Digipro, S.A. de C.V.

Hoja de revisión.

Este documento fue creado conforme a los requerimientos institucionales, revisado por el área de Control y Cumplimiento y aprobado por la Dirección de Tecnologías de Información.

Estamos de acuerdo con su contenido e implementación, en caso de haber cualquier modificación o adición a este documento, es responsabilidad del área emisora indicar la modificación o adición, previa aprobación de las áreas involucradas para evitar errores, incrementar el control interno y/o mejorar la productividad de los departamentos involucrados.

Control de Cambios		
Versión	**Cambios realizados**	**Fecha**
01	Documento de nueva creación	19/12/2024

Contenido

Política sobre el Uso de Controles Criptográficos

Establecer y dar a conocer los lineamientos para la correcta gestión de la seguridad de la plataforma en cuestión de algoritmos de cifrado, políticas de control de acceso, cifrado de datos y la gestión de estas llaves de cifrado.

1. **Uso de criptografía en la organización:**
   - Todos los mecanismos de autenticación, confidencialidad e integridad de la información deben implementar criptografía conforme a los estándares establecidos.
2. **Autenticación y acceso de usuarios:**
   - Todo usuario que acceda al sistema I&D Portal debe autenticarse mediante un nombre de usuario y una contraseña.
   - El nombre de usuario puede tener hasta 50 caracteres y puede incluir caracteres especiales, permitiendo el uso de direcciones de correo electrónico.
   - Las contraseñas deben cumplir con las siguientes configuraciones:
     - Definir longitudes mínimas y máximas.
     - Definir si se requieren el uso de caracteres alfabéticos (mayúsculas y minúsculas), numéricos y especiales.
     - Definir restricción en la repetición consecutiva de caracteres.
     - Definir restricción de las últimas contraseñas utilizadas.
     - Definir vigencia para obligar al usuario a cambiar su contraseña periódicamente.
3. **Bloqueo de usuarios:**
   - Los usuarios serán bloqueados automáticamente después de un número configurable de intentos fallidos de autenticación consecutivos o acumulados en el día.
   - Las cuentas de usuarios que no hayan sido utilizadas durante cierto período serán bloqueadas.
   - Las cuentas bloqueadas que no sean reactivadas dentro de un periodo definido serán dadas de baja automáticamente.
4. **Cifrado de contraseñas:**
   - Las contraseñas se almacenarán en la base de datos de forma segura utilizando un algoritmo de hash criptográfico como SHA-256.
5. **Acceso y seguridad de la base de datos:**
   - El acceso a las bases de datos sólo puede hacerse mediante los procedimientos almacenados disponibles.
   - Todos los accesos a la base de datos se hacen utilizando un usuario específico que se configura con los mínimos permisos posibles.
   - Las cadenas de conexión están almacenadas en la base de datos y cifradas utilizando el algoritmo AES-256 con una llave de cifrado.
   - Se implementa cifrado de datos en reposo mediante TDE (Transparent Data Encryption) de SQL Server.

6. **Seguridad del servidor:**
   - Si el servidor de base de datos está en el mismo dominio que el servidor IIS, se debe configurar autenticación mediante un usuario confiable del dominio.
   - En otros casos, se debe utilizar un usuario específico de SQL para acceder a la base de datos.
7. **Almacenamiento y transferencia de archivos:**
   - Las imágenes y documentos se cifran utilizando el algoritmo AES-256 en los siguientes casos:
     - Temporalmente al digitalizarlos o importarlos.
     - Definitivamente después de transferirlos al servidor.
   - La consulta de imágenes no genera archivos temporales en disco; la transferencia es directa entre el navegador y el servicio web.
8. **Token JWT:**
   - Se utiliza un token "Json Web Token" para la comunicación entre aplicaciones y servicios. Su tiempo de vida es configurable.
9. **Rastreabilidad:**
   - Se registra toda actividad administrativa, de acceso y uso:
     - **Administrativas:** Creación/actualización de usuarios, restablecimiento de contraseñas, desbloqueo de usuarios.
     - **De acceso:** Intentos exitosos, fallidos y bloqueos por intentos fallidos.
     - **De uso:** Visualización, modificación de datos e interacciones con expedientes en flujos de trabajo.
10. **Esquema de seguridad:**
    - **Grupos administrativos:**
      - Definen el dominio de información accesible para un usuario.
      - Son jerárquicos, permitiendo acceso a datos de grupos inferiores, pero restringiendo datos de grupos iguales o superiores.
    - **Permisos:**
      - Configuran accesos, visualización y acciones permitidas en el sistema.
      - Determinan estados operativos en flujos de trabajo.
    - **Perfiles:**
      - Agrupan permisos para actividades específicas (administradores, analistas, capturistas, etc.).
      - Un usuario puede pertenecer a varios perfiles; los permisos efectivos serán la unión de todos sus perfiles.
11. **Gestión de llaves criptográficas:**
    - Realizar copias de seguridad de los certificados y almacenarlos en medios seguros.
    - Eliminar llaves comprometidas.
    - Usar llaves diferentes para ambientes de desarrollo, UAT y producción.
    - Las cadenas de conexión para acceso a la base de datos cliente deben almacenarse en la base de datos principal (BDH).

Cumplimiento

- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.24 Uso de la criptografía.
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.2 Derechos de acceso privilegiados.
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.27 Arquitectura segura del sistema y principios de ingeniería.
- ISO / IEC 27001:2022 / A.7 Controles físicos / A.7.9 Seguridad de los activos fuera de las instalaciones.
- ISO / IEC 27001:2022 / A.5 Controles organizacionales / A.5.12 Clasificación de la información.
- ISO / IEC 27001:2022 / A.5 Controles organizacionales / A. 5.15 Control de acceso
- ISO / IEC 27001:2022 / A.5 Controles organizacionales / A.5.16 Gestión de identidades.