	8.3
CVE-2022-21914	Vulnerabilidad de elevación de privilegios en el Administrador de conexiones de acceso remoto de Windows	Importante	7.8
CVE-2022-21895	Vulnerabilidad de elevación de privilegios en el servicio de perfiles de usuario de Windows	Importante	7.8
CVE-2022-21916	Vulnerabilidad de elevación de privilegios en el controlador del sistema de archivos de registro común de Windows	Importante	7.8
CVE-2022-21855	Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server	Importante	9.0
CVE-2022-21851	Vulnerabilidad de ejecución remota de código en el cliente de Escritorio Remoto	Importante	8.8

CVE-2022-21903	Vulnerabilidad de elevación de privilegios en Windows GDI	Importante	7.0
CVE-2022-21890	Vulnerabilidad de denegación de servicio en la extensión IKE de Windows	Importante	7.5
CVE-2022-21902	Vulnerabilidad de elevación de privilegios en la biblioteca principal de DWM de Windows	Importante	7.8
CVE-2022-21852	Vulnerabilidad de elevación de privilegios en la biblioteca principal de DWM de Windows	Importante	7.8
CVE-2022-21900	Vulnerabilidad de omisión de la característica de seguridad de Hyper-V en Windows	Importante	4.6
CVE-2022-21867	Vulnerabilidad de elevación de privilegios en las aplicaciones de notificaciones Push de Windows	Importante	7.0
CVE-2022-21866	Vulnerabilidad de elevación de privilegios en el Iniciador de sistemas de Windows	Importante	7.0
CVE-2022-21865	Vulnerabilidad de elevación de privilegios en el servicio de plataforma de dispositivos conectados	Importante	7.0
CVE-2022-21864	Vulnerabilidad de elevación de privilegios en la API de servidor inmersivo de la interfaz de usuario de Windows	Importante	7.0
CVE-2022-21863	Vulnerabilidad de elevación de privilegios en el archivo de Windows StateRepository API Server	Importante	7.0
CVE-2022-21862	Vulnerabilidad de elevación de privilegios en la API principal del modelo de aplicaciones de Windows	Importante	7.0
CVE-2022-21861	Vulnerabilidad de elevación de privilegios en el motor de datos de flujo de tareas	Importante	7.0

CVE-2022-21860	Vulnerabilidad de elevación de privilegios en Windows AppContracts API Server	Importante	7.0
CVE-2022-21859	Vulnerabilidad de elevación de privilegios en el control de cuentas de Windows	Importante	7.0
CVE-2022-21901	Vulnerabilidad de elevación de privilegios en Windows Hyper-V	Importante	9.0
CVE-2022-21841	Vulnerabilidad de ejecución remota de código en Microsoft Excel	Importante	7.8
CVE-2022-21839	Vulnerabilidad de denegación de servicio en la lista de control de acceso discrecional de seguimiento de eventos de Windows	Importante	6.1
CVE-2022-21838	Vulnerabilidad de elevación de privilegios en el Administrador de limpieza de Windows	Importante	5.5
CVE-2022-21836	Vulnerabilidad de suplantación de certificados en Windows	Importante	7.8
CVE-2022-21835	Vulnerabilidad de elevación de privilegios en Microsoft Cryptographic Services	Importante	7.8
CVE-2022-21834	Vulnerabilidad de elevación de privilegios en el marco de controladores reflector del marco de controladores en modo de usuario de Windows	Importante	7.0
CVE-2022-21932	Vulnerabilidad de cross-site scripting de Microsoft Dynamics 365 Customer Engagement	Importante	7.6
CVE-2022-21915	Vulnerabilidad de divulgación de información en Windows GDI+	Importante	6.5
CVE-2022-21918	Vulnerabilidad de denegación de servicio en el archivo del kernel de gráficos DirectX	Importante	6.5

CVE-2022-21919	Vulnerabilidad de elevación de privilegios en el servicio de perfiles de usuario de Windows	Importante	7.0
CVE-2021-36976	Vulnerabilidad de ejecución remota de código en Libarchive	Importante	7.8
CVE-2022-21868	Vulnerabilidad de elevación de privilegios en la interfaz humana de dispositivos Windows	Importante	7.0
CVE-2022-21869	Vulnerabilidad de elevación de privilegios en el servicio de usuario del Portapapeles	Importante	7.0
CVE-2022-21858	Vulnerabilidad de elevación de privilegios en el controlador de filtro de enlace de Windows	Importante	7.8
CVE-2022-21871	Vulnerabilidad de elevación de privilegios en el tiempo de ejecución del recopilador estándar de Microsoft Diagnostics Hub	Importante	7.0
CVE-2022-21870	Vulnerabilidad de elevación de privilegios en el núcleo de aplicación de la interfaz de usuario de Tablet Windows	Importante	7.0
CVE-2022-21894	Vulnerabilidad de omisión de la característica de seguridad de arranque seguro	Importante	4.4
CVE-2022-21893	Vulnerabilidad de ejecución remota de código en el protocolo de Escritorio remoto	Importante	8.8
CVE-2022-21892	Vulnerabilidad de ejecución remota de código en el sistema de archivos resistente de Windows (ReFS)	Importante	6.8
CVE-2022-21888	Vulnerabilidad de ejecución remota de código en Windows Modern Execution Server	Importante	7.8
CVE-2022-21887	Vulnerabilidad de elevación de privilegios en Win32k	Importante	7.0
CVE-2022-21884	Vulnerabilidad de elevación de privilegios en el servicio de	Importante	7.8

	subsistema de autoridad de seguridad local		
CVE-2022-21883	Vulnerabilidad de denegación de servicio en la extensión IKE de Windows	Importante	7.5
CVE-2022-21843	Vulnerabilidad de denegación de servicio en la extensión IKE de Windows	Importante	7.5
CVE-2022-21882	Vulnerabilidad de elevación de privilegios en Win32k	Importante	7.0
CVE-2022-21885	Vulnerabilidad de elevación de privilegios en el Administrador de conexiones de acceso remoto de Windows	Importante	7.8
CVE-2022-21880	Vulnerabilidad de divulgación de información en Windows GDI+	Importante	7.5
CVE-2022-21872	Vulnerabilidad de elevación de privilegios en el seguimiento de eventos de Windows	Importante	7.0
CVE-2022-21881	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	7.0
CVE-2022-21874	Vulnerabilidad de ejecución remota de código en la API de Windows Security Center	Importante	7.8
CVE-2022-21875	Vulnerabilidad de elevación de privilegios en el almacenamiento de Windows	Importante	7.0
CVE-2022-21876	Vulnerabilidad de divulgación de información en Win32k	Importante	5.5
CVE-2022-21873	Vulnerabilidad de elevación de privilegios en el repositorio de datos de mosaico	Importante	7.0
CVE-2022-21878	Vulnerabilidad de ejecución remota de código en el servicio de geolocalización de Windows	Importante	7.8
CVE-2022-21879	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	5.5

CVE-2022-21877	Vulnerabilidad de divulgación de información en Storage Spaces Controller	Importante	5.5
CVE-2022-21929	Vulnerabilidad de ejecución remota de código en Microsoft Edge (basado en Chromium)	**Moderada**	2.5
CVE-2022-0108	Chromium: Implementación inapropiada en la navegación	Sin valor establecido	6.1
CVE-2022-0117	Chromium: Derivación de directivas en trabajadores de servicio	Sin valor establecido	6.1
CVE-2022-0116	Chromium: Implementación inadecuada en la composición	Sin valor establecido	6.1
CVE-2022-0115	Chromium: Uso no inicializado en la API de archivos	Sin valor establecido	6.1
CVE-2022-0114	Chromium: Acceso a memoria fuera de los límites en Web Serial	Sin valor establecido	6.1
CVE-2022-0113	Chromium: Implementación inapropiada en Blink	Sin valor establecido	6.1
CVE-2022-0112	Chromium: Interfaz de usuario de seguridad incorrecta en la interfaz de usuario del explorador	Sin valor establecido	6.1
CVE-2022-0111	Chromium: Implementación inadecuada en la navegación	Sin valor establecido	6.1
CVE-2022-0110	Chromium: Interfaz de usuario de seguridad incorrecta en Autofill	Sin valor establecido	6.1

CVE-2022-0109	Chromium: Implementación inadecuada en Autocompletar	Sin valor establecido	6.1
CVE-2022-0107	Chromium: Uso después de la liberación en la API del Administrador de archivos	Sin valor establecido	6.1
CVE-2022-0096	Chromium: Uso después de la liberación en el almacenamiento	Sin valor establecido	6.1
CVE-2022-0105	Chromium: Uso gratis en PDF	Sin valor establecido	6.1
CVE-2022-0104	Chromium: Desbordamiento del búfer del Heap en ÁNGULO	Sin valor establecido	6.1
CVE-2022-0103	Chromium: Uso después de la liberación en SwiftShader	Sin valor establecido	6.1
CVE-2022-0102	Chromium: Confusión de tipos en V8	Sin valor establecido	6.1
CVE-2022-0101	Chromium: Desbordamiento del búfer del Heap en marcadores	Sin valor establecido	6.1
CVE-2022-0100	Chromium: Desbordamiento del búfer del Heap en Media Streams API	Sin valor establecido	6.1
CVE-2022-0099	Chromium: Uso después de la liberación en el inicio de sesión	Sin valor establecido	6.1
CVE-2022-0098	Chromium: Usar después de gratis en Captura de pantalla	Sin valor establecido	6.1

CVE-2022-0097	Chromium: Implementación inapropiada en DevTools	Sin valor establecido	6.1
CVE-2022-0118	Chromium: Implementación inapropiada en WebShare	Sin valor establecido	6.1
CVE-2022-0106	Chromium: Usar después de la liberación en Autocompletar	Sin valor establecido	6.1
CVE-2022-0120	Chromium: Implementación inapropiada en contraseñas	Sin valor establecido	6.1

4. MITIGACIÓN / SOLUCIÓN

Para solucionar las vulnerabilidades, Microsoft ha publicado las actualizaciones de seguridad pertinentes. Se recomienda revisar las notas sobre la publicación de este mes y la guía de actualización.

5. REFERENCIAS ADICIONALES

- January 2022 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The January 2022 Security Update Review

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?