LINEAMIENTOS DE SEGURIDAD EQUIPOS DE ÁREA FINANCIERA

UNIVERSIDAD DE LOS LLANOS

OFICINA DE SISTEMAS
2022

Contenido

1. Objetivo

Establecer los requerimientos mínimos en seguridad de la información que deben cumplir los equipos de la Universidad de los Llanos en los que se realicen las transacciones financieras con recursos públicos, a través de los portales de internet que las entidades financieras disponen para tal fin.

2. Alcance

Aplica para los equipos del área de tesorería de la Universidad de los Llanos en los que se realicen las transacciones financieras.

3. Definiciones

- **Equipo**: Computadores con diferentes capacidades como: procesamiento, memoria, software, conexión permanente o intermitente a una red datos e Internet, (de escritorio, portátiles, tabletas, smartphones, entre otros).

- **Registrador de teclas (Keylogger):** Un keylogger (derivado del inglés: key (tecla) y logger (registrador)) 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 fin de su uso 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**: Es una aplicación independiente o un conjunto de programas que permiten detectar y eliminar virus de ordenadores y redes.

- **Vulnerabilidad**: Debilidad o deficiencia en el software o en el hardware, que permite a un atacante comprometer la integridad, disponibilidad o confidencialidad de los datos de un sistema.

- **Caché**: Memoria temporal donde se almacena información referente a las páginas que se visitan con los diferentes navegadores de internet.

- **Cookie**: Es un pequeño fragmento de texto que crean los sitios web y se almacenan en el navegador permitiendo así recordar accesos a las páginas.

- **Programas malintencionados (malware):** Término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

4. Lineamientos de Seguridad

De conformidad con la “Guía No. 18 lineamientos: Terminales de áreas financieras entidades públicas” definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, los siguientes son los lineamientos mínimos que se deben implementar en los equipos de la Universidad de los Llanos, para garantizar la seguridad de las transacciones financieras como son: pago de nómina, pagos de seguridad social, pagos de contratación y transferencias de fondos, entre otros.

4.1. Lineamientos de Seguridad Lógica

a) Se debe disponer de manera exclusiva el uso de un equipo para la realización de las transacciones financieras de la Universidad de los Llanos y su uso debe limitarse al personal autorizado para tal fin.

b) El equipo debe configurarse únicamente con los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para la correcta ejecución de las transacciones financieras de la Universidad.

c) Se requiere que el ingreso a los portales de las entidades financieras para realizar transacciones en la Universidad de los Llanos, se realice mediante el uso de credenciales de autenticación y certificados digitales y/o token.

d) El equipo dispuesto para realizar las transacciones financieras en la Universidad, se debe configurar de forma tal que se controle el tiempo de inactividad del usuario, a través del bloqueo automático del equipo.

e) Se deben limitar los privilegios de la cuenta del usuario responsable de realizar transacciones financieras en la Universidad, con el fin de restringir la instalación y ejecución de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VCN, entre otros), archivos, o programas no autorizados; dicha actividad será realizada únicamente por los funcionarios autorizados de la Oficina de Sistemas, o el personal designado por la Universidad para atender este tipo de requerimientos.

f) Se requiere que en el equipo se efectúe el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas.

g) Se debe asegurar que el equipo cuente mínimo con: antivirus (con módulos de anti-keylogger, firewall personal, antispyware, antispam), software licenciado y que las actualizaciones se realicen de manera supervisada.

h) Se deben restringir los puertos del equipo para evitar la conexión y/o acceso a dispositivos de almacenamiento extraíbles.

i) Se debe tener instalado un navegador que se encuentre permanentemente actualizado, en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las instituciones financieras con las que tenga relación la Universidad.

j) El personal encargado de realizar las transacciones financieras, deberá cerrar sesión de forma segura en el portal financiero donde haya trabajado y cerrar el navegador antes de apagar el equipo de cómputo.

k) El personal encargado de realizar las transacciones financieras, deberá bloquear el equipo cuando no lo esté utilizando, y apagarlo cuando termine la jornada laboral; sobre todo si dispone de una conexión permanente a Internet.

4.2. Lineamientos de Seguridad Física

Se recomienda que el acceso físico a las áreas donde esté el equipo dispuesto para realizar las transacciones financieras, sea restringido y de manera exclusiva al responsable directo de la realización de las transacciones. Teniendo en cuenta la implementación de los siguientes controles:

a) Restringir el acceso al área física desde donde se realizan las transacciones financieras, sólo permitir el ingreso a la persona autorizada.

b) En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el área donde se encuentre el equipo. Las imágenes deberán ser conservadas por lo menos seis (6) meses 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.

4.3. Lineamientos de Seguridad de la Red

a) Al usuario de dominio del equipo en el que se realizarán las transacciones financieras en la Universidad, se le debe restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones; esto, con el fin de evitar que, de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.

b) Se deben implementar políticas en el directorio activo que permitan verificar que el equipo desde el cual se están realizando las transacciones financieras es un dispositivo autorizado dentro de la red de la Universidad.

c) El equipo dispuesto para realizar las transacciones financieras de la Universidad, deberá siempre estar conectado a la red LAN, y se prohíbe su conexión a través de redes inalámbricas propias, o de terceros.

4.4. Lineamientos de Seguridad Frente a la Entidad Financiera

a) El equipo en el que se realicen las transacciones financieras, deberá tener una dirección IP fija pública, la cual debe ser informada a la(s) entidad(es) financiera(s) por parte de la Oficina de Tesorería, de forma que solo esta dirección IP sea la utilizada para realizar transacciones en los portales empresariales.

b) La persona responsable de realizar las transacciones financieras de la Universidad, deberá velar por la custodia de las claves y dispositivos de acceso tanto al equipo como al portal de la entidad financiera. Por lo tanto, deberá evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en el equipo de la Universidad deberá ser única y personalizada.

c) Se deben utilizar las medidas de autenticación y control que ofrecen la(s) entidad(es) financieras para realizar 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.

d) Se debe 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 se debe realizar esto a través de links, motores de búsqueda, ni favoritos o marcadores del navegador.