Tema
General
Controles y monitoreos para la detección y prevención de fraudes
Brindar detalle del modelo de responsabilidad en el tratamiento de los datos
Cuenta con planes de concientización a los usuarios internos. Detallar
Cuenta con un procedimiento para el manejo de incidentes de seguridad. Adjuntar documentación.
Cuenta con un módulo de seguridad de hardware (HSM) dedicados; por ejemplo, dispositivos de hardware que proporcionen almacenamiento de claves de seguridad y operaciones criptográficas dentro de un módulo de hardware resistente a prueba de manipulaciones
¿Cuenta con un proceso de evaluación y resolución de vulnerabilidades en las aplicaciones y recursos? Brindar detalle.
Cuenta con un firewall de aplicación web (WAF). Brindar información
Especificar cómo previene y contiene eventuales ataques de denegación de servicio distribuidos (DDoS) que se producen en la red y en la capa de transporte, además de la capacidad de escribir reglas personalizadas para mitigar ataques sofisticados en la capa de aplicación.
Especificar el servicio administrador de detección de amenazas.
Desarrollo y Testing de las aplicaciones
¿Existen ambientes separados para desarrollo, prueba y producción? Se recomienda que existan ambientes separados.
¿ Existe alguna evidencia de auditoría reciente sobre las políticas, procedimientos operativos y eficiencia operativa de su sitio? Se recomienda realizar auditorías internas/externas en forma trimestral.
¿Utiliza un framework para el desarrollo seguro, con pruebas estáticas y dinámicas del código?
¿Realiza pruebas de seguridad en forma regular incluyendo test de penetración? Especificar
¿Cuenta con un proceso para la gestión segura de privilegios elevados?
Comunicaciones
Algoritmos de cifrado utilizados en el intercambio de datos entre los diferentes componentes de la solución
Autenticación de los usuarios de sistema ¿soporta integración con Active Directory /Azure?
Permitir Single-Sign-on mediante autorización con Active Directory o Azure

La modificación de las contraseñas maestras y de cuentas especiales “por defecto” de los sistemas operativos, de los subsistemas administradores de seguridad, de las bases de datos y de las herramientas para la administración y el control.
El cambio obligatorio de las contraseñas de acceso en el primer inicio de sesión.
12 (doces) caracteres de longitud [MÍNIMA] para las claves provistas a todo sistema informático de la entidad.
El registro histórico de las últimas 12 (doce) contraseñas utilizadas, evitando ser reutilizadas.
El intervalo de caducidad automática de las mismas a los 28 (treinta) días.
El usuario debe poder cambiar su clave sin necesidad de esperar los 30 (treinta) días; siempre y cuando el cambio sea 1 por día.
El bloqueo permanente de la cuenta del usuario ante 3 (tres) intentos de acceso fallidos.
La deshabilitación de las cuentas de usuario inactivas por un período mayor a 90 (noventa) días.
Asignación de contraseñas para todas las cuentas.
Soportar el cambio de contraseñas de usuarios de servicio de forma regular.
Se podrá definir la obligación de cambio de clave luego de un blanqueo por parte de los administradores de seguridad.
Capacidad de desactivar cuentas de usuarios por ausencias.
Desconexión automática de la sesión de usuario por inactividad (15 minutos).
La identificación única (ID) de usuarios.
Capacidad para soportar Autorización con determinación de roles (Segregación de funciones).
Capacidad para asignar roles y jerarquías de aprobación para los usuarios. Contar con administración de perfiles de usuarios, cada usuario podrá asignarse a un único perfil
Capacidad para soportar auditoría y registrar acciones de los usuarios (Log de eventos).
Registra los cambios de sistemas, configuraciones de red o servicios, incluyendo la instalación de parches y actualizaciones de software u otros cambios en el software instalado
Soportar el envió de los registros en formato estándares a través de syslog, syslog-ng, o protocolos de red syslog similar a un sistema de gestión de registros central.
Capacidad de encriptar la información crítica en todos sus estados (enviada/recibida/procesada/almacenada) - Informar tipo de algoritmo de cifrado)
Las claves deben viajar encriptadas en la red.
Las claves deben viajar encriptadas en la base de datos.

Capacidad de interacción con herramientas de Backup (Configuración y datos).
Capacidad para dar soporte en un ambiente de alta disponibilidad.
Capacidad de asegurar los accesos o modificaciones no autorizadas con controles de integridad.
Cuenta con certificación de seguridad, hacking test/penetración o evaluación terceras partes. Detallar que certificados posee.
Capacidad de emisión de reportes de sistemas. (listado de usuarios, perfiles asignados, tiempos de inactividad, fecha ultimo login, composición de perfiles).
Capacidad de soportar los logs en Bases de Datos.
Capacidades MFA para el inicio de sesión. Especificar.
En acciones, transacciones, etc. de alto riesgo, se deben poner límites a las aprobaciones por los montos de que se trate. (Autorización de excepciones).
Poseer documentación técnica de seguridad.
Administración de parámetros y atributos de seguridad en forma centralizada en un solo modulo con acceso permitido solo a administradores.
Gestión de Alertas parametrizables (por ejemplo: para accesos inválidos).