Banco Argentino de Desarrollo BICE

Anexo - Requisitos de Seguridad para el Desarrollo y-o adquisición de aplicaciones

ANX.SI.07

Versión: 00

Vigencia: 21/07/2022

PARTICIPACIÓN DEL ÁREA DE SEGURIDAD INFORMÁTICA

El área de Seguridad Informática debe ser convocada en el inicio del proceso de Desarrollo o evaluación para la adquisición de un aplicativo o Software de Base, a fin de participar de dicho proceso, validando si se cumple con todos los requisitos mencionados en el presente documento.

AUTENTICACIÓN DE USUARIOS

Toda aplicación o software de base debe poseer un sistema de autenticación de usuarios.

Debe estar integrada con el sistema operativo o base de autenticación para el Banco, donde están definidas las cuentas de usuarios y respectivos perfiles funcionales. De ser esto imposible, debe estar debidamente justificado, y se debe proveer un esquema de autenticación robusto que verifique el estándar de contraseñas vigente en donde se contemple cómo mínimo los siguientes ítems, los cuales deben ser parametrizables desde el módulo de Seguridad:

- Cuenta de Usuario y respectiva contraseña única.
- Posibilidad de establecer una nueva contraseña a elección.
- Longitud mínima de contraseña para todas las cuentas.
- Solicitud de cambio de contraseña en el primer inicio de sesión.
- Expiración de contraseña, cada 30 días.
- Bloqueo de usuario luego de reiterados intentos de ingreso fallidos, a razón de 3 intentos.
- No repetición de las últimas contraseñas utilizadas, correspondiente a las 12 anteriores.
- Antigüedad mínima de contraseña ante cambios sucesivos, un periodo de 7 días.
- Almacenamiento cifrado de contraseñas con algoritmos de robustez reconocida internacionalmente.
- Desconexión de sesión luego de un período establecido de inactividad, 15 minutos.

ADMINISTRACIÓN DE ACCESOS

Las aplicaciones y/o software de base deben contar con un módulo de administración de seguridad en los accesos, que mínimamente permita:

- De no contar con Seguridad Integrada, debe permitir la creación, modificación, inhabilitación y eliminación de usuarios individuales.
- De no contar con Seguridad Integrada, debe permitir la creación, modificación y eliminación de grupos/perfiles de usuario, para permitir la separación de las distintas funcionalidades y transacciones.
- Asignar y eliminar permisos a los grupos/perfiles de usuario según su perfil funcional.

- Asignar y eliminar usuarios individuales a grupos/perfiles de usuario según su perfil funcional.
- Restringir a un único acceso concurrente por usuario.

CONTROL DE LOS ACCESOS, PARÁMETROS Y EVENTOS DE SEGURIDAD

Las aplicaciones y/o software de base deben contar con un módulo de control de seguridad en los accesos y las tareas realizadas, que mínimamente permita:

- Identificación del usuario que ingresa o ingresó a la aplicación.
- Ante un intento de ingreso fallido NO debe indicarle al usuario si el error se encuentra en la identificación del usuario o en su contraseña. Como ser por ejemplo “El nombre de usuario o contraseña no es correcto.”
- Contar con un módulo de configuración de seguridad completamente separado del resto, en especial de los módulos de parametrización.
- Contar con reportes de control de acuerdo con las definiciones de seguridad implementadas, como mínimo se deben poder ejecutar reportes en función de las pistas de auditoria que se detallan en el próximo punto.
- Incluir registros de pistas de auditoría sobre eventos de seguridad, entre los que se encuentran los siguientes:
    - Ingresos y egresos de usuarios.
    - Intentos de ingreso fallidos.
    - Fecha y hora del último ingreso por usuario.
    - Altas, bajas y modificaciones de perfiles.
    - Altas, bajas y modificaciones de usuarios.
    - Bloqueos y desbloqueo de usuarios.
    - Desconexiones de usuarios.
    - Blanqueos de contraseñas de usuario.
    - Cambios de permisos, conservando los valores anteriores y posteriores de cada cambio.
    - Cambios de parámetros, conservando los valores anteriores y posteriores de cada cambio.

CUMPLIMIENTO DE NORMAS Y REGULACIONES VIGENTES

Toda aplicación debe cumplir con lo exigido por la legislación vigente y las normas emitidas por el Banco Central de la República Argentina, en especial los requisitos mínimos de gestión, implementación, y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras, establecidos en la Com. "A" 4609 modificatorias, concordantes y complementarias.

MEJORES PRÁCTICAS DE SEGURIDAD (SECURITY BEST PRACTICES)

En general, las herramientas de desarrollo de aplicaciones, las aplicaciones en sí mismas, y el software de base, disponen de documentación en dónde el proveedor indica lo que son las "mejores prácticas de seguridad". Se deben considerar en todo momento la implementación de dichas prácticas.

ESTRUCTURA DE ALMACENAMIENTO DE LA APLICACIÓN

- Las contraseñas y claves de cifrado utilizadas por la aplicación se deben almacenar en archivos de configuración cifradas con un algoritmo aprobado por Seguridad Informática. Solamente los usuarios finales tienen permiso de lectura sobre esos archivos, y solamente Seguridad informática puede modificarlos.
- La aplicación debe contemplar una separación lógica de sus componentes,
    - Archivos temporales
    - Archivos de lectura-escritura
    - Archivos de datos de sólo lectura
    - Ejecutables
    - Configuraciones de seguridad
    - Registros de eventos de seguridad

  De esta manera se permite una correcta asignación de permisos sobre los mismos.

  De no ser posible esta segregación, se debe proveer la justificación correspondiente y proveer el detalle de los permisos a aplicar para cada una de las carpetas de la aplicación.
- Recursos compartidos: en caso de acceder a la aplicación o software de base a través de una carpeta compartida, se debe utilizar un único punto de entrada a la misma, parametrizable en un archivo de configuración.
- Bases de Datos: los usuarios deben acceder a los datos almacenados en las bases de datos exclusivamente utilizando la aplicación correspondiente y nunca de forma directa.

INFRAESTRUCTURA CLOUD

A continuación, se detallan los aspectos relevantes respecto de la seguridad ante la arquitectura Cloud:

- Rápida respuesta ante ataques de denegación de servicios (DoS). Bloqueo del ataque y plan de continuidad del negocio definido.
- El almacenamiento de los datos debe situarse en las localizaciones avaladas por el contrato.
- Persistencia de datos. Deben utilizarse técnicas para localizar de forma completa y efectiva los datos en la nube, así como también borrar/destruir datos asegurando que los mismos han sido completamente eliminados, ello en el caso de una migración a servidores locales o cambio de prestador de la infraestructura cloud.
- Utilizar un canal cifrado, seguro, para la transmisión de los datos. Es importante proteger la información sensible, incluso cuando los datos se trasmiten dentro de la red del proveedor de la nube.
- No permitir la lectura de los datos a través de ataques con intermediarios (MITM). Se deben implementar conocidas técnicas para evitar el ataque durante el proceso de intercambio de claves, tal como lo establecen las mejores prácticas utilizando autenticación mutua fuerte, clave pública, entre otros.
- Hardening [1]de los servidores físicos y/o virtuales. En el caso de ser virtual el proveedor debe garantizar la correcta seguridad del entorno.
- Respecto de la seguridad perimetral se debe implementar un sistema de prevención de intrusos (IPS), y evaluar si corresponde la contratación de un Firewall de aplicaciones Web (WAF).
- En el caso que el servicio incluya resguardo de información, el proveedor debe garantizar una adecuada frecuencia de dicha función para asegurar la integridad de la información y pruebas periódicas de restauración.

A fin de corroborar el cumplimiento de los puntos mencionados, y de la utilización de las mejores prácticas, se recomienda realizar un análisis de vulnerabilidades (pentest) antes de la puesta en producción, y luego cada 6 o 12 meses, además de establecer procesos de control y auditoría para que las áreas pertinentes del banco puedan corroborar lo implementado.

Dicho análisis debe ser efectuado por una compañía especializada, diferente a quien está a cargo del desarrollo o adquisición del nuevo software, y la contratación de la misma, a cargo del BICE con el fin de garantizar la imparcialidad de los resultados.

DOCUMENTACIÓN DE SEGURIDAD

Se debe proveer al Sector de Seguridad Informática la documentación técnica y de administración de seguridad de la aplicación y o software de base.

En la misma, y como ejemplo, se mencionan las siguientes configuraciones de seguridad:

- Servicios

[1] Fortalecimiento o endurecimiento de un sistema.

- Sistemas de archivos
- Privilegios de usuarios
- Políticas de Seguridad de la aplicación y/o software de base
- Seguridad en las comunicaciones de red
- Altas, bajas y modificaciones de usuarios/grupos

REGISTRO DE MODIFICACIONES AL DOCUMENTO

Cada persona que actualice el presente documento debe registrar la fecha, número de versión, nombre y la sección de este documento que fue modificada.

ANTECEDENTES DE APROBACIÓN Y CAMBIOS

Versión	Fecha de vigencia	Cambio realizado
0	18/01/2012	Versión inicial.
1	18/05/2022	Incorporación de los requisitos para Infraestructura Cloud.
2	01/03/2018	Adecuación Integral.
3	28/03/2018	Adecuación integral.
4	21/07/2022	Adecuación integral.