Mejores Prácticas en Seguridad Digital para Banca Online y Conectividad de Archivos

La mejor defensa se conoce como una "defensa en capas", que debe ser creada mediante la utilización de las mejores prácticas de la industria, los servicios del mercado financiero y la aplicación de la ley

Checklist para una defensa en capas:

Protección Perimetral

- Garantizar una conectividad segura entre terceros utilizando firewalls y cifrado
- Restringir el acceso a sistemas sensibles (por ejemplo, banca online, Enterprise Resource Planning (ERP) y los sistemas de gestión de tesorería)
- Realizar evaluaciones de vulnerabilidad para identificar y mitigar proactivamente las debilidades
- Utilizar herramientas anti-virus y anti-phishing filtrando correos electrónicos y enlaces sospechosos

Gestión de Transacciones

- Restringir los privilegios para funciones de alto riesgo tales como la iniciación de transacciones, los cambios de beneficiarios, las cuentas corporativas y los datos confidenciales dentro de la organización
- Crear límites de autorización y separación de derechos para transacciones de alto valor (por ejemplo, hasta 9 niveles de aprobación en CitiDirect BE®)
- Establecer controles para compartir y modificar archivos, mensajes y otros datos (por ejemplo, el monitoreo de los datos que salen de su empresa)
- Estar atentos al revisar los detalles de la transacción antes de enviarla a procesar

Gestión de Acceso

- Nunca dejar una sesión activa desatendida
- Cerrar la sesión al finalizar cada sesión de CitiDirect BE®
- Nunca compartir sus credenciales de acceso o anotar el PIN, especialmente en la parte posterior de los tokens físicos
- Utilizar contraseñas seguras o autenticación multifactor para proteger dispositivos y aplicaciones empresariales

Gestión de Procesos

- Crear y promover capacitación sobre fraude y los procedimientos del negocio
- Actualizar regularmente el software y los dispositivos de la empresa (por ejemplo, sistema operativo, navegadores, Java y Adobe Flash)
- Seguir los estándares de conectividad y cifrado de Citi al realizar el onboarding en CitiConnect
- Asegurarse que las políticas de la empresa estén vigentes y sean respetadas para lo referente a retención de datos, su almacenamiento y privacidad
- Rotar o requerir la ausencia obligatoria del personal en asignaciones sensibles o financieras
- Informar cualquier actividad sospechosa a su equipo de Seguridad de la Información o a Citi (por ejemplo, modificación de URL de Citi, correos electrónicos de phishing, llamadas de ingeniería social que afirman pertenecer a una fuente Citi, etc.)

Reconciliación y Respuesta

- Realizar una reconciliación diaria e intradía de las cuentas utilizando múltiples medios
- Validar periódicamente la información de los proveedores
- Revisar regularmente los reportes y tableros de control de las transacciones y llevar a cabo auditorías de usuarios
- Aprovechar los recursos internos de fraude para monitorear pagos sospechosos
- Emitir alertas y recordatorios al personal sobre lo que deben hacer en caso de un incidente real o potencial
- Documentar procesos de recuperación de transacciones y realizar pruebas periódicas de respuesta

Treasury and Trade Solutions
transactionservices.citi.com

GRA27735 01/2017