SUPERINTENDENCIA
DE BANCOS
REPÚBLICA DOMINICANA

TÉRMINOS DE REFERENCIA

ADQUISICION DE PLATAFORMA DE MANEJO DE ARCHIVOS DE MANERA SEGURA PARA LA SUPERINTENDENCIA DE BANCOS.

Levin David Torres Rodríguez	Juan Daniel Pujols
Encargado de División de Seguridad de la Información	Subdirector de Seguridad de la Información
Firma:	Firma:

1. PLANTEAMIENTO DE LA NECESIDAD

En la Superintendencia de Bancos, las transferencias de archivos de un lugar a otro son esenciales para la institución. Actualmente existen transferencias de archivos a lo interno de la Superintendencia de Bancos, así como a lo externo, donde se intercambian datos e información con instituciones gubernamentales y en casos especiales con entidades financieras, para ejecutar los distintos procesos. Los sistemas utilizados para las transferencias de archivos son manejados de manera individual para los diferentes casos, utilizando mecanismos que ofrecen medidas de protección de la confidencialidad de los datos en la transmisión de los archivos, sin embargo, carecen de otros controles como la garantía de entrega de los archivos, retomar la transferencia en el punto que se quedó si ocurre un fallo, etc. Con los procesos de digitalización y modernización de la Superintendencia de Bancos se espera que los casos de uso de transferencias de archivos aumenten, por lo que se hace necesaria la adquisición de una plataforma de transferencia gestionada de archivos (MFT) que ayude a la Superintendencia de Bancos a satisfacer todos los aspectos de la transferencia de archivos entrantes y salientes.

2. OBJETIVOS

2.1. Objetivo General

El objetivo de la adquisición de la plataforma de transferencia gestionada de archivos (MFT) es centralizar, automatizar, simplificar y agilizar las transferencias de datos, ya sea en toda la organización, dentro de una red privada o a usuarios externos.

2.2. Objetivos específicos

- Centralizar, simplificar y automatizar los movimientos de datos de una forma segura dentro y fuera de la empresa, y poder acelerar los movimientos de big data.
- Ofrecer una estrategia de seguridad preventiva con supervisión en tiempo real, y políticas y controles de seguridad de validación para proteger los datos en tránsito o en reposo.
- Ofrecer capacidades avanzadas y soporte para múltiples plataformas, dispositivos móviles, aplicaciones y otras infraestructuras de TI existentes.
- Obtener visibilidad operativa sobre los movimientos de los archivos que conduzca a la resolución proactiva de problemas, como las transferencias fallidas y la mejora del cumplimiento de los compromisos de los SLA.

3. Especificaciones de Plataforma de Transferencia Gestionada de Archivos

Requerimos las licencias necesarias para implementar la plataforma de transferencia gestionada de archivos en la Sede Principal y el Site Alterno de la Superintendencia de Bancos.

Las funcionalidades requeridas de la plataforma de transferencia gestionada de archivos (MFT) son:

3.1. Auditoría e informes

Los registros de auditoría ayudan a supervisar la actividad en el entorno para todo el movimiento de archivos. Las métricas de los informes proporcionan detalles estadísticos, gráficos y tablas de esta actividad.

- Auditoría
  - Audita la actividad de inicio de sesión de los usuarios
  - Genera registros de las acciones del administrador
  - Registra los intentos no autorizados
  - Registra toda la actividad de las cuentas de los socios comerciales
  - Almacenamiento en la base de datos de las entradas del registro de auditoría
  - Alimentación opcional de SYSLOG de los registros de auditoría
  - Puede archivar automáticamente las entradas de auditoría antiguas
  - Período de retención personalizable
  - Supervisión en tiempo real de las sesiones activas
  - Alertas por correo electrónico en caso de intentos de inicio de sesión no válidos
  - Visualización de los registros de auditoría desde el panel de control basado en el navegador
  - Filtrar los resultados por usuario, fecha, hora, IP, etc.
  - Centrarse en determinadas actividades (por ejemplo, descargas, subidas, etc.)
  - Seleccionar qué columnas mostrar/ocultar
  - Ordenar las columnas por usuario, fecha, hora, etc.
  - Exportar las entradas de auditoría filtradas en formato CSV
- Informes
  - Generar informes de gestión y analíticos en formato PDF
  - Cree informes personalizados basados en datos de una base de datos, Excel, XML, JSON o archivos planos
  - Filtros personalizados, incluyendo rangos de fechas
  - Programar informes para que se ejecuten en fechas y horas futuras
  - Ejecutar informes bajo demanda y visualizarlos en el navegador
  - Distribuir los informes por correo electrónico o almacenarlos en el servidor

3.2. Operabilidad desde el navegador y el móvil

La plataforma debe ofrecer una interfaz basada en el navegador que permita realizar transferencias de archivos a través de HTTPS. Además, ofrecer un buen soporte móvil, que permita comprobar las métricas de transferencia de archivos y la actividad del sistema sobre la marcha desde cualquier dispositivo, incluyendo tablets y smartphones.

- Navegadores soportados
  - Microsoft Edge
  - Mozilla Firefox
  - Google Chrome
  - Apple Safari
- Transferencias de archivos adhoc
  - Cliente web HTML 5 basado en navegador para transferencias de archivos adhoc
  - Cliente web de applet opcional para transferencias de archivos mejoradas
  - Selección múltiple de archivos y carpetas
  - Menús de clic derecho sensibles al contexto
  - Arrastrar y soltar archivos para cargar y descargar
  - Seguimiento del progreso de las transferencias
  - Cola para procesar un gran número de transferencias
  - Verificación de la integridad de los archivos
  - Soporte de archivos de gran tamaño
  - Cambia la marca del cliente web con un logotipo, colores y fuentes personalizados
  - Descargo de responsabilidad y política de privacidad personalizables

3.3. Compatibilidad con la nube:

La solución debe ofrecer la flexibilidad de automatizar y asegurar las transferencias de archivos en la nube, independientemente de dónde residan esos archivos. Debe funcionar con plataformas como Amazon Web Services y Microsoft Azure.

3.4. Capacidades de correo electrónico seguro (alternativa de correo electrónico para el envío de archivos grandes o sensibles)

La solución debe ofrecer una forma segura de enviar correo electrónico que ayude a garantizar la seguridad de sus mensajes y archivos convirtiéndolos en paquetes encriptados. Estos paquetes pueden ser descargados a través de una conexión HTTPS protegida. Entre sus capacidades debe ofrecer:

- Cantidad de usuarios (5)
- Enviar correo seguro desde Outlook 2010 y posteriores
- Opción de envío de correo seguro mediante un formulario basado en el navegador
- Los archivos adjuntos se eliminan automáticamente y se almacenan de forma centralizada
- Puede enviar solicitudes de archivos que permitan a los destinatarios cargar archivos
- Se generan enlaces HTTPS para cada paquete de correo seguro
- Opción de caducar el paquete después de un número X de días
- Opción de limitar el número de descargas
- Protección por contraseña opcional
- Plantillas personalizables para las notificaciones por correo electrónico

- El remitente puede recuperar los paquetes
- El remitente puede recibir notificaciones cuando los paquetes son leídos
- Limpieza automática de paquetes caducados
- Control local de los paquetes de correo seguro (no alojados)

3.5. Colaboración

La solución debe ofrecer funciones que apoyen y mejoren las capacidades básicas de MFT como:

- Cantidad de usuarios (5)
- Sincronización e intercambio de archivos de empresa
- Arrastrar y soltar archivos y carpetas desde el escritorio al servidor.
- Sincronizar archivos con ordenadores portátiles/desktops Windows y Mac
- Compartir archivos y carpetas con otros usuarios
- Especificar permisos granulares (por ejemplo, sólo lectura, edición, etc.) para las carpetas y archivos compartidos
- Recibir notificaciones automáticas por correo electrónico cuando otros usuarios accedan a las carpetas y archivos compartidos
- Ver imágenes y archivos PDF a través del navegador mediante el visor multimedia
- Añadir comentarios a los archivos y carpetas
- Buscar archivos o carpetas
- Conservar las revisiones de los archivos, con la posibilidad de restaurar las versiones anteriores
- Bloquear archivos para restringir temporalmente el acceso
- Restaurar archivos desde la papelera
- Miniaturas y vistas previas de imágenes
- Compatibilidad con dispositivos móviles para iPhone, iPad y Android

3.6. Conectividad

La plataforma debe permitir la conexión a una amplia variedad de servidores para realizar transferencias seguras de archivos de servidor a servidor y así mantener un único punto de control y administración con una solución centralizada y no invasiva. Entre los servidores a los que puede conectarse la plataforma se encuentran:

- Almacenamiento Azure Blob
- Servidores de bases de datos
- Servidores FTP
- Servidores FTPS
- Servidores HTTP(S)
- Servidores de correos
- Carpetas compartidas
- REST
- Servidores SCP
- Servidores SFTP

- Servidores SNMP

3.7. Amplios controles de seguridad

La solución debe ofrecer seguridad de nivel empresarial que ayude a cumplir con las políticas internas y requisitos de cumplimiento, así como tener funciones que protejan sus datos y restrinjan el acceso de los usuarios sólo a las áreas del producto que necesitan.

- Creación de cuentas de usuario
  - Creación de cuentas mediante plantillas
  - Importación de cuentas desde archivos CSV o XML
  - Autorregistro de cuentas con proceso de aprobación opcional
  - Permitir que los usuarios inviten a otros a registrarse
  - Crear cuentas a través de llamadas a la API desde aplicaciones externas
- Métodos de autenticación de usuarios
  - Directorio Activo (AD)
  - LDAP
  - SAML para el inicio de sesión único
  - Autenticación Kerberos para el cliente de escritorio de la plataforma
  - Base de datos de la plataforma
  - Certificados SSL
  - Claves públicas SSH
  - Autenticación de dos factores
- Seguridad de contraseñas
  - Política de seguridad de contraseñas (longitud mínima, caracteres especiales, etc.)
  - Aplicación de la antigüedad de la contraseña (número mínimo/máximo de días)
  - Historial de contraseñas (no permitir la reutilización de contraseñas anteriores)
  - Intervalos de caducidad de la contraseña (en días)
  - Notificaciones por correo electrónico de la caducidad de la contraseña
  - El administrador puede forzar el restablecimiento de la contraseña
  - El usuario puede cambiar su propia contraseña
- Seguridad de la cuenta de usuario
  - Autorizar servicios (SFTP, HTTPS, etc.) por usuario
  - Adoptar los permisos de usuario de los grupos
  - Configurar listas blancas de IPs (IPs permitidas) por usuario
  - Cerrar sesiones después de X segundos de inactividad
  - Expirar cuentas temporales en fechas específicas
  - Desactivar automáticamente las cuentas de usuario después de X intentos de inicio de sesión no válidos
  - Desactivar automáticamente las cuentas de usuario sin actividad en X días
  - Desactivar manualmente las cuentas de usuario

  - Limitar o desactivar el acceso anónimo
- Configuraciones y permisos de carpetas/archivos
  - Creación automática de carpetas mediante variables y/o constantes
  - Nombres de archivos y carpetas virtuales (alias de fácil uso)
  - Definidos a nivel de usuario, grupo y plantilla
  - Subcarpetas ilimitadas
  - Carga (escritura)
  - Descarga (lectura)
  - Listar
  - Sobrescribir
  - Anexar
  - Renombrar
  - Borrar
  - Crear subcarpeta
  - Subcarpeta Renombrar
  - Subcarpeta Borrar
- Cifrado
  - Cifrado de datos en tránsito mediante SSL, TLS o SSH
  - Encriptación de archivos en reposo mediante encriptación AES de 256 bits
  - Cifrado de archivos Open PGP y firma digital de archivos
  - Desencriptación de archivos PGP abiertos y verificación de firmas digitales
  - Cifrados fuertes: AES128, AES192, AES256, Triple DES
  - Soporte de cifrado heredado: DES, RC4, Blowfish
  - Configurar los cifrados permitidos para las conexiones de los clientes
  - Forzar canales de comandos encriptados
  - Soporte para SSL implícito y explícito
  - Algoritmos validados por FIPS 140-2 de RSA
- Gestión de llaves y certificados
  - Gestión de llaves basada en el navegador
  - Crear nuevas llaves Open PGP, claves SSH y certificados SSL
  - Importar llaves Open PGP, claves SSH y certificados SSL existentes
  - Exportar llaves Open PGP, claves SSH y certificados SSL
  - Asignar una o más claves SSH por usuario
  - Autorizar la función de gestión de claves sólo a determinados administradores
- Filtrado de IP
  - Listas negras y blancas de IP globales
  - Listas negras y blancas de IP a nivel de usuario
  - Monitorización de nombres de usuario maliciosos con lista negra automática
  - Monitorización de ataques DoS con lista negra automática
  - Monitorización de ataques de fuerza bruta con lista negra automática
  - Lista negra de IPs temporal y permanente
  - Alertas por correo electrónico sobre las IPs de la lista negra automática

3.8. Agentes remotos

La solución debe poder automatizar las transferencias de archivos y los flujos de trabajo en sistemas en toda la institución mediante agentes remotos, los cuales son gestionados por una implementación central del producto, permitiéndoles ejecutar procesos y transferencias en múltiples ubicaciones o con otras organizaciones, tanto en las premisas como en la nube, así como monitorear automáticamente las carpetas.

- Cantidad de agentes (5)
- Monitoreo de carpetas
    - Escanee las carpetas de red en busca de archivos nuevos, modificados o eliminados
    - Escanear servidores SFTP, FTP/s, Amazon S3 y Microsoft Azure Blob en busca de archivos nuevos, modificados o eliminados
    - Utilice patrones comodín o regex para buscar varios archivos
    - Configurar la frecuencia de escaneo y las horas del día
    - Garantizar la disponibilidad de los archivos mediante el bloqueo de los mismos o la comparación de las marcas de tiempo/tamaño
    - Enviar alertas por correo electrónico si faltan archivos

3.9. Gateway seguro DMZ

La solución debe mantener los servidores de intercambio de archivos dentro de tu red privada y lejos de la DMZ.

- Proxy inverso entrante
- Puede mantener los archivos sensibles en la red privada (fuera de la DMZ)
- Permite cerrar los puertos de entrada a la red interna/privada
- Puede servir opcionalmente como proxy saliente (hacia adelante)
- Un único gateway de seguridad DMZ puede dar servicio a múltiples sistemas
- La lista negra de IP se realiza en la DMZ

3.10. Compatibilidad con una gran variedad de protocolos

- SFTP - FTP sobre SSH
- SCP - Copia segura sobre SSH
- FTP estándar
- HTTP/s
- Correo electrónico (SMTP, POP3, IMAP)

3.11. Integración de la prevención de la pérdida de datos

La plataforma debe integrarse con la solución de prevención de pérdida de datos (DLP) McAfee MVISION DLP para poder detectar, inspeccionar y proteger los datos críticos en el correo electrónico, la web y la nube, así como minimizar el riesgo de pérdida accidental de datos, exfiltración de datos y ciberataques, además de reducir el impacto en las operaciones diarias.

3.12. Automatización

La solución MFT debe contar con automatización por lotes que permita determinar cuándo realizar las transferencias de archivos. Esta opción debe poder ejecutar múltiples transferencias simultáneamente, que se active cuando se complete otro proceso y que cuente con un planificador incorporado.

- Disparadores (triggers)
  - Cree disparadores basados en cargas, descargas, etc.
  - Condiciones de varios niveles utilizando IFs, ANDs y ORs
  - Expresiones complejas utilizando paréntesis
  - Condiciones de filtrado basadas en el usuario, el nombre del archivo, la carpeta, etc.
  - Enviar notificaciones por correo electrónico personalizadas
  - Lanzar programas y scripts externos con parámetros
  - Mover archivos
  - Copiar archivos
  - Renombrar archivos
  - Eliminar archivos
  - Ejecutar flujos de trabajo del proyecto
- Planificador
  - Ejecute trabajos de flujo de trabajo por minuto, hora, día, semana o mes
  - Reintento automático de trabajos fallidos
  - Utilice calendarios de vacaciones personalizados (omita los días festivos o ejecute el día anterior/posterior)
  - Alertas por correo electrónico sobre éxitos y fracasos
  - Pase de variables personalizadas a los flujos de trabajo
- Flujos de trabajo (workflow)
  - Diseñar flujos de trabajo (proyectos) mediante una interfaz gráfica basada en el navegador
  - No es necesario programar ni crear scripts
  - Ofrece más de 60 tareas diferentes que se pueden encadenar
  - Controla la ejecución con lógica condicional (If/Else)
  - El depurador permite ver/cambiar variables y omitir tareas
  - Historial de revisiones del proyecto y restauración de versiones anteriores
  - Organice y priorice los flujos de trabajo utilizando múltiples colas de trabajo
  - Ejecutar flujos de trabajo desde el administrador de la plataforma MFT o aplicaciones de terceros
  - Integrar desde Windows, Linux, Java, .NET, REST, etc.

3.13. Sistemas de archivos

- Sistema de archivos local
- Rutas UNC
- Unidades montadas (por ejemplo, NFS)

- Sistema de archivos local • Rutas UNC
- Unidades montadas (por ejemplo, NFS)

- Almacenamiento conectado a la red (NAS) • Red de área de almacenamiento (SAN)
- Unidades mapeadas
- Almacenamiento Blob de Microsoft Azure

3.14. Sistemas operativos compatibles

- Windows Server 2012, 2016 y 2019
- Windows 8 y 10
- Linux (Red Hat, SUSE, Ubuntu, CentOS, etc.) • Mac OS X

3.15. Administración

- Administración basada en el navegador (sin instalación en el PC)
- Acceso seguro a través de HTTPS
- Configuración y supervisión remotas
- Dominios para múltiples zonas de seguridad
- Panel de control intuitivo con enlaces rápidos, estadísticas y análisis
- Gadgets del panel de control con configuraciones y diseños personalizados
- Pantallas gráficas con asistentes de apuntar y hacer clic • Texto de ayuda sensible al contexto
- Separación de funciones (permisos basados en roles para los administradores)

3.16. Entrega garantizada

- Soporte para la reanudación automática del cliente / apéndice
- Suma de comprobación de la integridad de los archivos
- Algoritmos Mac de SHAI y MD5

3.17. Conectividad de entrada

- Banners de inicio de sesión personalizados
- Se permiten múltiples listeners
- Números de puerto configurables

Adquisición de Plataforma de Transferencia de Archivos Gestionada para la Superintendencia de Bancos.

- Se puede limitar el número de conexiones simultáneas
- Compresión para reducir los requisitos de ancho de banda
- Rechazar o aceptar archivos con determinadas extensiones • Redirigir el tráfico HITP a HTTPS

3.18. Capacitación

- Ofrecer capacitación oficial de la solución para 5 personas

SSB

4. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Propuesta de plataforma de Transferencia de Archivos Gestionada
- Metodología de trabajo de implementación de plataforma de Transferencia de Archivos Gestionada
- Cronograma de implementación de plataforma de Transferencia de Archivos Gestionada
- Plataforma de Transferencia de Archivos Gestionada de la Superintendencia de Bancos en funcionamiento

5. PERFIL PROFESIONAL:

- El proveedor de la plataforma de Transferencia de Archivos Gestionada debe tener al menos 5 años de experiencia en el mercado de seguridad implementando la solución.
- El proveedor de la plataforma de Transferencia de Archivos Gestionada debe proporcionar referencias sobre proyectos exitosos en clientes, presentando al menos 3 cartas de referencia de clientes donde haya sido implementada la solución.
- El proveedor debe proporcionar evidencia de liderazgo año tras año en plataforma de Transferencia de Archivos Gestionada para empresas, basada en datos independientes de la industria, tales como Data-Quadrant, G2 Grid, entre otras.
- El personal que estará implementando la plataforma debe presentar evidencia de que está capacitado para realizar las tareas necesarias de la implementación mediante certificados oficiales de la solución.