



Mejores prácticas de Seguridad en CitiDirect BE

En Citi, la seguridad de nuestros clientes es muy importante. Ya que existen personas con intenciones maliciosas que siguen intentando obtener acceso no autorizado a la información, nos gustaría destacar algunas de las mejores prácticas recomendadas para su uso, para ayudar a garantizar que Usted esté seguro.

Para mantener el nivel más alto de seguridad, es imperativo que revise periódicamente sus controles:

- CitiDirect BE contiene hasta nueve niveles de aprobación. Se recomienda que su organización configure uno o más niveles de aprobación.
- Asegúrese que las transacciones de alto riesgo o de alto valor atraviesen la mayor cantidad de procesos de aprobación.
- Aproveche las plantillas o preformatos de CitiDirect BE para asegurarse que Usted está pagando a beneficiarios conocidos y pre-aprobados.
- Monitoree la actividad de la cuenta de alto riesgo como ser, los intentos de cambio de los detalles de la cuenta bancaria del beneficiario. Estos intentos fraudulentos, si son exitosos, pueden resultar en la pérdida de sus fondos.

Si precisa asistencia para implementar las mejores prácticas mencionadas anteriormente, utilice el módulo de capacitación del Client Academy o contacte a su representante de servicio al cliente de Citi.

Tenga cuidado con los ataques de Ingeniería Social

La Ingeniería Social involucra a criminales que obtienen acceso no autorizado a su información y/o cuentas a través de la manipulación y el engaño. El objetivo de la Ingeniería Social

es permitir que un usuario no autorizado cometa fraude, espionaje industrial o robo de identidad, o que simplemente ingrese forzosamente a una red para poder alterar los sistemas y las aplicaciones.

En lugar de *hackear* sistemas, los ingenieros sociales intentan obtener información a través del engaño. Utilizan presas con características típicas de la naturaleza humana, como por ejemplo el deseo de ayudar, la tendencia a confiar en la gente, y el temor a meterse en problemas. Los ingenieros sociales utilizan una serie de métodos muy diversos, por lo que es muy importante que Usted esté consciente de los mismos.

Citi ha recibido informes de inteligencia empresarial advirtiéndole que ha habido algunos incidentes donde los ingenieros sociales se hacen pasar por empleados del banco, representantes de servicio al cliente o del sistema de pagos. **Por favor tome nota que Citi jamás lo llamará de manera espontánea para pedirle sus credenciales de banca electrónica tales como los números de identificación personal (PINs), contraseñas o cualquier otra información de seguridad.** Si Usted recibe cualquier llamada sospechosa (no solicitada o inesperada en donde la persona que llama requiere información), por favor contacte inmediatamente a su Security Manager o a su representante de servicio al cliente de Citi.

Aproveche CitiDirect BE Mobile

Usted puede utilizar CitiDirect BE Mobile para aprobar pagos y consultar sus saldos diarios cuando esté haciendo uso del roaming. Las alertas también se pueden establecer para transacciones de alto volumen o cuando se alcanzan los límites de saldo.

Nunca comparta su tarjeta SafeWord

Las tarjetas SafeWord o tokens no deben ser compartidos. Compartir una tarjeta SafeWord aumenta el riesgo de fraude. Recuerde que, como Usted ha acordado mantener la tarjeta SafeWord para su uso personal, cualquier transacción realizada con esa tarjeta le será atribuida. El mecanismo de seguridad clave de CitiDirect BE está pensado para distinguir entre la persona ingresando una transacción y el autorizador de la transacción. Si las tarjetas SafeWord se comparten, se hace más fácil que una persona pueda ingresar y también autorizar una transacción.

Mantenga su PIN confidencial

De igual forma, es muy importante mantener su PIN de manera confidencial. Su PIN es la primera línea de defensa contra alguien que está utilizando su tarjeta SafeWord para ingresar o autorizar una transacción en su nombre. Trate su PIN de la misma manera que trataría el PIN de su cuenta bancaria personal y no lo guarde en una ubicación visible como ser el envoltorio de la tarjeta. Tome nota que el PIN de su tarjeta SafeWord puede ser cambiado y Citi recomienda que los usuarios cambien su PIN periódicamente.

Elimine Ex Empleados

Asegúrese que cuando un empleado deja la empresa o cambia de puesto sea eliminado del sistema y que su tarjeta SafeWord también sea eliminada. Es importante que las tarjetas no sean reasignadas a nuevos usuarios. También tenga en cuenta que los usuarios pueden configurarse para que venzan automáticamente en una fecha futura de forma tal que las tarjetas no sean usadas inapropiadamente.

Revise Privilegios

Ejecute revisiones periódicas de los usuarios y sus privilegios dentro del sistema para asegurarse que el acceso se encuentre al corriente y alineado con la descripción de tareas, y que la segregación de roles esté vigente. Se recomienda ampliamente que las actividades de gestión de IDs de usuarios, la iniciación, autorización y el control de las transacciones no sean realizados por la misma persona. Asegúrese que

el usuario de CitiDirect BE haya recibido tanto su tarjeta SafeWord como su PIN antes de habilitarlo en el sistema. Los usuarios que están fuera de la oficina por periodos prolongados (por ejemplo vacaciones, licencias extendidas, etc.) deben ser inhabilitados hasta que regresen a la oficina.

Otros consejos

Los informes intraday pueden ser utilizados para supervisar la iniciación de transacciones durante sus días hábiles; Automated File y Reports Delivery (AFRD) puede ser usado para automatizar la generación y entrega de estos informes.

Las Mejores Prácticas en su PC

- Sólo instale aplicaciones y software de compañías reconocidas en las que Usted confíe.
- Instale software anti-virus, anti-spyware y de detección de malware – una manera de defenderse contra los ataques a su computadora es utilizar software preventivo. Necesitará actualizar el software periódicamente para protegerse contra nuevos riesgos, por lo que recomendamos configurarlo para que realice actualizaciones automáticas.
- Utilice un bloqueador de pop-ups – configure sus preferencias de su navegador de internet para que bloquee pop-ups. Además de ser molestos, estos pop-ups pueden desplegar contenidos inapropiados o tener intenciones maliciosas.
- Cierre la sesión – asegúrese de cerrar la sesión y de salir del navegador de internet o de cerrar la ventana de su navegador una vez que haya terminado de utilizar CitiDirect BE.
- Actualizar – mantenga su navegador de internet y el Java plug-in actualizado a su versión más reciente.
- Protégase con una contraseña – Asegúrese que los dispositivos (computadoras personales, desktops, laptops, etc.) que hayan utilizado para acceder a CitiDirect BE estén protegidos por una contraseña.

Además, es probable que Usted necesite que su departamento de IT se involucre para brindarle las mejores prácticas de uso de su PC y que realicen análisis de riesgos junto con controles de evaluación periódicos.

Por favor, si Usted nota actividad sospechosa en su cuenta, si experimenta incidentes relacionados con la seguridad de la información, o si tiene alguna inquietud acerca de la seguridad en Citi, contacte a su representante de servicio a clientes de Citi inmediatamente.