Reseña técnica sobre DocuSign eSignature

El Grupo Banco Mundial (GBM) utiliza **DocuSign eSignature** como su solución de firma electrónica. DocuSign permite enviar y firmar documentos en forma electrónica, de manera conveniente y segura desde cualquier computadora o dispositivo móvil.

1. **Breve descripción del procedimiento de firma**
   - DocuSign eSignature es un sistema de *software* como servicio (SaaS) basado en la nube.
   - El método más común para reunir firmas en DocuSign es a través del correo electrónico, en el que el sistema DocuSign envía a cada firmante un mensaje de correo electrónico que contiene un enlace seguro al sobre que este debe firmar.
   - En el caso de los documentos enviados por el GBM, si el firmante está registrado en DocuSign, debe iniciar sesión (nombre de usuario y contraseña o, si la organización del firmante utiliza el servicio de inicio de sesión único [SSO]) para acceder al documento y firmarlo. Si no está registrado en DocuSign, solo debe hacer clic para acceder al documento y firmarlo.
   - No reenvíe los mensajes de correo electrónico enviados por DocuSign. Están dirigidos exclusivamente al destinatario del mensaje. Los códigos de acceso y los métodos de verificación de la identidad pueden reducir la posibilidad de que destinatarios no previstos accedan a los documentos y actúen en consecuencia.
   - Existe una Divulgación de Registros y Firmas Electrónicas específica (redactada por los departamentos jurídicos del Banco Internacional de Reconstrucción y Fomento [BIRF], la Corporación Financiera Internacional [IFC], el Organismo Multilateral de Garantía de Inversiones [MIGA] y el Centro Internacional de Arreglo de Diferencias Relativas a Inversiones [CIADI]) que los firmantes deben aceptar para acceder al documento y firmarlo en forma electrónica.

2. **Información técnica y en materia de seguridad**
   - Los documentos enviados por el GBM están cifrados (cifrado AES-25 bits para los últimos métodos aprobados de conformidad con los Estándares Federales de Procesamiento de la Información [FIPS]) por dispositivos de seguridad instalados en nuestros centros de datos y protegidos por los cortafuegos corporativos. Esto implica que el proveedor, DocuSign, no puede acceder en ningún momento a los documentos que el GBM envía.
   - DocuSign utiliza tecnología de infraestructura de clave pública (PKI) con certificados que cumplen con el estándar X.509. Una autoridad de certificación garantiza la seguridad de la clave. El Banco Mundial no mantiene ni guarda ninguna clave para la firma y no almacena datos para registrar la identidad de los individuos.
   - En lo referente a la retención de los documentos, el GBM ha optado por eliminar los documentos de la nube del proveedor al cabo de 90 días. Después de ese período, todos los documentos son eliminados de DocuSign. Todos los documentos firmados se almacenan en el sistema de registros institucionales del GBM, y se gestionan de conformidad con la política de retención y eliminación, en lugar de permanecer en la nube del proveedor.
   - Para obtener información acerca de la seguridad de DocuSign eSignature visite el Centro de confianza en su sitio web.
     - DocuSign eSignature se basa en tecnología PKI con certificados X.509.

- DocuSign cumple con la norma ISO 27001 y la normativa SOC 1 tipo 1 y SOC 2 tipo 2, y las normas de seguridad de los datos (DSS) para el sector de tarjetas de pago (PCI).
- DocuSign cumple con el Reglamento General de Protección de Datos (RGPD).

- DocuSign se ajusta a las mejores prácticas de la industria para separar de manera lógica los datos de los clientes individuales y para cifrar los datos de los clientes. En todas las actividades de acceso y transferencia de datos se utiliza el protocolo HTTPS y otros protocolos seguros, como SSL, SSH, IPsec, SFTP, o la firma y marca en un canal seguro.
- Los destinatarios pueden solicitar un nivel adicional de seguridad en torno a la firma mediante el uso de un código de acceso, como una contraseña válida una sola vez, que se debe ingresar antes de acceder al documento y firmarlo. Los códigos de acceso permiten, de manera sencilla, proporcionar un nivel más alto de confidencialidad y no repudio. Solo el remitente del documento y la persona que lo firma conocen el código de acceso, que se debe compartir fuera de DocuSign.
- Las organizaciones destinatarias pueden incluir los dominios y las direcciones de IP de DocuSign en una lista blanca.
- Además, los destinatarios pueden implementar la funcionalidad de búsqueda del marco de políticas del remitente (SPF) y el mecanismo de autenticación de mensajes, informes y conformidad basada en dominios (DMARC) para impedir la suplantación de identidad (*phishing*).

3. Tipos de firmas

- Por defecto, DocuSign utiliza la firma de su plataforma para firmar todos los documentos PDF que se descargan de su sistema con un certificado digital que cumple con el estándar X.509 emitido por Entrust.
  - Esta es la firma básica o la **firma electrónica estándar**. El PDF se firma utilizando la firma de la plataforma de DocuSign y se incluye el texto “Firmado por DocuSign, inc.”. La información sobre no repudio y sobre el firmante se basa en un documento resumido separado, y en el registro de auditoría se indica quién firmó y cuándo y cómo lo hizo, sobre la base de la autenticación del correo electrónico.

4. Autenticidad, integridad y no repudio

- Cuando se utilizan firmas estándar, DocuSign firma el PDF con la firma de su plataforma para proporcionar una marca inviolable. Cualquier modificación del documento se consignará en el panel de firmas del *software* de PDF que se utilice.
- En forma adicional, en un documento resumido y un registro de auditoría, que DocuSign denomina “certificado de finalización”, se enumeran todos los eventos relacionados con la transacción de firma (quién firmó, cuándo y cómo lo hizo, etc.). Esta información se proporciona a todos los destinatarios incluidos en el proceso. Cualquier modificación del documento se consignará en el panel de firmas del *software* de PDF que se utilice.