Capacitación Acuerdo 6573, texto ordenado 2989

- Aplicación:
  - sujetos alcanzados por los Acuerdos Nros. 2988 y 6453:
    - RENDICIÓN DE CUENTAS ENTES PÚBLICOS
    - RENDICION DE CUENTAS PERSONAS JURIDICAS PRIVADAS Y FIDEICOMISOS

- Forma y fechas de presentación:
  - Digital
    - NO impresa: Cooperando con el cuidado del medio ambiente
    - Promoviendo el trabajo colaborativo en equipos multidisciplinarios e inter-áreas
  - 15 de febrero 2022

- Vigencia:
  - A partir de enero de 2022

- **<u>Art. 1</u>**: **<u>Sistemas de información del organismo</u>**

Se deberá presentar el inventario completo (sistema de información contable y los sistemas y subsistemas que se relacionan o no con el mismo)

En el caso de que se haya implementado un solo sistema de información integral e integrado consignar los módulos o funcionalidades que abarca.

<u>Aclaraciones:</u>

1. Integración con el sistema de información contable: Automático/Manual

   Se considera integración Automática: cuando no existe intervención humana en ninguna transacción de datos.

   El resto se considerará manual.

2. Criticidad de la disponibilidad

La criticidad debe ser valorada en Alta, Media o Baja, considerando el impacto de la falta de disponibilidad de ese sistema/subsistema/módulo en la operatoria del organismo.

3. Desarrollo Propio/**Tercerizado**; Servidor de aplicaciones Propio/ **Tercerizado**; Servidor de base de Datos Propio/ **Tercerizado**

   En caso de estar **tercerizado**, indicar Proveedor o Repartición Estatal que presta el servicio

---

- **Art. 2º - Requisitos mínimos de seguridad:** del sistema de información contable y los sistemas y subsistemas implementados en el organismo.

a. **Política de Seguridad de la Información del organismo:** Normas, procedimientos, lineamientos y/o guías acordes a los procesos que lleva a cabo el organismo y su plataforma tecnológica

   Los organismos deben elaborar una Política de Seguridad de la Información relacionada con su responsabilidad primaria. Aprobada por las máximas autoridades del organismo, y comunicada a todo el personal y a aquellos terceros involucrados cuando resulte pertinente.
   Utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el organismo, su plataforma tecnológica y demás recursos de los que disponga.

   Asimismo, deberán informar, de existir, el Área del organismo o responsable con competencia en seguridad de la información; entendiendo que tiene como función principal:

   - ✓ abordar los aspectos referidos a la seguridad de la información en el diseño y la gestión de todos los proyectos que lleve adelante el organismo.
   - ✓ establecer mecanismos adecuados de seguridad para el trabajo remoto y para el uso de dispositivos móviles, según la criticidad de la información involucrada.

b. **Autenticación, Autorización y Control de Accesos:** forma de autentificación, perfiles, privilegios de acceso, métodos de autorización, gestión de altas, bajas y modificación de usuarios

c. **Uso de herramientas criptográficas:** certificados digitales utilizados en los sitios de internet del organismo y cualquier otro medio para garantizar comunicaciones seguras.

   La confidencialidad, integridad, autenticidad y/o no repudio de la información del organismo debe ser protegida mediante técnicas de cifrado, tanto en el caso de los datos que se encuentran almacenados como cuando son transmitidos.
   En este marco se solicita: detalle de los certificados digitales utilizados en todos los sitios de Internet del organismo y/o cualquier otro medio para garantizar comunicaciones seguras.

---

d. **Seguridad física y ambiental:** en el recinto donde residen el/los servidores, (bases de datos, aplicativos).

   Los activos de información del organismo deben ser protegidos mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.
   Esto implica detallar:

   - ✓ Descripción edilicia del espacio donde residen los servidores.
   - ✓ Controles físicos de ingreso/egreso, con los respectivos controles de identificación, en aquellas áreas donde se encuentren resguardados los activos de información.
   - ✓ Protección frente a interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.
   - ✓ Detección, de diferencias de temperatura, de humo, humedad; alarmas o comunicación on line con el responsable.
   - ✓ Protección anti incendios.

e. **Adquisición, desarrollo y mantenimiento de sistemas de información:** lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema.

   Para ello se debe describir:
   - ✓ Procedimiento de seguridad utilizado desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el propio organismo.
   - ✓ Controles de los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción.
   - ✓ Proceso para proteger los datos utilizados en las pruebas, preservando la confidencialidad de bases de datos reales.
   - ✓ Proceso de evaluación de la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.

f. **Manuales de operación o usuario**: poner a disposición los manuales de operación de los sistemas implementados, consignar link si los mismos se encuentran en línea.

---

g. **Gestión de incidentes de seguridad:** procedimientos para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad.

   Para ello debe describir:
   - ✓ Formas de detección, y registro de las modificaciones efectuadas en los campos clave.
   - ✓ Responsable del control y seguimiento de los mismos.

h. **Aspectos de seguridad para la continuidad de la gestión:** procedimientos existentes para mantener la operatividad del organismo durante situaciones adversas. Procedimiento de respaldo (Back up).

   Para ello se debe describir:

- ✓ Procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad y disponibilidad de la información crítica y de las instalaciones durante situaciones adversas.
- ✓ Responsables, periodicidad para la verificación y revisión de los procedimientos.

• **Art. 3º -** Los sistemas implementados estarán sujetos a una revisión permanente por este Tribunal, por lo que la documentación e información respaldatoria relacionada al sistema de información del Organismo, deberá encontrarse, a disposición del Tribunal.

• **Art. 4º -** Tener presente lo establecido en las Normas de Seguridad Informática para la Administración Pública, los "Objetivos de Control para la Información y Tecnologías relacionadas" (COBIT), los Estándares Tecnológicos de la Administración Pública Nacional (E.T.A.P.) y lo establecido por la O.N.T.I.