


Control de la seguridad digital

Configuración básica de equipos



CONFIGURACIÓN BÁSICA DE EQUIPOS

En la siguiente tabla se describe paso a paso la configuración de cada uno de los equipos más usados para la protección de los sistemas en las entidades.

EQUIPO / HERRAMIENTA	CONFIGURACIÓN
Llaves U2F	<p>REGISTRO (Verificación en dos pasos de Google)</p> <ol style="list-style-type: none"> 1. Inicie sesión con de <i>google Chrome</i> en una computadora. 2. Haz <i>click</i> en "Mi cuenta" -> "Inicio de sesión y seguridad" -> "Verificación en dos pasos". 3. Haga <i>clic</i> en "Agregar clave de seguridad" y siga las instrucciones para completar el registro. 4. Se le informará que inserte su llave de seguridad <i>ePass FIDO®</i> durante el proceso de registro. 5. Haga <i>clic</i> / toque el botón para comprobar la presencia del usuario cuando el indicador de autenticación parpadee. Su registro se completará en un momento. <p>REGISTRO (Programa de protección avanzada de Google)</p> <ol style="list-style-type: none"> 1. Acceso: página de inicio de Programa de protección avanzada con un Navegador Chrome:  Enlace web. https://landing.google.com/advancedprotection/ 2. Haz <i>click</i> en "¡EMPIEZA YA!". Prepares 2 llaves de seguridad y haga clic en "TENGO 2 3. LLAVES DE SEGURIDAD". Se le pedirá que ingrese la contraseña otra vez. 4. Registre la clave de seguridad una por una y haga <i>clic</i> en "CONTINUAR". 5. Lea y confirme las notificaciones sobre el Programa de protección avanzada y haga <i>clic</i> en "ENCENDER". Su registro se completará en un momento.
Firewall por hardware	<p>CONEXIÓN CON WAN</p> <ol style="list-style-type: none"> 1. Deshabilitar todas las conexiones a internet. 2. Conecte por el puerto <i>LAN</i> del computador a un puerto <i>LAN</i> del equipo.

	<ol style="list-style-type: none"> Abra el navegador y digite: http://setup.meraki.com (No debe estar conectado a internet). Click en <i>Uplink</i> configuration en la pestaña <i>Local status</i>. Los datos de acceso están por defecto: Usuario – Numero de serial del equipo; Contraseña – Espacio en blanco. En la opción de asignación IP, seleccionar <i>Static</i>. Ingrese la dirección IP, la máscara de <i>subred</i>, la IP de la puerta de enlace predeterminada y la información del servidor DNS.
Router VPN – VPN Box	<p>INSTALACIÓN DEL HARDWARE</p> <ol style="list-style-type: none"> Compruebe que usted tiene una conexión a Internet. Apague su cable <i>módem</i> o DSL. Desconecte el cable de red de su Cable o DSL <i>módem</i> y de su PC. Conecte un extremo del cable de red a uno de los puertos LAN de TW100-BRV214. Conecte la otra punta del cable al puerto Ethernet del PC. Conecte un extremo del cable de red al puerto WAN de TW100-BRV214. Conecte el otro extremo del cable a su módem. Conecte el adaptador de alimentación AC al TW100-BRV214 y luego a una toma de corriente. Presione el botón de encendido para llevarlo a la posición de encendido. Encienda su cable <i>módem</i> o DSL Espere hasta que los LED indiquen que el <i>módem</i> se ha reiniciado por completo. Consulte la guía de usuario del <i>módem</i> para más información. Compruebe que las siguientes luces del panel están encendidas: Estado (verde), LAN el puerto (1,2,3,4) (verde) y WAN (verde). Abra el navegador Web, introduzca http://192.168.10.1 en la barra de direcciones, luego pulse la tecla <i>Enter</i> (Intro). Introduzca la <i>System Password</i> (contraseña del sistema), y luego haga clic en <i>Login</i> (Inicio). Por defecto: <i>System Password</i> (Contraseña del sistema): admin.

	<ol style="list-style-type: none"> 11. Seleccione <i>Wizard</i> (Asistente de instalación) y después haga <i>clic</i> en <i>Enter</i> (Intro). 12. Siga las instrucciones del asistente para completar la configuración. Haga <i>clic</i> en <i>Apply Settings</i> (Aplicar opciones de configuración). 13. Abra su navegador y escriba un URL (Ej. www.trendnet.com) para comprobar que tiene conexión a Internet.
Hardware de cifrado	<p>INSTALACIÓN DEL HARDWARE</p> <ol style="list-style-type: none"> 1. Basado en el rendimiento “listo para usar” con una placa base SATA Rev. 3.0. La velocidad puede variar según el tipo de <i>hardware</i> que aloja al dispositivo, el <i>software</i> y el uso. IOMETER de lectura/escritura aleatoria de 4K se basa en particiones de 8 GB. 2. Algunas de las capacidades enumeradas en un dispositivo de almacenamiento <i>Flash</i> se emplean para formatear y otras funciones, por lo cual no están disponibles para el almacenamiento de datos. Por esta razón, la capacidad real de almacenamiento de datos es inferior a la indicada en los productos. Consulte información más detallada en la Guía de memoria <i>Flash</i> de <i>Kingston</i>, en kingston.com/flashguide. 3. Garantía limitada basada en cinco años o “Vida remanente de la SSD”, que puede consultarse utilizando el 4. Administrador de SSD de <i>Kingston</i> (Kingston.com/SSDManager). Un producto nuevo y sin usar mostrará un valor indicador de desgaste de cien (100), mientras que un producto que haya alcanzado el límite de ciclos de borrado del programa mostrará un valor indicador de desgaste de uno (1). Consulte información detallada en kingston.com/wa. El total de <i>bytes</i> escritos (TBW) procede de la carga de trabajo de cliente JEDEC (JESD219A)
Tokens PKI	<p>INSTALACIÓN</p> <p>La descarga e instalación del middleware se detalla en los</p>

	<p>manuales de Soporte Técnico eFirma que se encuentra a disposición de descarga en los siguientes links:</p> <p>Manual de descarga e instalación:</p> <p> Enlace web. https://efirma.com.py/descargas/Instalaciontoken_ME_bit4id.pdf</p> <p>Video explicativo:</p> <p> Enlace web. https://www.efirma.com.py/descargas/configuracion_token_ME_Bit4id.mp4</p> <p>Software “Administración de tokens”</p> <ol style="list-style-type: none"> 1. Una vez instalado el <i>Middleware</i> Bit4id PKI Manager al ingresar en el menú “Inicio” ya se podrá observar el ícono del <i>software</i> “Bit4id – PKI Manager”. 2. Se abrirá la ventana “Bit4id – PKI Manager” con el cual el usuario podrá acceder a todos los recursos y las claves de activación del <i>token</i>. Inicialmente el cuadro se encontrará vacío. 3. Al insertar el módulo criptográfico (<i>token</i>) en el puerto USB de la terminal, aparecerá en la pantalla la etiqueta del <i>token</i> e ingresando en la opción “Iniciar sesión” podemos ingresar el PIN del <i>Token</i> y así tener habilitado todas las opciones de la administración del <i>token</i>.
Acelerador SSL/TLS	<ol style="list-style-type: none"> 1. Scan: Ingrese al <i>host</i> que va a escanear y el puerto apropiado. 2. Clear: Limpie los resultados. 3. Option - Solo mostrar conjuntos de cifrado admitidos. 4. Experimental: Huellas dactilares de motor <i>SSL engine</i> (ver “<i>Fingerprint</i>” Experimental).
Sistema de pago seguro	<ol style="list-style-type: none"> 1. Autenticación: el ingreso al sistema de información se debe realizar a través del portal de aplicaciones SEBRA (que hace parte de la plataforma SEBRA). En este portal, el proceso de autenticación fuerte es de múltiple factor (pin definido por el usuario y token OTP-One time Password). Luego de completar la autenticación en

SEBRA, se habilita a través de este el acceso del usuario hacia el CUD mediante un mecanismo de *single-sign-on* (SSO).

2. **Control de acceso y autorización:** existen dos fases de control de acceso: la primera ya descrita en el anterior ordinal a través del portal SEBRA, y la segunda fase, se realiza al ingresar al sistema CUD a través de su integración con el sistema S3 donde el acceso a las funciones o pantallas está controlado según los roles y perfiles que el delegado de la Entidad Participante haya configurado para el usuario (únicamente se pueden ejecutar las funciones autorizadas por los roles y/o perfiles).
3. **Integridad y confidencialidad:** la comunicación entre los usuarios y el aplicativo se realiza usando protocolos seguros de comunicación (en este caso https con TLS versión X).
4. **Observancia:** Las principales acciones de los usuarios, desde la autenticación inicial hasta la captura y aprobación de transferencias de fondos, son almacenadas en tablas de la base de datos del sistema cuya información no puede ser modificada debido a los controles de cambio de datos implementados a través de herramientas de monitoreo, alerta y protección de bases de datos (tecnologías de *Database Security*) del Banco de la Republica.
5. **Trazabilidad de las transacciones realizadas en el CUD:** Desde el momento en que se autentica en el sistema, a través del proceso de *single-sign-on* desde el portal SEBRA, el usuario es almacenado en una tabla que registra las acciones de los usuarios con un registro de inicio de sesión.
6. **Registro:** Los registros de operación de los servicios involucrados en el Portal SEBRA, Servicio de autenticación fuerte y S3 son conservados en una herramienta de industria que el Banco maneja para este fin.
7. **No repudio:** debido a que todas las acciones realizadas

	<p>por los usuarios están completamente registradas y protegidas por los esquemas de observancia y auditoría ya descritos, las transacciones hechas a través del sistema cuentan con evidencia digital suficiente para evitar el repudio de estas.</p>
Cartera digital	<p>INGRESO</p> <ol style="list-style-type: none"> 1. Para realizar el ingreso al servicio de Carpeta Ciudadana Digital, se abre la URL “gov.co”, en la parte superior derecha aparece el botón que direcciona al servicio. 2. Al ingresar a “Carpeta Ciudadana” se dirige a página de entrada para el servicio donde se tienen dos opciones, la primera es realizar el ingreso y la segunda para registrar el usuario en el servicio de autenticación digital. 3. Al dar <i>clic</i> en el botón “Iniciar sesión”, se direcciona al usuario al formulario de autenticación para el acceso al servicio de Carpeta Ciudadana Digital.
Sensores biométricos	<p>IDENTIFICACIÓN/VERIFICACIÓN DE USUARIO</p> <p>Es el proceso de comparar la huella que lee el equipo con las huellas almacenadas, luego la identificación de la huella o plantilla correspondiente y finalmente la verificación del usuario que la registró.</p> <p>Tipo de autenticación</p> <ol style="list-style-type: none"> 1. Autenticación (Verificación) 1:1. De este modo, ingrese un número de ID de usuario y luego la huella dactilar correspondiente. Las huellas dactilares asociadas al número de ID serán comparadas 1-1 con la huella leída. Esta autenticación 1-1 tarda un muy breve período de tiempo sin importar el número de usuarios registrados. No hay necesidad de hacer modificaciones especiales en la configuración del sistema. 2. Autenticación (Identificación) 1:N. En este modo, sólo es necesario que el usuario ponga su huella dactilar en el sensor del equipo. Aunque el procedimiento de la autenticación es simple, este método durará un poco más



	<p>de tiempo que la autenticación 1.1 si hay muchos usuarios registrados. No hay necesidad de hacer ningún ajuste especial en la configuración del sistema.</p> <p>Autenticación por Clave. Una clave de 1-5 dígitos de largo puede ser usada para validar una autenticación de acceso. Ud. Puede usar este método en casos especiales, como cuando las huellas de un trabajador están muy deterioradas, o el sensor del equipo esté dañado.</p>
Candado Kensington	<ol style="list-style-type: none"> 1. Conecte el extremo de llave del cable al puerto de candado del laptop. 2. Manipule la llave del candado hasta que esté fija en el <i>laptop</i> y no se pueda soltar. 3. Extienda el cable del candado hasta la distancia deseada. 4. Conecte el otro extremo del cable al lugar donde se va fijar. 5. Realice pruebas en cada extremo, para asegurarse que quedó bien instalado y el cable no se suelta.