LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PARTICIPANTES EN EL SISTEMA DE LIQUIDACIÓN BRUTA EN TIEMPO REAL (LBTR)

Guatemala, 18 de abril de 2013.

CONTENIDO

I. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

La información del Sistema de Liquidación Bruta en Tiempo Real (LBTR) es confidencial, por lo que la misma debe ser resguardada adecuadamente para evitar el uso indebido de personas no autorizadas. Derivado de lo anterior, los participantes deben observar los lineamientos siguientes:

A. Autenticación por contraseña de usuarios de dispositivos y software

1. Las contraseñas predeterminadas de acceso para los usuarios del Sistema LBTR, así como para el acceso a cualquier otro dispositivo o software relacionado con el sistema, deberán reemplazarse inmediatamente al ingresar por primera vez. Las nuevas contraseñas serán personales y deberán observar las características establecidas en el presente documento.

2. Los usuarios serán responsables del uso de sus contraseñas de acceso en el Sistema LBTR y en los dispositivos que tenga asignados, manteniendo la confidencialidad de las mismas.

3. La longitud mínima de las contraseñas debe ser de ocho (8) caracteres, conteniendo una combinación de mayúsculas, minúsculas, números y/o símbolos.

4. Los usuarios no deben utilizar contraseñas con palabras de uso común o fácilmente asociables a él mismo.

5. Las contraseñas podrán anotarse en sobres de seguridad, los cuales deben ser resguardados en caja fuerte o archivo de seguridad y serán utilizados como contingencia. Las contraseñas almacenadas en medios digitales como contingencia, deberán resguardarse y estructurarse bajo un mecanismo de cifrado, vigente y confiable tecnológicamente.

6. Las contraseñas tendrán una vigencia máxima de 30 días.

7. Las contraseñas no deben repetirse.

8. Las contraseñas del Sistema LBTR no deben utilizarse en servicios externos, tales como correo electrónico público, servicios de compras y otros.

9. Las redes privadas virtuales (VPN) deberán hacer uso de métodos de autenticación con “contraseña fuerte” que contenga mayúsculas, minúsculas, números y/o símbolos.

B. Inicio y pausa de estaciones de trabajo

1. Al iniciar una sesión en el Sistema LBTR, se desplegará un mensaje que indica el cambio de situación y que el sistema está restringido a usuarios autorizados. Al ingresar, el usuario acepta las responsabilidades que conlleva el uso del sistema.

2. Las computadoras personales y/o servidores relacionados con el Sistema LBTR, deberán ejecutar el protector de pantalla luego de un lapso de tiempo en que el usuario no interactúe con dicho equipo.

3. Los intervalos de espera para ejecutar los protectores de pantalla deberán ser de un máximo de quince (15) minutos para computadoras personales y de diez (10) minutos para servidores.

4. El protector de pantalla deberá contar con un mecanismo de autenticación que le permita al usuario el reingreso a la sesión.

C. Manejo y destrucción de la información

1. Configurar todo mecanismo de acceso al Sistema LBTR, permitiendo un mínimo de privilegios de acceso a los datos en función a los roles de trabajo que el usuario desempeña.

2. Tomar las medidas preventivas que aseguren que los procesos sensibles de actualización requieran la participación de más de una persona en su ejecución.

3. Destruir toda información sensible generada por los sistemas y cuyo resguardo no representa ninguna utilidad.

4. Contar con bitácoras que registren los sucesos y eventos de seguridad, de los equipos utilizados para acceder al Sistema LBTR.

D. Escritorio de ayuda

1. La asignación de contraseñas a los funcionarios de las entidades participantes responsables del Sistema LBTR, se hará de manera personal y confidencial, las cuales se entregarán impresas en sobres de seguridad. El funcionario responsable deberá firmar una boleta de recepción de contraseñas.

2. El operador del escritorio de ayuda deberá solicitar y verificar los datos de identificación del usuario solicitante, los cuales se encuentran registrados en el expediente de la entidad participante en el Sistema LBTR.

3. El operador del escritorio de ayuda llevará una bitácora de servicios para localizar fácil y rápidamente las solicitudes efectuadas por los participantes en el Sistema LBTR durante el día de operaciones.

4. Las contraseñas no podrán revelarse por vía telefónica u otros medios diferentes a los establecidos en estos lineamientos.

E. Respuesta a incidentes informáticos

1. Se considerarán incidentes informáticos los eventos que expongan los componentes del Sistema de Liquidación Bruta en Tiempo Real, bajo las condiciones siguientes:

- Denegación de servicio
- Intrusión
- Vandalismo
- Virus
- Ingeniería social
- Sabotaje

- Violación de derechos de autor
- Uso comercial indebido
- Desclasificación o publicación indebida
- Uso criminal
- Robo
- Otros catalogados como delitos

2. Al ocurrir un incidente informático de los mencionados en el numeral anterior, deberá preservarse la evidencia, no alterando su configuración original de los equipos de cómputo. En caso de no tener la evidencia, en la medida de lo posible deberá simularse íntegramente toda la información, archivos relacionados, configuraciones e imágenes de pantalla relacionados con el incidente.

3. Todo incidente informático deberá ser informado a las Direcciones de los Departamentos de Contabilidad y Sistema de Pagos y de Tecnologías de Información del Banco de Guatemala.

F. Firewall y Redes Privadas Virtuales (VPN)

1. Los equipos relacionados directamente con el Sistema LBTR, no podrán hacer uso de módems, de conexiones inalámbricas de red o de cualquier otra conexión para enlazarse a Internet.

2. El Departamento de Tecnologías de Información del Banco de Guatemala podrá bloquear el acceso a cualquier dirección o puerto de red por razones de vulnerabilidad o cuando derive de razones de trabajo y de eficiencia en el servicio que se presta a los participantes del Sistema LBTR. Asimismo, mantendrá un registro de los accesos hacia los servidores del Sistema LBTR.

3. El ciframiento en las transmisiones por redes privadas virtuales (VPN) debe ser bajo un mecanismo simétrico mayor o igual a 128 bits y asimétrico mayor o igual a 2048 bits. Estos mecanismos de ciframiento simétrico serán del tipo “3DES” y “AES”. Para el ciframiento asimétrico será de tipo “RSA”.

4. Las redes privadas virtuales (VPN) deberán estar documentadas y deberán incluir, como mínimo, la información de las entidades participantes y sus usuarios, los horarios de uso y las actividades autorizadas a realizar con el servicio.

G. Comunicación de la red por discado telefónico

1. Los equipos utilizados para acceder el Sistema LBTR no deberán tener instalado otros dispositivos para acceder a Internet u otra red pública, a menos que estos sean filtrados por un firewall de la entidad usuaria de dichos dispositivos.

2. El módem utilizado como activo de contingencia en caso de falla del canal principal de comunicación, deberá mantenerse desactivado y ser incapaz de recibir conexiones externas cuando no se requiera su uso y, como mínimo, para responder externamente, tendrá que poseer un mecanismo de autenticación por usuario y contraseña fuerte.

II. LINEAMIENTOS DE SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS

Las entidades participantes en el Sistema LBTR deberán observar los lineamientos de seguridad física en sus equipos informáticos, de la manera siguiente:

1. Las entidades participantes deberán contar con instalaciones y mecanismos para prevenir daños ocasionados por pérdida, robo y/o falla de los dispositivos informáticos relacionados con el Sistema LBTR.

2. Los usuarios del Sistema LBTR deberán practicar políticas de escritorios limpios, para garantizar un manejo ordenado, confidencial y seguro de la información. Dichas políticas deben incluir el manejo de contraseñas, de documentos con información confidencial, del manejo de agendas y calendario de escritorio, los cuales deben mantenerse en gavetas con llave cuando no se utilicen.

3. Los dispositivos informáticos para acceder al Sistema LBTR deben estar bajo un mecanismo de inventario que corrobore su existencia y uso, el cual estará bajo la responsabilidad de cada entidad participante.

4. Las computadoras portátiles no deben utilizarse para acceder al Sistema LBTR. A dicho sistema sólo debe ingresarse por medio de computadoras de escritorio, ubicadas en un lugar específico.

5. Los monitores de los equipos informáticos utilizados en cualquier servicio del Sistema LBTR deben encontrarse lo suficientemente distantes o contrapuestos a ventanas exteriores o interiores al ambiente privado de trabajo.

6. Las fuentes de energía eléctrica que se utilicen deben contar con mecanismos de protección y contingencia contra posibles variaciones de voltaje, apagones cortos o de larga duración.

7. Los equipos de cómputo, así como los dispositivos de acceso al Sistema LBTR deben ubicarse en un área privada y contar con el suficiente aislamiento del público interno (empleados no involucrados) y externo (público en general). Dichos ambientes de trabajo deben contar con puertas con cerradura o cualquier otro mecanismo de cierre seguro. Asimismo los dispositivos de seguridad y los lectores de dispositivos de seguridad, deberán ser resguardados en escritorios con cerradura física y llave propia.