Lineamientos: Terminales de áreas financieras entidades públicas

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 18

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	15/12/2010	Versión inicial del documento
2.0.0	30/09/2011	Restructuración de forma
2.0.1	30/11/2011	Actualización del documento
3.0.0	03/03/2015	Revisión documento
3.0.1	11/03/2016	Alineación con el MSPI

TABLA DE CONTENIDO

PÁG.

1. DERECHOS DE AUTOR

2. AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

En este documento encontrará los lineamientos que las entidades deben implementar para elevar el aseguramiento de los equipos o terminales móviles asignados por la entidad, donde se realizan las transacciones a financieras como los son: pago de nómina, pagos de seguridad social, pagos de contratación y transferencias de fondos, entre otros.

El presente documento se estructura de la siguiente manera:

En el capítulo tres (3), se presentan los lineamientos y requerimientos mínimos que las entidades deben cumplir, este capítulo esta subdividido en cinco (5) campos de acción los cuales son: lineamientos de seguridad lógica, lineamientos de seguridad física, lineamientos de seguridad de la red, lineamientos de seguridad frente a la entidad financiera y lineamientos de seguimiento y monitoreo de controles. En el capítulo cuatro (4) se listan recomendaciones a tener en cuenta durante la realización de las transacciones financieras a través de los portales empresariales de las entidades financieras. Por último se encuentra un anexo con una lista de chequeo la cuál puede ser utilizada por la entidad como una herramienta de apoyo para la implementación, monitoreo y evaluación del cumplimiento de los lineamientos formulados en este documento.

4. GLOSARIO

Con el fin de establecer un lenguaje común cuando hablamos de seguridad de la información en equipos y/o terminales móviles donde se realizan transacciones financieras con recursos públicos y teniendo en cuenta el propósito del presente documento, es indispensable adoptar los siguientes conceptos.

- **Equipo y/o terminal móvil:** Computadoras con diferentes capacidades como: procesamiento, memoria, software, conexión permanente o intermitente a una red datos e Internet, que han sido destinados para una función específica, pero se pueden llevar a cabo otras funciones más generales gracias a su facilidad de uso y portabilidad (p.e., computadores de escritorio, portátiles, tabletas, Smartphone, entre otros).
- **Registrador de teclas (Keylogger):** Un keylogger (derivado del inglés: key (tecla) y logger (registrador); registrador de teclas) es un tipo de software o un dispositivo de hardware específico, que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet a un interesado. El objetivo de utilización de este tipo de mecanismos en equipos o terminales con acceso privilegiado a transacciones financieras, es el de robar información de acceso y demás medios de autenticación en los sistemas o portales transaccionales dispuestos por las entidades financieras, con el propósito de poder usar esta información con fines fraudulentos.
- **Programa Antivirus:** Los programas antivirus exploran la memoria del ordenador y las unidades de disco en busca de virus. Si localizan un virus, la aplicación informa al usuario y puede limpiar, eliminar o poner en cuarentena cualquier archivo, directorio o disco afectado por el código malintencionado.
- **Vulnerabilidad:** Fallo no intencionado de un programa que causa acciones que ni el usuario ni el programa pretendían realizar.
- **Caché:** Cuando se descarga una página Web, los datos se guardan en “caché”, lo que quiere decir que quedan temporalmente almacenados en su ordenador. La próxima vez que se utilice la página, en vez de solicitar el archivo al servidor Web, su navegador accederá a ella de manera automática desde la memoria caché, con lo que la página se cargará más rápido.
- **Cookie:** Bloques de texto colocados en un archivo del disco duro del ordenador. Las páginas Web utilizan las cookies para identificar a los usuarios que las visitan.

- **Usurpación de identidad:** Ocurre cuando un atacante finge ser usted o se hace pasar por usted. Adquiere información clave, tal como su número de la Seguridad Social, su fecha de nacimiento, su carné de conducir o cualquier otra información confidencial.
- **Programas malintencionados (malware):** Término genérico utilizado para describir programas malintencionados tales como virus, troyanos, spyware o contenidos activos malintencionados.

5. LINEAMIENTOS

A continuación se presentan los requerimientos mínimos en seguridad de la información e informática que deben cumplir las entidades públicas de orden nacional y orden territorial en cuanto a los equipos o terminales móviles utilizados para la realización de transacciones financieras con recursos públicos, a través de los portales de internet que las entidades bancarias disponen para tal fin.

5.1. LINEAMIENTOS DE SEGURIDAD LÓGICA

La entidad deberá asegurarse de lo siguiente:

a) Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad (longitud mínima de ocho caracteres alfanúmeros y caracteres especiales) de conformidad con la tecnología y mecanismos técnicos que dispongan las instituciones financieras para este fin.
b) Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil (se sugiere máximo cinco minutos).
c) Limitar los privilegios de la(s) cuenta(s) de usuario(s) utilizada(s) para realizar transacciones financieras en los equipos y/o terminales para este fin, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.
d) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.
e) Establecer procedimientos automatizados o por medio del soporte técnico que disponga la entidad, para efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas (se sugiere mínimo una vez a la semana).
f) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil,

sea realizada únicamente por los funcionarios del área de sistemas o tecnología, o el personal designado por la Entidad para este tipo de requerimientos, adicionalmente, estas actividades deben ser revisadas y aprobadas por el funcionario que desempeñe el rol de oficial de seguridad de la información, y/o las áreas responsables de la seguridad de la información y/o los designados por la entidad para efectuar este tipo de aprobaciones.

g) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones.

h) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada.

i) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).

j) Restringir el software de acceso remoto al equipo que pueda ofrecer o tener preinstalado el Sistema Operativo del respectivo equipo o terminal.

k) Procurar tener instalado un solo navegador, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las instituciones financieras con las que tenga relación, con mejores mecanismos de seguridad posibles debidamente configurados y el cual deberá estar permanentemente actualizado a efecto de garantizar la disposición de mejoras o correcciones a su funcionamiento.

l) Activar mecanismos para que el equipo o terminal pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.

m) Mantener activos y en operación sólo los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades, en el equipo o terminal.

n) En lo posible, el equipo o terminal deberá ser destinado de manera exclusiva para la realización de las transacciones financieras.

o) En lo posible, apagar el equipo o terminal cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet.

5.2. LINEAMIENTOS DE SEGURIDAD FÍSICA

Las entidades deben asegurar que el acceso físico a las áreas donde estén los equipos o terminales móviles, sea lo más restringido posible y de manera exclusiva al responsable directo de la realización de las transacciones. A continuación se listan los controles a ser implementados:

a) Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.
b) Limitar el uso de las terminales móviles corporativas al interior de la entidad, si excepcionalmente la terminal móvil debe llevarse fuera de la entidad, deberán tomarse las precauciones necesarias para evitar el acceso al mismo por parte de personas no autorizadas, o en caso de pérdida o hurto y deberán mantenerse separados de mecanismos de seguridad que habiliten la ejecución de las transacciones.
c) En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo o terminal móvil. Las imágenes deberán ser conservadas por lo menos seis (6) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

5.3. LINEAMIENTOS DE SEGURIDAD DE LA RED

a) Restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o terminal. Esto con el objeto de evitar que de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.
b) Implementar mecanismos de autenticación que permitan confirmar que el equipo o terminal móvil es un dispositivo autorizado dentro de la red de la entidad.
c) Deberá evitarse realizar transacciones financieras desde dispositivos móviles o conexiones a redes inalámbricas de terceros no confiables.
d) Asegurar las redes inalámbricas (WIFI) desde las cuales se realicen transacciones financieras, cuenten con las mejores condiciones y estándares

técnicos disponibles. Definir un usuario con contraseña robusta y cambiarla periódicamente.

e) Si la entidad cuenta con una red inalámbrica (WIFI) para invitados, esta deberá estar totalmente aislada y segmentada de las redes LAN de la entidad.

5.4. LINEAMIENTOS DE SEGURIDAD FRENTE A LA ENTIDAD FINANCIERA

a) Asignar una dirección IP fija pública al equipo o terminal móvil, la cual debe ser informada a la(s) entidad(es) financiera(s), de forma que solo esta dirección IP fija sea la utilizada para realizar transacciones en los portales empresariales.

b) Garantizar la protección de las claves y dispositivos de acceso al equipo o terminal móvil y al portal empresarial de la entidad financiera. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en el equipo y/o terminal móvil de la entidad deberá ser única y personalizada.

c) Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones. Particularmente, definir perfiles de autorización de transacciones, utilizar la preinscripción de beneficiarios, parametrizar montos y horarios para la realización de operaciones y realizar la inscripción para recibir notificaciones en línea.

5.5. LINEAMIENTOS DE SEGUIMIENTO Y MONITOREO DE CONTROLES

a) El máximo responsable del área financiera de la Entidad, deberá coordinar con las áreas de TI y/o de seguridad de la información y/o las Oficinas de Control Interno, el responsable de verificar el cumplimiento de las condiciones de seguridad del equipo y en general, las consagradas en este instructivo, al menos cada tres (3) meses.

b) Para la verificación del cumplimiento de las condiciones de seguridad y los lineamientos aquí establecidos, se deberá diligenciar el anexo adjunto a este documento, el cual deberá ser suscrito tanto por el responsable del área financiera, como por el designado para la respectiva verificación.

6. RECOMENDACIONES DE SEGURIDAD EN LA REALIZACIÓN DE LAS TRANSACCIONES

a) Acceder a la página de la entidad financiera o a través de la cual va a realizar la transacción únicamente digitando la dirección en el navegador. Nunca realice esto a través de links, motores de búsqueda o de los favoritos o marcadores del navegador.
b) Siempre cerrar la sesión del portal transaccional al terminar las transacciones.
c) En lo posible y teniendo en cuenta la afectación de algún servicio, parametrizar ante su banco de tal manera que ninguna transacción financiera pueda realizarse antes de las 6:00 a.m. y después de las 8:00 p.m., ni durante los fines de semana y/o días festivos.
d) Asegurar la restricción en el acceso a los portales transaccionales de los usuarios durante sus períodos de vacaciones o licencias y darlos de baja en casos de traslado o retiros.
e) Llevar un adecuado control de los usuarios y perfiles del equipo. Estos deben ser personalizados y de uso restringido al funcionario asignado (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).
f) Mantener los mecanismos de comunicación con la(s) entidad(es) financiera(s) actualizados, con el fin de informar inmediatamente en caso de identificar algún evento de riesgo que tenga relación las transacciones financieras (ej. pérdida de token, vulneración de clave, solicitud reiterada de credenciales, demoras y retardo en respuestas del Portal, mensajes de mantenimiento, notificaciones de ingresos y transacciones no reconocidas, etc.).
g) Asegurar que las personas que realizan transacciones financieras con los recursos de la entidad cuentan con capacitación en relación con la seguridad de la información y de las medidas que debe adoptar para mitigar los riesgos de fraude financiero.

7. ANEXO – CHECKLIST MONITOREO Y CUMPLIMIENTO

A continuación se presenta un Checklist el cual está compuesto por los lineamientos descritos en el capítulo 3 del presente documento. Este Checklist ha sido elaborado con el fin de brindar una herramienta de apoyo para la implementación, monitoreo y evaluación del cumplimiento de los lineamientos formulados en este documento.

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	a) Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad (longitud mínima de ocho caracteres alfanúmeros y caracteres especiales) de conformidad con la tecnología y mecanismos técnicos que dispongan las instituciones financieras para este fin.	Implementar políticas en el directorio activo de la entidad o mecanismo y/o solución equivalente, que exija la autenticación y controle el tiempo de inactividad del usuario. Para el caso de plataformas Microsoft, consultar las guías con las líneas base de seguridad publicadas por Microsoft para sus plataformas de servidores (2003, 2008 y 2012) http://www.microsoft.com/en-us/download/details.aspx?id=8222 (este link es específico para Windows server 2003, para las otras versiones, consultarlos en la librería de Microsoft online http://technet.microsoft.com/en-us/library)		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	b) Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil (se sugiere máximo cinco minutos).	Implementar políticas en el directorio activo de la entidad o mecanismo y/o solución equivalente, que exija la autenticación y controle el tiempo de inactividad del usuario. Para el caso de plataformas Microsoft, consultar las guías con las líneas base de seguridad publicadas por Microsoft para sus plataformas de servidores (2003, 2008 y 2012) http://www.microsoft.com/en-us/download/details.aspx?id=8222 (este link es específico para Windows server 2003, para las otras versiones, consultarlos en la librería de Microsoft online http://technet.microsoft.com/en-us/library)		
	c) Limitar los privilegios de la(s) cuenta(s) de usuario(s) utilizada(s) para realizar transacciones financieras en los equipos y/o terminales para este fin, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.	Implementar una política en el Directorio Activo o mecanismo y/o solución equivalente, que restrinja los permisos de administración local sobre el equipo o terminal móvil, de los usuarios que realicen transacciones financieras en éste.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	d) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.	Implementar una política a través de herramientas o soluciones como: antivirus o mecanismo de control de equipo y/o terminal móvil, que permitan restringir la ejecución de este tipo de archivos. Implementar una política en el Directorio Activo o mecanismo y/o solución equivalente, la cual restrinja los permisos de administración local sobre el equipo o terminal móvil, de los usuarios que realicen transacciones financieras en este.		
	e) Establecer procedimientos automatizados o por medio del soporte técnico que disponga la entidad, para efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas (se sugiere mínimo una vez a la semana).	Implementar un procedimiento periódico en el cuál se definan las actividades necesarias por medio del soporte técnico que disponga la entidad, para que el equipo o terminal móvil se mantenga depurado de archivos innecesarios.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	f) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil, sea realizada únicamente por los funcionarios del área de sistemas o tecnología, o el personal designado por la Entidad para este tipo de requerimientos, adicionalmente, estas actividades deben ser revisadas y aprobadas por el funcionario que desempeñe el rol de oficial de seguridad de la información, y/o las áreas responsables de la seguridad de la información y/o los designados por la entidad para efectuar este tipo de aprobaciones.	Implementar una política en el Directorio Activo o mecanismo y/o solución equivalente, que restrinja los permisos de administración local sobre el equipo o terminal móvil de los usuarios que realicen transacciones financieras en éste. Implementar un procedimiento para que dichas actividades sean escaladas, autorizadas y ejecutadas, sólo por el personal definido por la entidad.		
	g) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones.	Implementar una política a través de herramientas o soluciones como: antivirus o mecanismos que permitan restringir la ejecución de este tipo de aplicaciones. Implementar una política en el Directorio Activo o mecanismo y/o solución equivalente, la cual restrinja los permisos de administración local sobre el equipo o terminal móvil, de los usuarios que realicen transacciones financieras en este.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	h) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada.	Establecer una lista de software base con el que debe contar el equipo o terminal móvil (p.e., programa antivirus, listado de parches de seguridad del sistema operativo y de los programas instalados, un único navegador, entre otros)		
	i) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).	Implementar políticas en el directorio activo de la entidad o mecanismo y/o solución equivalente que restrinja el uso de este tipo de dispositivos y programas. Para el caso de plataformas Microsoft, consultar las guías con las líneas base de seguridad liberadas por Microsoft para sus plataformas de servidores (2003, 2008 y 2012) http://www.microsoft.com/en-us/download/details.aspx?id=8222 (este link es específico para Windows server 2003, para las otras versiones, consultarlos en la librería de Microsoft online http://technet.microsoft.com/en-us/library) Implementar una política a través de herramientas o soluciones como: antivirus o mecanismo de control de equipos y/o terminales móviles, para restringir el uso de este tipo de dispositivos y programas.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	j) Restringir el software de acceso remoto al equipo que pueda ofrecer o tener preinstalado el Sistema Operativo del respectivo equipo o terminal.	Implementar políticas en el directorio activo de la entidad o mecanismo y/o solución equivalente que restrinja el uso de este tipo de dispositivos y programas. Para el caso de plataformas Microsoft, consultar las guías con las líneas base de seguridad liberadas por Microsoft para sus plataformas de servidores (2003, 2008 y 2012) http://www.microsoft.com/en-us/download/details.aspx?id=8222 (este link es específico para Windows server 2003, para las otras versiones, consultarlos en la librería de Microsoft online http://technet.microsoft.com/en-us/library) Implementar una política a través de herramientas o soluciones como: antivirus o mecanismo de control de equipos y/o terminales móviles, para restringir el uso de este tipo de dispositivos y programas.		
	k) Procurar tener instalado un solo navegador, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las instituciones financieras con las que tenga relación, con mejores mecanismos de seguridad posibles debidamente configurados y el cual deberá estar permanentemente actualizado a efecto de garantizar la disposición	Establecer una lista de software base con el que debe contar el equipo o terminal móvil (p.e., programa antivirus, listado de parches de seguridad del sistema operativo y de los programas instalados, un único navegador, entre otros)		

	de mejoras o correcciones a su funcionamiento.			
Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	l) Activar mecanismos para que el equipo o terminal pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.	Implementar políticas en el directorio activo y/o el servidor WSUS de la entidad o mecanismo y/o solución equivalente que restrinja el uso de este tipo de dispositivos y programas. Para el caso de plataformas Microsoft, consultar las guías con las líneas base de seguridad liberadas por Microsoft para sus plataformas de servidores (2003, 2008 y 2012) http://www.microsoft.com/en-us/download/details.aspx?id=8222 (este link es específico para Windows server 2003, para las otras versiones, consultarlos en la librería de Microsoft online http://technet.microsoft.com/en-us/library) Implementar una política a través de herramientas o soluciones como: antivirus o mecanismo de control de equipos y/o terminales móviles, para restringir el uso de este tipo de dispositivos y programas.		
	m) Mantener activos y en operación sólo los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades, en el equipo o terminal.	Analizar y establecer una lista de los procesos estrictamente necesarios para la ejecución de las herramientas, programas, utilitarios, entre otros, para el correcto funcionamiento de las actividades desempeñadas por el usuario del equipo.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad lógica	n) En lo posible, el equipo o terminal deberá ser destinado de manera exclusiva para la realización de las transacciones financieras.	Verificar que la utilización del equipo o terminal móvil sea realizada solo por el personal autorizado y para las actividades definidas.		
	o) En lo posible, apagar el equipo o terminal cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet.	Habilitar opciones de hibernación y/o suspensión automática.		
Seguridad física	a) Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.	Mantener el seguro de la cerraduras y/o puertas activos y disponibles para acceso solo al personal autorizado para utilizar el equipo o terminal móvil Contar con guardas de seguridad, que registren y evalúen los ingresos al área física donde se encuentra el equipo o terminal móvil		
	b) Limitar el uso de las terminales móviles corporativas al interior de la entidad, si excepcionalmente la terminal móvil debe llevarse fuera de la entidad, deberán tomarse las precauciones necesarias para evitar el acceso al mismo por parte de personas no autorizadas, o en caso de pérdida o hurto y deberán mantenerse separados de mecanismos de seguridad que habiliten la ejecución de las transacciones.	Para este lineamiento, es necesario implementar una política de uso del equipo o terminal móvil en las afueras de la entidad, e implementar las actividades recomendadas en los lineamientos de seguridad generales - capitulo 3 lineamientos del "a)" hasta el "o)".		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad física	c) En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo o terminal móvil. Las imágenes deberán ser conservadas por lo menos seis (6) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.	La entidad decidirá si es necesario implementar este tipo de controles de acuerdo a las necesidades y/o la evaluación de riesgos asociados, que haya efectuado la entidad.		
Seguridad de la red	a) Restringir el acceso a correos personales , redes sociales , y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o terminal. Esto con el objeto de evitar que de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.	Implementar una política a través de la solución con la que disponga la entidad para filtrado de contenido o servidor proxy (si es posible) con el fin de restringir la el acceso a este tipo contenidos y portales de internet.		
	b) Implementar mecanismos de autenticación que permitan confirmar que el equipo o terminal móvil es un dispositivo autorizado dentro de la red de la entidad.	Implementar políticas de filtrado de direcciones MAC, matricula del equipo en el dominio (aplica para plataformas Microsoft) y/o mecanismos que permitan identificar la veracidad y autenticidad del equipo o terminal móvil.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad de la red	c) Deberá evitarse realizar transacciones financieras desde dispositivos móviles o conexiones a redes inalámbricas de terceros no confiables.	Definir un listado de equipos o terminales móviles las cuáles serán las únicas autorizadas para la realización de este tipo de transacciones. Implementar mecanismos de conexión segura o cifrada, para los escenarios en los que los equipos o terminales móviles deban conectarse a los portales empresariales dispuestos por las entidades financieras, desde conexiones externas a la entidad y no confiables.		
	d) Asegurar las redes inalámbricas (WIFI) desde las cuales se realicen transacciones financieras, cuenten con las mejores condiciones y estándares técnicos disponibles. Definir un usuario con contraseña robusta y cambiarla periódicamente.	En lo posible utilizar sistemas de protección WPA2 - con cifrado AES. Consultar las buenas prácticas de seguridad publicadas por la WiFi Alliance http://www.wi-fi.org/discover-and-learn/security.		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad de la red	e) Si la entidad cuenta con una red inalámbrica (WIFI) para invitados, esta deberá estar totalmente aislada y segmentada de las redes LAN de la entidad.	El segmento de red utilizado para la red inalámbrica (WIFI) ofrecida a invitados, debe pertenecer a un segmento o VLAN aislada de la red corporativa de la entidad, restringiendo así el acceso desde esta a servicios como el servidor de: correo, DNS, proxy, impresión, archivos, bases de datos, y en general todos los servidores del ambiente de producción de la entidad.		
Seguridad frente a la entidad financiera	a) Asignar una dirección IP fija pública al equipo o terminal móvil, la cual debe ser informada a la(s) entidad(es) financiera(s), de forma que solo esta dirección IP fija sea la utilizada para realizar transacciones en los portales empresariales.	Consultar con el proveedor de servicios de internet (ISP), el procedimiento para solicitar la dirección ip fija pública, posteriormente asignar esta dirección ip fija únicamente para el equipo o terminal móvil donde se realizaran las transacciones financieras de la entidad		

Checklist para realizar el seguimiento y evaluación del cumplimiento de lineamientos estipulados en el presente documento				
Lineamientos	**Especificación**	**Actividad/Control recomendado**	**Resultado**	**Cumplimiento**
Seguridad frente a la entidad financiera	b) Garantizar la protección de las claves y dispositivos de acceso al equipo o terminal móvil y al portal empresarial de la entidad financiera. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en el equipo y/o terminal móvil de la entidad deberá ser única y personalizada.	Emitir una política con el fin de asegurar la custodia de este tipo de claves y dispositivos de acceso a los sistemas de información. Crear usuarios personalizados en los sistemas de información que permitan identificar la trazabilidad de lo realizado por los funcionarios que utilizan el equipo o terminal móvil.		
	c) Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones. Particularmente, definir perfiles de autorización de transacciones, utilizar la preinscripción de beneficiarios, parametrizar montos y horarios para la realización de operaciones y realizar la inscripción para recibir notificaciones en línea.	Solicitar la asesoría de la entidad financiera, para implementar las medidas necesarias para minimizar los niveles de riesgo y fraude a los que están expuestas las entidades.		