DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES GESTIONADOS A TRAVÉS DE SISTEMAS DE LA SECRETARÍA DE LA CONTRALORÍA DEL ESTADO.

Con base en el artículo 3, fracción XIV y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; se crea el presente documento de seguridad en el cual se cubre lo correspondiente a la gestión de datos personales a través de sistemas de información gestionados por la SECOES.

El marco jurídico del documento de seguridad se encuentra en el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes [2]físicos, electrónicos o ambos[2] en los cuales residen dichos datos y según del nivel de protección que los mismos requieran.

COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SECOES

ABRIL DEL 2023

CONTENIDO

INTRODUCCIÓN

Se elabora el presente Documento de Seguridad de conformidad con lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) se establece la obligación del responsable de elaborar un documento de seguridad.

La presente información, abarca los aspectos en materia de Tecnologías de la Información y Comunicación del Documento de Seguridad, se incluye únicamente información sobre los sistemas desarrollados, adquiridos y transferidos a la SECOES.

Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

El sistema de gestión se identifica como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la Ley General y la ley local.

Objetivo

Establecer las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales (SGSDP) para garantizar que todos los datos personales, incluyendo los datos sensibles que recabe y trate la secretaria, sean protegidos desde su obtención, registro, organización, almacenamiento, utilización y hasta su aprovechamiento, de cualquier acceso no autorizado o de cualquier tratamiento distinto a los fines para los que fueron recabados, independientemente del soporte en el que se encuentren, físico, electrónico o en redes de datos.

PARTE1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

1. Coordinación General Administrativa.

1.1. **Nombre del Sistema:** Sistema Reloj Checador ZKTECO.

1.1.1. **Responsable:**

1.1.1.1. **Unidad Administrativa:** Coordinación de Recursos humanos.

1.1.1.2. **Nombre:** Lic. Rosa María Rodríguez Ek.

1.1.1.3. **Cargo:** Coordinadora de Recursos Humanos.

1.1.1.4. **Funciones:** Control de Asistencia de Personal.

1.1.1.5. **Obligaciones:** Captura de Incidencias del personal (Vacaciones, Comisiones, Días extraordinarias y Días económicos, licencias médicas).

1.1.2. **Datos contenidos:**

1.1.2.1. **Datos Generales:** Nombre, apellido paterno, apellido materno, alias, teléfono, Extensión, Correo institucional, género, puesto, Unidad Administrativa.

1.1.2.2. **Datos Personales:** Fecha de nacimiento, dirección particular, teléfono de casa, teléfono celular, correo personal, tipo de sangre, fotografía.

1.1.2.3. **Datos Laborales:** Número de empleado, RFC, seguro social, fecha de ingreso, nivel, tipo de empleado, grupo cuatrimestral, estado, sueldo, compensación, canasta, despensa, quinquenio, apoyo a vivienda.

2. Coordinación General de los Órganos Internos de Control

2.1. **Nombre del Sistema:** Sistema de Entrega- Recepción (SENTRE).

2.1.1. **Responsable**.

2.1.1.1. **Unidad Administrativa:** Coordinación de Apoyo Jurídico de

los Órganos Internos de Control.

2.1.1.2. **Nombre:** Lic. Pastor Sima Iuit

2.1.1.3. **Cargo:** Coordinador de Apoyo Jurídico de los Órganos Internos de Control

2.1.1.4. **Funciones:** Administrar el Sistema de Entrega y Recepción (SENTRE).

Obligaciones: Creación de Unidades Administrativas;

- Creación y Asignación de Usuarios Administradores para los Enlaces del SENTRE de las Dependencias y Entidades de la Administración Pública del Estado;
- Asignación de fechas corte y liberación de Unidades Administrativas de las Dependencias y Entidades de la Administración Pública del Estado;
- Transferencias solicitadas entre Dependencias y Entidades de la Administración Pública del Estado;
- Activación de los pre cierres.

2.1.2. **Datos contenidos en el sistema.**

2.1.2.1. **Datos Personales:** Nombre, apellido materno, apellido paterno, correo electrónico y número de teléfono.

2.1.2.2. **Datos Laborales:** Cargo, empleo o comisión y dependencia de adscripción.

a. **Usuarios:** Enlaces del Sistema de entrega-Recepción en Línea (SENTRE).

b. **Funciones:**

- Operar en General el Sistema de Entrega Recepción.

c. **Obligaciones:**

- Verificación y consulta de la información de las unidades administrativas de la dependencia de su adscripción y anexos aplicables.
- Transferencias entre unidades administrativas de la dependencia de su adscripción y
- Capturar datos de los responsables de la dependencia de su adscripción

3. Coordinación General Jurídica y de Vinculación

3.1. **Nombre del Sistema:** Sistema de Evolución Patrimonial, de Declaración de Intereses y Constancia de presentación de Declaración Fiscal de la Plataforma Digital Estatal (S1).

3.1.1. **Responsable**

3.1.1.1. **Área usuaria:** Coordinación General Jurídica y de Vinculación.

3.1.1.2. **Responsable:** Lic. Lucas Alejandro Padilla Franyutti

3.1.1.3. **Cargo:** Coordinador de Situación Patrimonial.

3.1.1.4. **Funciones:** Verificación y consulta de las declaraciones patrimoniales.

3.1.1.5. **Obligaciones:**

- Consulta en el Sistema del Estatus de las declaraciones patrimoniales de los servidores públicos.

3.1.1.6. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombré, apellido materno, apellido paterno, número de teléfono, correo electrónico, nacionalidad y país de nacimiento, fecha de nacimiento, nivel académico, domicilio, R.F.C. sueldo, estado civil, régimen matrimonial, percepciones anuales, C.U.R.P., bienes muebles e inmuebles, del declarante y sus dependientes económicos, así como del cónyuge o concubino.

b. **Datos Laborales:** Situación, nivel, tipo de plaza, nombre del ente público, empleo cargo o comisión, función principal, fecha de posesión, teléfono de oficina y domicilio del empleo.

3.1.1.7. **Encargados:** No aplica.

3.1.1.8. **Usuarios:** Enlaces del Sistema designados por los titulares de cada dependencia y Entidades de la Administración Pública Estatal...

- **Cargo:** Área de recursos humanos u homóloga.
- **Funciones:** Administrar y operar el sistema S1.
- **Obligaciones:** Identificar, determinar y capturar datos de los datos de las personas servidoras públicas adscritas a estos y que les sea exigible la presentación de las declaraciones de Situación patrimonial y de Intereses o del aviso por cambio de dependencia, incluyendo la categorización de los formatos en que deberán presentarlas, dar usuarios y contraseñas y, activar o desactivar las declaraciones de situación patrimonial y de intereses que les corresponda.

4. Coordinación General de Fiscalización de Obra Pública, Adquisiciones y Servicios.

4.1. **Nombre del Sistema:** Guardianes de la Obra Pública.

4.1.1. **Responsable:**

4.1.1.1. **Unidad Administrativa:** Coordinación General de Fiscalización De Obra Pública, Adquisiciones Y Servicios

4.1.1.2. **Nombre:** Arq. Ángel Leopoldo Sánchez González.

4.1.1.3. **Cargo:** Coordinador General de Fiscalización de Obra Pública, Adquisiciones y Servicios.

4.1.1.4. **Funciones:** Monitoreo del sistema.

4.1.1.5. **Obligaciones:** Coordinar la verificación de la información cargada en el sistema por parte del personal adscrito a la Coordinación General de Fiscalización de Obra Pública, Adquisiciones y Servicios, así como de Instancias ejecutoras referente a la obra pública.

4.1.1.6. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombré y apellidos, número de teléfono.
b. Datos laborales: Número de empleado, Cargo.

4.1.2. **Usuarios:**

4.1.2.1. **Nombre:** Nicolas Puga Mendoza

4.1.2.2. **Cargo:** Coordinador de supervisión de obra pública, adquisiciones y servicios.

4.1.2.3. **Funciones:** Monitoreo del Sistema y elaboración de Informes.

4.1.2.4. **Obligaciones:** Coordinar la verificación de la información cargada en el sistema por parte de las Instancias ejecutoras referente a la obra pública, así como los informes del personal adscrito a la Coordinación de Supervisión de Obra Pública, Adquisiciones y Servicios y Elaborar y monitorear informes de Supervisión Técnica

4.1.2.5. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.6. **Nombre:** C. Sergio André Herrera Romero

4.1.2.7. **Unidad Administrativa:** Departamento de Supervisión Técnica de Obra Pública.

4.1.2.8. **Cargo:** Jefe del Departamento de Supervisión Técnica de Obra Pública

4.1.2.9. **Funciones:** Monitoreo del Sistema y elaboración de Informes.

4.1.2.10. **Obligaciones:** Realizar la asignación de las Instancias ejecutoras que los supervisores verificarán para comprobar la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como verificar los

informes del personal adscrito a su departamento con respecto las verificaciones realizadas, y realizar el monitoreo de la información cargada por las Instancias Ejecutoras y Elaborar informes de Supervisión Técnica.

4.1.2.11. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.12. **Nombre:** Arq. Jesús Alberto Bañuelos Jiménez
4.1.2.13. **Unidad Administrativa:** Departamento de Supervisión Técnica de Obra Pública.
4.1.2.14. **Cargo:** Analista Profesional
4.1.2.15. **Funciones:** Monitoreo del Sistema y elaboración de Informes.
4.1.2.16. **Obligaciones:** Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar los informes respectivos, para remitirlos al Jefe del Departamento de Supervisión Técnica de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) verificada(s) y Elaborar informes de Supervisión Técnica
4.1.2.17. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.18. **Nombre:** Ing. José Carlos Tut Martínez
4.1.2.19. **Unidad Administrativa:** Departamento de Supervisión Técnica de Obra Pública.
4.1.2.20. **Cargo:** Supervisor de Obra
4.1.2.21. **Funciones:** Monitoreo del Sistema y elaboración de Informes.
4.1.2.22. **Obligaciones:** Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar los informes respectivos, para remitirlos al Jefe del Departamento de Supervisión Técnica de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) verificada(s) y Elaborar informes de Supervisión Técnica
4.1.2.23. **Datos contenidos en el sistema:**

a. **Datos personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.24. **Nombre:** Ing. Jonathan Azur Rosado Caballero
4.1.2.25. **Unidad Administrativa:** Departamento de Supervisión

Técnica de Obra Pública.

4.1.2.26. **Cargo:** Supervisor de Obra

4.1.2.27. **Funciones:** Monitoreo del Sistema y elaboración de Informes.

4.1.2.28. **Obligaciones:** Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar los informes respectivos, para remitirlos al Jefe del Departamento de Supervisión Técnica de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) verificada(s) y Elaborar informes de Supervisión Técnica

4.1.2.29. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.30. **Nombre:** Ing. Antonio González Landero

4.1.2.31. **Unidad Administrativa:** Departamento de Supervisión Técnica de Obra Pública.

4.1.2.32. **Cargo:** Supervisor de Obra

4.1.2.33. **Funciones:** Monitoreo del Sistema y elaboración de Informes.

4.1.2.34. **Obligaciones:** Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar los informes respectivos, para remitirlos al Jefe del Departamento de Supervisión Técnica de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) verificada(s) y Elaborar informes de Supervisión Técnica

4.1.2.35. **Datos contenidos en el sistema:**

a. **Datos personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.36. **Nombre:** Ing. Ángel Rey Pérez Trujeque

4.1.2.37. **Unidad Administrativa:** Departamento de Análisis de Precios Unitarios.

4.1.2.38. **Cargo:** Jefe del Departamento de Análisis de Precios Unitarios.

4.1.2.39. **Funciones:** Monitoreo del Sistema y supervisión.

4.1.2.40. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública y Realizar la consulta y revisión de las tarjetas de precios unitarios que las Instancias ejecutoras de obra cargan en el sistema según le sea solicitado por el Coordinador de Supervisión de Obra Pública, Adquisiciones y Servicios.

4.1.2.41. **Datos contenidos en el sistema:**
   a. **Datos Personales:** Nombre y apellidos, número de teléfono.
   b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.42. **Nombre:** Arq. José Luis León León
4.1.2.43. **Unidad Administrativa:** Departamento de Análisis de Precios Unitarios.
4.1.2.44. **Cargo:** Analista Profesional
4.1.2.45. **Funciones:** Monitoreo del Sistema y supervisión.
4.1.2.46. **Obligaciones:** Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar los informes respectivos, para remitirlos al Jefe del Departamento de Supervisión Técnica de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) verificada(s).
4.1.2.47. **Datos contenidos en el sistema:**
   a. **Datos Personales:** Nombre y apellidos, número de teléfono.
   b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.48. **Nombre:** Ing. Gustavo Misael Caamal Poot.
4.1.2.49. **Unidad Administrativa:** Departamento de Análisis de Precios Unitarios.
4.1.2.50. **Cargo:** Supervisor de Obra.
4.1.2.51. **Funciones:** Monitoreo del Sistema y supervisión.
4.1.2.52. **Obligaciones:** Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar los informes respectivos, para remitirlos al Jefe del Departamento de Supervisión Técnica de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) verificada(s).
4.1.2.53. **Datos contenidos en el sistema:**
   a. **Datos personales:** Nombre y apellidos, número de teléfono.
   b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.54. **Nombre:** C. Joaquín Enrique Domínguez Cruz
4.1.2.55. **Unidad Administrativa:** Departamento de Verificación de Obra con Laboratorio Móvil.
4.1.2.56. **Cargo:** Jefe del Departamento de Verificación de Obra con Laboratorio Móvil
4.1.2.57. **Funciones:** Monitoreo del Sistema y laboratorio.

4.1.2.58. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública; Elaborar y monitorear informes referentes a pruebas de calidad de laboratorio de las obras verificadas.

4.1.2.59. **Datos contenidos en el sistema:**

a. **Datos personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.60. **Nombre:** M. C. Ileana Guadalupe Poot Ocejo

4.1.2.61. **Unidad Administrativa:** Departamento de Verificación de Obra con Laboratorio Móvil.

4.1.2.62. **Cargo:** Laboratorista.

4.1.2.63. **Funciones:** Monitoreo del Sistema y laboratorio.

4.1.2.64. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública; Elaborar y monitorear informes referentes a pruebas de calidad de laboratorio de las obras verificadas.

4.1.2.65. **Datos contenidos en el sistema:**

a. **Datos personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.66. **Nombre:** C. José Vladimir Tuz Canto

4.1.2.67. **Unidad Administrativa:** Departamento de Verificación de Obra con Laboratorio Móvil.

4.1.2.68. **Cargo:** Laboratorista.

4.1.2.69. **Funciones:** Monitoreo del Sistema y laboratorio.

4.1.2.70. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública; Elaborar y monitorear informes referentes a pruebas de calidad de laboratorio de las obras verificadas.

4.1.2.71. **Datos contenidos en el sistema:**

a. **Datos personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.72. **Nombre:** Ing. Víctor Manuel Briceño García

4.1.2.73. **Unidad Administrativa:** Departamento de Verificación de Obra con Laboratorio Móvil.

4.1.2.74. **Cargo:** Laboratorista.

4.1.2.75. **Funciones:** Monitoreo del Sistema y laboratorio.

4.1.2.76. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública;

Elaborar y monitorear informes referentes a pruebas de calidad de laboratorio de las obras verificadas.

4.1.2.77. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.78. **Nombre:** Ing. Marvin Daniel Arellano de la Cruz
4.1.2.79. **Unidad Administrativa:** Departamento de Verificación de Obra con Laboratorio Móvil.
4.1.2.80. **Cargo:** Laboratorista Técnico de Obra.
4.1.2.81. **Funciones:** Monitoreo del Sistema y laboratorio.
4.1.2.82. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública; Elaborar y monitorear informes referentes a pruebas de calidad de laboratorio de las obras verificadas.
4.1.2.83. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.84. **Nombre:** C. Cesar Augusto Herrera Romero
4.1.2.85. **Unidad Administrativa:** Departamento de Verificación de Obra con Laboratorio Móvil.
4.1.2.86. **Cargo:** Laboratorista Técnico de Obra
4.1.2.87. **Funciones:** Monitoreo del Sistema y laboratorio.
4.1.2.88. **Obligaciones:** Realizar la consulta de la información cargada en el sistema por las Instancias Ejecutoras de obra pública; Elaborar y monitorear informes referentes a pruebas de calidad de laboratorio de las obras verificadas.
4.1.2.89. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.90. **Nombre:** Ing. Graciela Borges Zepeda.
4.1.2.91. **Unidad Administrativa:** Coordinación de Auditoría de Obra Pública, Adquisiciones y Servicios
4.1.2.92. **Cargo:** Coordinadora de Auditoría de Obra Pública,

Adquisiciones y Servicios.

4.1.2.93. **Funciones:** Auditar la información de obra generada por las unidades ejecutoras.

4.1.2.94. **Obligaciones**: Auditar la información generada por las unidades ejecutoras y registrar las observaciones que se generen.

4.1.2.95. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo.

4.1.2.96. **Nombre:** C. Israel Caamal Castillo.

4.1.2.97. **Unidad Administrativa:** Departamento de Auditoría de Obra Pública.

4.1.2.98. Departamento de Auditoría de Obra Pública.

4.1.2.99. **Cargo:** Jefe del Departamento de Auditoría de Obras

4.1.2.100. **Funciones:** Coordina las solvataciones que aporten las unidades ejecutoras observadas.

4.1.2.101. **Obligaciones**: Consulta la información de obra de las unidades ejecutoras y también las observaciones generadas en el proceso de auditoría. Genera las observaciones de solvatación.

4.1.2.102. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo

4.1.2.103. **Nombre:** Ing. Briseida Tome Reyna

4.1.2.104. **Unidad Administrativa:** Departamento de Auditoría de Obra Pública.

4.1.2.105. Departamento de Auditoría de Obra Pública.

4.1.2.106. **Cargo:** Analista Profesional

4.1.2.107. **Funciones:** Monitoreo del sistema.

4.1.2.108. **Obligaciones**: Realizar la verificación de la información cargada en el sistema de la Instancia (s) ejecutora (s) referente a la obra pública, así como realizar la captura de los resultados de las Auditorías de obra pública llevadas a cabo, para remitirlos al Jefe del Departamento de Auditorías de Obra Pública para su revisión y aprobación, para ser remitidos a la(s) Instancia(s) Ejecutora(s) Auditadas(s).

4.1.2.109. **Datos contenidos en el sistema:**

a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo

4.1.2.110. **Nombre:** Arq. Yosuara Amairani Parra Góngora
4.1.2.111. **Unidad Administrativa:** Departamento de Auditoría de Obra Pública.
4.1.2.112. **Área administrativa:** Departamento de Auditoría de Obra Pública.
4.1.2.113. **Cargo:** Auditora
4.1.2.114. **Funciones:** Captura de resultados de auditoría.
4.1.2.115. **Obligaciones**: Captura de resultados de las Auditorías realizadas a obras públicas, adquisiciones y servicios
4.1.2.116. **Datos contenidos en el sistema:**
a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo

4.1.2.117. **Nombre:** C. Pamela Yoshira Alamilla Juárez
4.1.2.118. **Unidad Administrativa:** Departamento de Auditoría Financiera de Obra Pública.
4.1.2.119. **Cargo:** Auditor (financiero)
4.1.2.120. **Funciones:** Captura de resultados de auditoría.
4.1.2.121. **Obligaciones**: Captura de resultados de las Auditorías realizadas a obras públicas, adquisiciones y servicios
4.1.2.122. **Datos contenidos en el sistema:**
a. **Datos Personales:** Nombre y apellidos, número de teléfono.
b. **Datos laborales:** Número de empleado, Cargo

5. Coordinación General de Investigación.

5.1. **Nombre del Sistema:** Sistema de Denuncia ciudadana.
5.1.1. **Unidad Administrativa:** Coordinación General de Investigación.
5.1.1.1. **Nombre Responsable:** C. Ana Karen Peña Sánchez.
5.1.1.2. **Cargo:** Coordinadora de Quejas y Denuncias.
5.1.1.3. **Funciones:** Recibir, clasificar y tramitar las manifestaciones ciudadanas que se presenten sobre los trámites y servicios a cargo de la administración pública estatal y actos u omisiones que que pudieran constituir o vinculantes con faltas administrativas.
5.1.1.4. **Obligaciones:** Atender, clasificar, tramitar y concluir las manifestaciones ciudadanas que se presenten sobre los trámites y servicios a cargo de la administración pública estatal, y actos u omisiones que pudieran constituir o vinculantes con faltas administrativas.
5.1.1.5. **Datos personales contenidos en el sistema**: RFC, CURP, número de seguridad social, apellido paterno, apellido

materno, nombre, estado civil, lugar de nacimiento, sexo, domicilio, nivel académico, licenciatura y tipo de discapacidad.

5.1.2. **Encargado #1:** Lic. Margely Alicia Castro Santeliz.

5.1.2.1. **Cargo del encargado #1:** Coordinador General de Investigación.

5.1.2.2. **Funciones del encargado #1:** coordinar los medios de captación ciudadana establecidos para la atención, trámite y conclusión de las manifestaciones ciudadanas que se presenten, vigilando la aplicación de los lineamientos o disposiciones generales que regulen los procedimientos para su atención trámite y conclusión.

5.1.2.3. **Obligaciones del encargado #1:** Vigilar, supervisar y ordenar que se dé trámite a las manifestaciones ciudadanas que se presenten sobre los trámites y servicios a cargo de la administración pública estatal y actos u omisiones que pudieran constituir o vinculantes con faltas administrativas.

5.1.3. **Nombre del encargado #2:** Alejandra Santiago Pablo.

5.1.3.1. **Cargo del encargado #2:** Jefa del Departamento de Denuncias A.

5.1.3.2. **Funciones del encargado #2:** Proyectar los acuerdos y oficios para atender, tramitar las denuncias, quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la administración pública estatal.

5.1.3.3. **Obligaciones del encargado #2:** Atender las denuncias de quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la administración pública estatal, dentro de los plazos y términos señalados en las disposiciones legales aplicables.

5.1.4. **Nombre del encargado #3:** Luigina Karel Cristerna Guerrero.

5.1.4.1. **Cargo del encargado #3:** Jefa del Departamento de Denuncias B.

5.1.4.2. **Funciones del encargado #3:** Proyectar los acuerdos y oficios para atender, tramitar las denuncias, quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la administración pública estatal.

5.1.4.3. **Obligaciones del encargado #3:** Atender las denuncias de quejas, reconocimientos y solicitudes que se presenten sobre

los trámites y servicios a cargo de la administración pública estatal, dentro de los plazos y términos señalados en las disposiciones legales aplicables.

5.1.5. **Nombre del encargado #4:** Heidy Joanna Liceas Rodríguez.
5.1.5.1. **Cargo del encargado #4:** Auxiliar Jurídico.
5.1.5.2. **Funciones del encargado #4:** Proyectar los acuerdos y oficios para atender, tramitar las denuncias, quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la administración pública estatal.
5.1.5.3. **Obligaciones del encargado #4:** Atender las denuncias de quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la administración pública estatal, dentro de los plazos y términos señalados en las disposiciones legales aplicables.

5.1.6. Usuarios.
5.1.6.1. **Nombre del usuario:** Órganos Internos de Control.
5.1.6.2. **Cargo del usuario:** Órganos Internos de Control.
5.1.6.3. **Funciones del encargado:** Conocer el estatus de las denuncias, quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la entidad y/o dependencia de los cuales funjan como OIC.
5.1.6.4. **Obligaciones del encargado:** Colaborar con las solicitudes de información y documentación que solicite la coordinación de Quejas y Denuncias respecto a las denuncias, quejas, reconocimientos y solicitudes que se presenten sobre los trámites y servicios a cargo de la entidad y/o dependencia de los cuales funjan como OIC.

6. Coordinación General de Planeación y Contraloría Social.

6.1. **Nombre del Sistema:** Guardianes de la Obra Pública (Módulo Contraloría Social).
6.1.1. **Unidad Administrativa:** Coordinación Operativa de Contraloría Social.
6.1.1.1. **Responsable:** Lic. Juan de Dios Noh Dzul.
6.1.1.2. **Cargo:** Coordinador operativo de Contraloría Social.

6.1.1.3. **Funciones:** Consulta de información para generar estadística de la ciudadanía atendida en los eventos de materia de Contraloría Social, así como, monitorear la captura de información relacionada con la Contraloría Social realizada por las instancias ejecutoras de obras públicas con la finalidad de verificar el cumplimiento sobre las acciones de promoción de esta política social.

6.1.1.4. **Obligaciones:** Brindar capacitación o asesoría a los usuarios de las instancias ejecutoras acerca del proceso de registro de la información en el apartado de Contraloría Social, la cual es recabada en las actividades de difusión, capacitación y seguimiento dirigidas a la ciudadanía beneficiada con los recursos públicos.

6.1.1.5. **Datos personales:** Nombre, apellido paterno, apellido materno, teléfono, Sexo, dirección, correo electrónico, ciudad, municipio, estado y país.

6.1.1.6. Usuarios:

6.1.1.7. **Nombre:** Lic. Juan de Dios Noh Dzul

6.1.1.8. **Cargo:** Coordinador operativo de Contraloría Social.

6.1.1.9. **Funciones:** Consulta de información para generar estadística de los usuarios que se han registrado y culminado el curso virtual auto formativo.

6.1.1.10. **Obligaciones:** Brindar atención a los usuarios sobre cualquier duda o aclaración durante el desarrollo de la Capacitación de Contraloría Social.

6.1.1.11. Datos Personales Contenidos en el Sistema: Nombre(s), apellido(s), teléfono, correo electrónico, ciudad, municipio, país.

7. Coordinación General de Sustanciación y Resoluciones.

7.1. **Nombre del Sistema:** Sistema de Consulta de Servidores Públicos Sancionados.

7.1.1. **Área usuaria:** Coordinación General de Sustanciación y Resoluciones en conjunto con la mesa de Resoluciones “A” y los Jefes de Departamento de Resoluciones 1 y 2.

7.1.1.1. **Responsable:** Letifica Olguin Vargas.

7.1.1.2. **Cargo:** Coordinador General de Sustanciación y Resoluciones.

7.1.1.3. **Funciones:** Procesar información y enviar los datos necesarios mediante la cédula de inscripción para el registro de la sanción o sanciones impuestas.

7.2. **Nombre del Sistema:** Sistema de Consulta de Servidores Públicos Sancionados.
7.2.1. **Área usuaria:** Coordinación de Tecnologías de la Información.
7.2.1.1. **Responsable:** Lic. Adolfo Eduardo Vazquez Salazar.
7.2.1.2. **Cargo:** Coordinador de Tecnologías de la Información.
7.2.1.3. **Funciones:** Inscripción de la sanción o sanciones impuestas en el sistema.

8. Coordinación General de Auditoría y Control Interno.

8.1. **Nombre del Sistema:** Registro Único de Servidores Públicos para Entidades Federativas.
8.1.1. **Unidad Administrativa:** Coordinación General de Auditoría y Control Interno.
8.1.1.1. **Responsable:** Ing. Víctor Alfonso Yam Cahuil.
8.1.1.2. **Cargo:** Coordinador General de Auditoría y Control Interno.
8.1.1.3. **Funciones:** Generar usuarios y contraseñas a los enlaces de cada entidad pública estatal, así como generar un reporte para la publicación de la información en la página de la Contraloría.
8.1.1.4. **Obligaciones:** Generar usuarios y contraseñas a los enlaces de cada entidad pública estatal, para que realicen la identificación, clasificación y registro de los servidores públicos de las mismas, así como generar reporte para la publicación de la información en la página de la Contraloría, para dar cumplimiento a lo establecido en el art. 43 de la ley General de Responsabilidades Administrativas.
8.1.1.5. **Datos personales en el sistema**: Institución, Nombre completo y puesto dentro de la Institución pública.

9. Coordinación de Tecnologías de la Información.

9.1. **Nombre del Sistema:** Plataforma de Capacitación en Línea.
9.1.1. **Responsable:** Lic. Adolfo Eduardo Vazquez Salazar.
9.1.1.1. **Unidad Administrativa:** Coordinación de Tecnologías de la Información
9.1.1.2. **Nombre:** Lic. Adolfo Eduardo Vazquez Salazar.
9.1.1.3. **Cargo:** Coordinador de Tecnologías de la Información
9.1.1.4. **Funciones:** Procurar la disponibilidad tecnológica de la plataforma para uso del personal, Alta de usuarios capacitadores.
9.1.1.5. **Obligaciones:** Brindar atención a los usuarios capacitadores para publicar y operar la plataforma con respecto a sus correspondientes cursos. Brindar capacitación para la publicación de contenidos.
9.1.1.6. Datos Personales Contenidos en el Sistema: Nombre(s), apellido(s),

teléfono, correo electrónico, ciudad, municipio, país.

9.2. **Nombre del Sistema:** Directorio Único de Gobierno

9.2.1. **Responsable:** Lic. Adolfo Eduardo Vazquez Salazar.

9.2.1.1. **Unidad Administrativa:** Coordinación de Tecnologías de la Información

9.2.1.2. **Nombre:** Lic. Adolfo Eduardo Vazquez Salazar.

9.2.1.3. **Cargo:** Coordinador de Tecnologías de la Información

9.2.1.4. **Funciones:** Implementar estrategias para procurar la alimentación del directorio por parte de las diferentes instituciones del poder ejecutivo.

9.2.1.5. **Obligaciones:** Garantizar la operatividad del directorio Único, dar soporte técnico y capacitación a las diferentes instituciones del poder ejecutivo.

9.2.1.6. **Datos Personales Contenidos en el Sistema**: Nombre(s), apellido(s), CURP, Último grado de Estudios, Teléfono, Correo electrónico, Puesto, Cargo, Número de Empleado, Número de Seguridad Social, Tipo de Sangre

RIESGO	ETAPA DEL CICLO	AMENAZA IDENTIFICADA
ACCESO NO AUTORIZADO	Almacenamiento de los datos	Pérdida del equipo o fuga de información
MODIFICACIÓN NO AUTORIZADA	TRATAMIENTO	Ataque cibernético para la suplantación de identidad y cuentas bancarias
ELIMINACIÓN DE DATOS	TRATAMIENTO	Fallo en el suministro eléctrico / desastres naturales

PARTE 2. POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES O BUENAS PRÁCTICAS.

Políticas internas definidas por la CTI aplicables a todos los sistemas.

1. **Seguridad de accesos a los sistemas.**
   1.1. **Área usuaria**. Por cada sistema, siempre existe un área usuaria quien es la responsable del proceso con base a sus facultades y atribuciones. Por ejemplo, para el sistema de entrega recepción (SENTRE), el área usuaria es el responsable del proceso de entrega recepción, en este caso, la Coordinación de Entrega-Recepción.
   1.2. Para los sistemas desarrollados o adquiridos, siempre deberá existir el rol del área usuaria.
   1.3. Para asignar a un servidor público con rol de Área Usuaria, deberá existir una solicitud por escrito suscrita por el titular del área responsable del proceso, señalando los datos del servidor público:
   - Nombre completo
   - Cargo
   - Número de empleado
   - Correo electrónico institucional
   - Correo electrónico personal.
   - Número telefónico de su oficina.
   - Número de celular.
   - Señalar que está de acuerdo con que se le contacte a su celular.

   1.4. Se le dará respuesta a solicitud indicando que la información de sus credenciales de acceso, se enviarán al correo electrónico del servidor público señalado en la solicitud.
   1.5. Se capacita al usuario en la administración del sistema, donde se le explica cómo crear nuevos usuarios con roles inferiores que colaboran en alguna parte del proceso.

1.6. El servidor público asignado como responsable del área usuaria, firma el documento de responsabilidad de administración de los sistemas.

2. Norma o mejor práctica implementada:

2.1. Los sistemas web y las bases de datos se encuentran alojados en equipos de tipo servidor y con sistemas operativos especiales que implementan una seguridad de acceso más alta a la convencional.

2.2. Estos equipos servidores están físicamente aislados del acceso y sólo el personal técnico autorizado puede tener acceso a este SITE. Los sistemas cuentan con sub procesos alternos que almacenan las actividades prioritarias en bitácoras dentro de la base de datos de cada sistema.

2.3. Todos los sistemas cuentan con accesos controlados mediante contraseñas seguras y optimizadas mediante criterios de control en el ingreso de caracteres; también cuenta con subprocesos de actividades mediante roles que limitan los privilegios y las acciones que pueden realizan los usuarios dentro del sistema y la información a la que pueden acceder.

2.4. El alta y baja de los usuarios estándar la realiza el área usuaria mediante su usuario administrador. Al tener la facultad del tratamiento de la información en su sistema cada usuario administrador determina su proceso de entrega de usuarios y el rol que va ejercer en el sistema.

2.5. El análisis y desarrollo de sistemas informáticos se realizan a solicitud de las Unidades Administrativas responsables del tratamiento de la información y se lleva a cabo mediante los procedimientos vigentes y metodologías de acopio de información, diseño de sistemas que mejor se adapten al proyecto a desarrollar.

2.6. Los sistemas que son transferidos por otras instituciones o adquiridos bajo licenciamiento a la Secretaría, cuentan con los accesos por roles y contraseñas seguras, de igual forma se encuentran alojados en el SITE de la Secretaría por lo cual, le aplican las medidas antes señaladas.

PARTE 3. ANÁLISIS DE RIESGO.

Aplicables a todos los sistemas.

1. **Tipo de soporte:** Los sistemas de información relacionados en este documento, se encuentran almacenados y operando en servidores físicos de la Secretaría. Cuentan con soporte digitales como control de versiones, ya que se realizan respaldarlos antes de implementar cambios en el código. La información que procesan los sistemas se encuentra en gestores de base datos y están automatizados los respaldos diarios, semanales o mensuales según se requiera.

2. **Características del lugar donde se resguardan los soportes:** Los equipos que contienen los sistemas y las bases de datos que se requieren para su funcionamiento, se encuentran alojados en el SITE de servidores de la Secretaría, el cual está restringido el acceso ya que requieren llave física para poder ingresar.

3. **Amenazas y vulnerabilidades:**

    a. Vulnerabilidad física o ambiental: Los equipos se encuentran en una zona que tiene riesgo de impacto de huracanes cada año.

- Consecuencias:
  El SITE se encuentra en la primera planta y es susceptible a inundaciones cuando hay lluvias intensas, lo que pone en riesgo el equipamiento en servidores que alojan los sistemas. Esto podría representar pérdida de información por daño de los equipos;

- Acciones:
  Para evitar daños por inundación, todos los equipos que lo permiten, están colocados arriba del nivel del piso.

  Para disminuir el riesgo, se requiere elevar el nivel del piso de los Sites a través de la implementación de un piso falso.

  Para eliminar el riesgo, se tiene que trasladar el SITE a la segunda planta del edificio o a otra ubicación geográfica segura.

    b. Vulnerabilidad económica: No hay presupuesto asignado para la actualización de la infraestructura tecnológica y/o renta de nube pública para respaldo en espejo en otra zona geográfica.

- Consecuencias:
  Riesgo de no integridad de la información, pérdida parcial o total, dañó a los equipos activos.
- Acciones:
  Solicitud de inversión para actualización con base a proyectos enfocados a las funciones sustantivas.

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDAD	EJEMPLO DE AMENZA	POSIBLES CONSECUENCIAS
Software	No cerrar la sesión al abandonar la computadora.	Acceso no autorizado	Pérdida, destrucción robo, extravío o copia no autoriza- da, uso, acceso o tratamiento no autorizado daño, altera- ción o modificación
Redes	Falta de mecanismos de identificación y autenticación del usuario	Suplantación de identidad	
Personal	Servidores público no sensibilizados en la materia de protección de datos personales.	Fraude y robo	Uso, acceso o tratamiento no autorizado.

PARTE 4. ANÁLISIS DE LA BRECHA.

Aplicables a todos los sistemas.

1. Transmisiones de datos personales

1.1. **Transmisiones mediante el traslado de soportes físicos:**
Esta Coordinación de Tecnologías de la Información no maneja el traslado de información de forma física impresa, por lo que no requiere de aplicar medidas de seguridad en este tema.

1.2. **Transmisiones mediante el traslado de soportes electrónicos:**

- La información que generan los sistemas se mantiene en los equipos servidores que los contienen y solo son tratados a través de los sistemas y los usuarios autenticados, no se cifran ya que son manejo del Sistema Operativo. En caso de que se requiera cambio de plataforma o equipo se generan los backups en

archivos de tipo SQL; estos son los que se trasladan al nuevo equipo y posteriormente se eliminan de forma segura.

1.3. **Transmisiones mediante el traslado sobre redes electrónicas:**

- No se ha requerido realizar este tipo de transmisiones.

2. Resguardo de sistemas de datos personales con soportes físicos.

Esta Coordinación de Tecnologías de la Información no maneja respaldo de los sistemas de forma física impresa, por lo que no requiere de aplicar medidas de seguridad en este tema.

3. Bitácoras para accesos y operación cotidiana.

3.1. Bitácoras electrónicas de acceso a los sistemas de información.

- Tanto los sistemas operativos en los que corren los sistemas, así como los gestores de servicios web generan sus bitácoras electrónicas de acceso y errores, pero por falta de personal especializado, sólo se revisan en caso de fallo o error reportado.
- Los sistemas cuentan con tablas de sesiones que registran la fecha y hora del último acceso del usuario y las bitácoras de los sistemas contienen las actividades significativas de los usuarios.
- Las bitácoras sólo se revisan en caso de reporte o para verificar y corregir errores en los sistemas, ya que no se cuenta con personal dedicado a esta actividad.

3.2. Si las bitácoras están en soporte físico o en soporte electrónico.

- Las bitácoras electrónicas forman parte de las bases de datos de los sistemas y se encuentran alojado en los equipos servidores que se resguardan en el SITE de la Secretaría. Su tiempo de vida depende del tiempo que esté en función el sistema.

3.3. Respecto del análisis de las bitácoras.

- No se cuenta con personal dedicado al análisis de bitácoras por falta de presupuesto.

- En el caso de que se requiera revisión de las bitácoras a solicitud o por un incidente detectado, el área responsable es el Departamento de Desarrollo de Sistemas e Infraestructura Tecnológica.
- Las bitácoras del sistema operativo son gestionadas y protegidas automáticamente por el sistema operativo y al momento no se cuenta con un proceso de respaldo ni de análisis.
- No se cuenta con ninguna aplicación de análisis o de generación de estadísticos en base al tratamiento de las bitácoras.

3.4. Registro de incidentes.

En caso de incidentes, se realizará el siguiente procedimiento:

- El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes electrónicos afectados y, en su caso, los recuperados.
- El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados.
- En caso de robo o extravío de información de algún sistema, el Coordinador de la CTI, al tener conocimiento del incidente, da vista al titular de la dependencia.
- En caso de ser un incidente delictivo por robo a vandalismo, por ejemplo, se hace de conocimiento al titular del área jurídica.

4. Acceso a las instalaciones

4.1. **Seguridad perimetral exterior** del edificio donde se encuentra el equipo activo para la operación de los sistemas de información.

- Se cuenta con personal de vigilancia para el acceso al edificio, el cual solicita la identificación de las personas y si

consulta con el área que desea visitar si se autoriza el acceso.

- El personal de vigilancia es administrado por la Coordinación General Administrativa, por lo que ellos son los que determinan los criterios de acceso que aplica la vigilancia.

4.2. **Seguridad perimetral interior** para el centro de datos para soportes electrónicos:

- El SITE de servidores está siempre cerrado bajo llave y sólo lo puede acceder personal de la CTI autorizado por el Coordinador o el Jefe del Departamento de Desarrollo de Sistemas e Infraestructura Tecnológica.
- Si algún proveedor u otra institución requiere acceso, este es autorizado por el Coordinador de la CTI y es acompañado por personal del Departamento de Desarrollo de Sistemas e Infraestructura Tecnológica.

  Debe existir solicitud previa de la solicitud de acceso e instrucción del Coordinador de la CTI de permitirlo.

  Debe presentar credenciales de la empresa que representa o de la Institución.

  El acceso se autoriza en respuesta a la solicitud de acceso ya sea de forma escrita, correo electrónico o registro en la Mesa de Ayuda.

5. **Actualización de la información contenida en el sistema.**

Este apartado refiere al mecanismo o procedimiento institucional para la actualización de la información personal contenida en los sistemas, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

5.1. Para la actualización de los datos personales de alguna persona.

- Toda vez que la Coordinación General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (CGTAIPPDP) es quien recibe las solicitudes de actualización de datos personales, debe existir una solicitud por escrito de su titular dirigido al Coordinador de la CTI, con

copia al área usuaria del sistema en el cual se desea actualizar el dato personal.

6. Perfiles de usuario y contraseñas

6.1. El Modelo de control de acceso está basado en roles de usuarios y perfiles de grupos.

6.2. Perfiles de usuario y contraseñas manejados por el software aplicativo de los sistemas:

- Los sistemas ofrecen un manejo riguroso de perfiles de usuario y contraseñas.
- Los sistemas cifran las contraseñas cuando las almacenan.

6.3. Administración de perfiles de usuario y contraseñas:

- Por cada sistema existe un área usuaria con un responsable de la creación de sus respectivos usuarios.
- Los perfiles de usuarios están creados mediante código y creados a medida del proceso administrativo con base al análisis del proceso sobre el cual fue desarrollado.
- Nuevos perfiles en los sistemas son creados a solicitud del área usuaria con autorización del Coordinador en respuesta a la solicitud del área usuaria.

6.4. Acceso remoto a sistemas de información.

- Los usuarios generales no requieren acceso remoto a sus equipos de cómputo que por lo general utilizan para trabajar con el sistema.
- Los administradores de los sistemas no requieren acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento, ya que el acceso es local.

7. Procedimientos de respaldo y recuperación de datos.

7.1. Se realizan respaldos completos de las bases de datos por sistema.

7.2. Los respaldos se realizan y se resguardan en los equipos servidores que se alojan en el SITE de la Secretaría y en medios digitales designados para tal fin, resguardados fuera

del SITE.

7.3. Los respaldos son generados automáticamente por las aplicaciones gestoras de base de datos y los servicios de los Sistemas Operativos.

7.4. Se realizan respaldos por indicación del Coordinador de la CTI, cuando hay actualización de sistemas o de infraestructura donde se soporta el sistema.

8. **Plan de contingencia.**

8.1. El plan de contingencia se encuentra en desarrollo. Aunque no se cuenta con un plan de contingencia como tal, sí existe el conocimiento de criterios para la cultura de protección de datos y más por las implicaciones de estar en una zona de alto riesgo de impacto de huracanes

8.2. No se cuenta con un sitio redundante debido a la limitación de recursos económicos para TICS.

9. **Medidas de seguridad deseadas**

9.1. Se debe contar con personal dedicado al análisis de la actividad de los usuarios en los sistemas y en los servicios de la red interna, esto permite identificarlas secciones vulnerables y realizar las correcciones necesarias. Al no contar con el personal, se realiza la actividad de forma reactiva por lo que es un riesgo de seguridad.

- Análisis del tráfico de la red.
- Análisis de la actividad de los sistemas.
- Seguimiento diario a sistemas críticos.
- Implementación de medidas de seguridad en la red interna y la publicación en internet.
- Mantener los Sistemas Operativos y las Aplicaciones Actualizados en todos los equipos.
- Todos los equipos tengan un Antivirus actualizado.
- Contar un segmento de red exclusivo para los servidores y aplicaciones protegidos por un dispositivo de seguridad perimetral.

9.2. Se requiere de la contratación de personal enfocado a las actividades que no se realizan y la capacitación del personal

existente para contar con el nivel de seguridad deseado.

9.3. Actualmente en la Secretaría se cuentan con sistemas web que están obsoletos en relación al soporte al software y representan un grave problema de seguridad ya que desde el 2017 no se cuenta con soporte de seguridad y corrección de vulnerabilidades.

De igual forma, no todos los equipos de la Secretaría cuentan con antivirus actualizados para mitigar las filtraciones de datos en los equipos.

Algunos de los sistemas en riesgo son:

- SENTRE
- DECLARANET
- INHABILITADOS
- RELOJ CHECADOR ZKTECO.
- GESTIÓN DOCUMENTAL
- DIRECTORIO ÚNICO DE GOBIERNO

El seguimiento y verificación de los sistemas es por incidentes reportados por los usuarios, y al realizarse sólo por incidentes se pone un alto riesgo en pérdida de información que se integra en estos.

Los antivirus son la primera defensa de los equipos ya que bloquean los intentos de infiltraciones y pérdida de información de los equipos. Que no todos los equipos lo tengan es un riesgo latente que afecta a los usuarios y las aplicaciones que se usan en los equipos.

En este momento se tienen equipos servidores que funcionan en la red interna y conviven con los equipos de toda la Secretaría, esta práctica representa un alto nivel de inseguridad y un riesgo constante.

PARTE 5. MEDIDAS DE SEGURIDAD A IMPLEMENTAR.

Para la mitigación de los problemas de seguridad plasmados en la parte 4. Se pretende integrar restricciones a la información que se presenta a los usuarios, que cumpla los criterios de información pública y confidencial.

Para esto se van actualizar todos los sistemas de la Secretaría para hacer uso de las herramientas y las funcionalidades más actuales, aplicando los criterios de seguridad y desarrollo de aplicaciones, así como los criterios de manejo de información pública y confidencial.

Los sistemas a actualizar por la obsolescencia alcanzada son:

- SENTRE
- DECLARANET (histórico)
- INHABILITADOS
- RELOJ CHECADOR ZKTECO
- GESTIÓN DOCUMENTAL
- SISA

Objetivo de control	Descripción
Perímetro de seguridad	Implementar mecanismos de seguridad en el perímetro de las oficinas.
Control de entrada física	Implementar mecanismos que permitan sólo el acceso a personas autorizadas a la zona o área en la que se realiza el tratamiento de datos personales.
Seguridad en entorno de trabajo	Implementar mecanismos para mantener las áreas de resguardo y/o tratamiento a las personas autorizadas.
Seguridad del cableado	Verificación periódica de las conexiones de telecomunicaciones.
Mantenimiento del equipo de cómputo	Asegurar que los activos secundarios reciban periódicamente mantenimiento.
Aseguramiento de los activos fuera de las instalaciones.	Establecimiento de controles para la salida fuera de las instalaciones de cualquier activo que contenga datos personales y la seguridad física y electrónica que se deberá

	observar para el traslado del activo.
Borrado seguro de información	Cuando se elimine un activo deberá aplicarse mecanismos de borrado seguro o destrucción adecuada. La acción anterior deberá quedar asentada en acta circunstanciada.
Escrito limpio	Cualquier documento o activo de información debe estar resguardado, fuera de la vista, cuando éste no sea atendido.

Para el siguiente año se deberá contar con la totalidad de los equipos con antivirus instalado y actualizado para la protección de su información. Conjuntamente se les implementarán criterios de navegación y uso del internet.

Se van a realizar los ajustes necesarios a la infraestructura para tener todos los equipos servidores en la red protegida por un equipo de seguridad perimetral, para tener la información resguardada de la mejor forma posible.

Se va contratar personal para realizar los trabajos de verificación y seguimiento a los riesgos de seguridad en los equipos, sistemas y aplicaciones de la Secretaría. De igual forma se va a buscar proporcionar la capacitación requerida al personal del área en busca de mejorar los procesos de detección y mitigación de incidentes con la información de los usuarios ya sea en sistemas o en los equipos de uso diario.

El **nivel de riesgo** en los sistemas de tratamiento de datos personales puede disminuirse con mecanismos como:

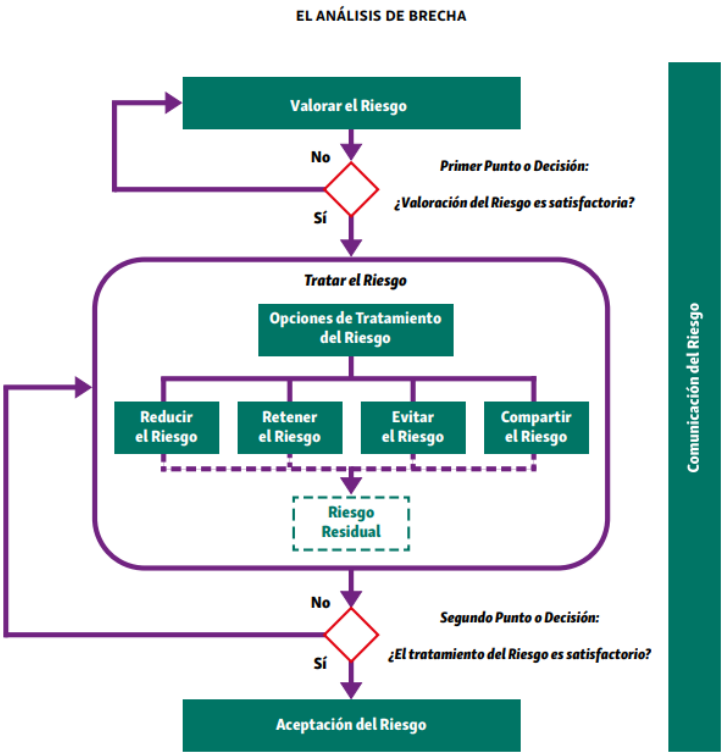
Disociación: Se aíslan los datos de modo que por sí no aporten información valiosa de un titular o éste no pueda ser identificable.

Así, el valor de la base de datos para una persona no autorizada se ve disminuido.

Separación: Se separan los activos de información grandes en otros más

pequeños. Por ejemplo, una base de datos de clientes en dos bases de datos: clientes corporativos y personas físicas.

Entre mayor cantidad de información tiene un activo, éste resulta más atractivo para una persona no autorizada.



Tipo	Amenaza	Origen
Fallas técnicas	Falla en el equipo	**Ambiental**
	Mal funcionamiento del equipo	**Ambiental**
	Saturación del sistema de información	**Deliberado, Ambiental**
	Mal funcionamiento del software	**Ambiental**
	Incumplimiento del mantenimiento del sistema de información	**Deliberado, Ambiental**
Acciones no auto-rizadas	Uso no autorizado de equipos	**Deliberado**
	Copia fraudulenta de software	**Deliberado**
	Uso de software falsificado o copiado	**Deliberado, Ambiental**
	Corrupción de datos	**Deliberado**
	Tratamiento ilegal de datos	**Deliberado**
Compromiso de funciones	Error en uso	**Ambiental**
	Abuso de derechos	**Deliberado, Ambiental**
	Forja de derechos	**Deliberado**
	Negación de acciones	**Deliberado**
	Incumplimiento de disponibilidad de personal.	**Accidental, Deliberado, Ambiental**

Activo	Amenaza	Impacto			
Currículum vitae		C	I	D	**Impacto inherente total**
	Incendio	1-Muy bajo	1-Muy bajo	2-Bajo	**1.3=1-Muy bajo**
	Robo de documentos	**3-medio**	**3-medio**	**2-bajo**	**2.6= 3-Medio**

impacto total = confidencialidad + integridad + disponibilidad

3

I. Análisis de riesgos

Información reservada

II. Análisis de brecha

Información reservada

PARTE 6. PROGRAMA GENERAL DE CAPACITACIÓN

1. **POR PARTE DE LA COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.**

   Para mejorar la seguridad con respecto a los usuarios finales de los sistemas, equipos de cómputo y herramientas con las que los servidores públicos realizan sus actividades cotidianas dentro de las cuales puede incluir tratamiento de datos personales; se realizarán las siguientes acciones:

a. Publicar en la Plataforma de Capacitación de la SECOES, recomendaciones para el correcto uso de las herramientas informáticas y sistemas para mejorar el nivel de seguridad a nivel de usuario.

I. Creación de contraseñas seguras.
II. Análisis de dispositivos de almacenamiento y computadoras para detección de virus y malware.
III. Uso de herramientas de libre uso para reducir la piratería y con eso disminuir el riesgo de infección de virus y accesos no autorizados.
IV. Uso racional de los recursos en red e Internet.

PARTE 7. PLAN DE TRABAJO

1. POR PARTE DE LA COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

1. Plan de Trabajo

Información reservada

1. Se creará un protocolo de seguridad física para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento que nos permita:
   a. Prevenir el acceso no autorizado en el perímetro en donde se resguarden los datos personales en sus instalaciones físicas.
   b. Prevenir el daño o interferencia a las instalaciones físicas, recursos e información.
   c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones De la secretaria.

2. Las acciones a monitorear son las siguientes:
   a. Posibles modificaciones necesarias en los activos, por ejemplo, cambio o migración tecnológica, entre otras.
   b. Patrones de comportamiento que nos permitan anticipar nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas.
   c. Cambios en vulnerabilidades identificadas para determinar aquellas amenazas que puedan ser recurrentes.
   d. Medir el impacto de amenazas valoradas, vulnerabilidades y riesgos en conjunto que resulten en un nivel inaceptable de riesgo.

2. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

1. Se mantendrá actualizado el inventario de los sistemas de tratamiento de datos personales y el detalle de los mismos en cada sistema.

2. Se mantendrá actualizado el inventario de los sistemas de tratamiento de datos personales y el detalle de los mismos en cada sistema.

PARTE 8. ANEXOS TÉCNICOS

1. **POR PARTE DE LA COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.**

No se adjuntan anexos técnicos.

APROBACIÓN DEL LA SECCIONES QUE CORRESPONDEN A TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DOCUMENTO DE SEGURIDAD

Responsable del desarrollo:

Nombre:

L. I. Edgar Leonel Xool Cab

Cargo:

Jefe de Depto. de Desarrollo de sistema e infraestructura tecnológica.

Tel: 983-8350800 Ext. 41638 E-mail: edgar.xool@qroo.gob.mx

Autorizó:

Nombre:

Lic. Adolfo Eduardo Vazquez Salazar

Cargo:

Coordinador de Tecnologías en Información.

Tel: 983-8350800 Ext. 41638 E-mail: eduardo.vazquez@qroo.gob.mx

APROBACIÓN DEL LA SECCIONES QUE CORRESPONDEN A LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE LA CONTRALORIA.

Titular Unidad de Transparencia y Protección de Datos Personales:

Nombre:

Mtro. Félix Díaz Villalobos

Cargo:

Coordinador General de Transparencia.
Tel: 983-1293258 E-mail: transparencia.secoes@gmail.com

Fecha: ABRIL DEL 2023.

Términos y definiciones

1) **Activo.** Todo elemento de valor para la SECOES, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

2) **Aviso de privacidad.** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

3) **Bases de datos.** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

4) **Borrado seguro.** Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

5) **Ciclo vital del documento.** Las tres fases por las que pasan los documentos de archivo, sea cual fuere su soporte, desde su recepción o generación hasta su conservación permanente o baja documental, a saber: archivo de trámite, archivo de concentración y archivo histórico.

6) **Confidencialidad.** Es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por el área universitaria respectiva.

7) **Control de seguridad en la red.** Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales.

8) **Disponibilidad.** Es el principio de seguridad de la información que consiste en ser accesible y utilizable a solicitud de personas o procesos autorizados por el área universitaria respectiva.

9) **Documento de seguridad.** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

10) **Encargado**. La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias que realizan el tratamiento de los datos personales a nombre de la SECOES, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

11) **Evaluación de impacto en la protección de datos personales (EIDP).** Documento mediante el cual las áreas universitarias que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales sobre determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

12) **Integridad.** Es el principio de seguridad de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que estos no puedan ser modificados sin autorización, sea de manera accidental o intencionada.

13) **Medidas de seguridad.** Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales.

14) **Medidas de seguridad administrativas.** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

15) **Medidas de seguridad físicas.** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

16) **Medidas de seguridad técnicas.** Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en formato digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
a. Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b. Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones;
c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

17) **Red de datos.** Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

18) **Responsable.** Las áreas universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

19) **Seguridad de la información.** La preservación de la confidencialidad, integridad y disponibilidad de la información, que puede abarcar además otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

20) **Servicios de nube privada**. Modelo de servicio de tecnología de información proporcionados bajo demanda a las áreas universitarias, en infraestructura propiedad de la SECOES y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

21) **Servicios de nube pública.** Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena a la SECOES.

22) **Sistema de Gestión de Seguridad de Datos Personales.** Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales.

23) **Sistemas para el tratamiento.** Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

24) **Soporte.** Medio, ya sea electrónico o físico, en el que se registra y guarda información, como el papel, así como los audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

25) **Soportes electrónicos.** Son los medios de almacenamiento accesibles solo mediante del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CD, DVD y Blue-ray), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

26) **Soportes físicos.** Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

27) **Transferencia.** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

28) **Tratamiento**. Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

29) **Vulneración de seguridad**. En cualquier fase del tratamiento de datos, se considera la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

INVENTARIO DE DATOS PARA EL AVISO DE PRIVACIDAD

Con fundamento en la Ley de Protección de Datos personales en posesión de sujetos obligados para el Estado de Quintana Roo ARTÍCULOS 24, 25 y 26, solicito el aviso de privacidad Integral y Simplificado, para el tiramiento de los datos personales con motivo de: _____ que se llevará a cabo a partir del día __/__/2024

En las instalaciones de: _____

Responsable _____ Área Administrativa: _____ Correo institucional: _____

Sujeto Obligado	**SECRETARIA DE LA CONTRALORIA**	
Artículo 27		
Fracción I	Denominación del responsable	
Fracción II	Finalidades del tratamiento	**Las finalidades son acciones específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser «contratación de personal»; y las finalidades, «evaluación de currículum para la selección de personal**
Unidad Administrativa	**Descripción de las Funciones del Personal que da Tratamiento a DP**	
	Descripción general de la ubicación física y/o electrónica de los datos personales	
Fracción III	Transferencia o remisión de datos	☐ Transferencia ☐ Remisión
	Fundamentos para la transferencia o remisión de datos	**Incluir el fundamento que le faculta**
A)	A quién se transfieren o remiten	**Describir brevemente**
B)	Finalidad de la transferencia o remisión	**Describir brevemente**
Artículo 28		

Fracción I	Domicilio	
Fracción II Datos personales requeridos:		**Nombre, Teléfono y firma etc**
Señalar si habrá toma de fotografía y video, así como los medios en los que se publicarán:		**Describir**
En caso de haber menores de edad, deberá de contar con la autorización escrita de los padres o tutores para publicar la imágenes o fotografías		**Describir**
La lista de servidores públicos que tienen acceso a los sistemas de tratamiento:		**Nombre y cargo …**
Mencione las medidas de seguridad existentes que utiliza para resguardar y proteger los datos que tratará:		**Archivero con llave …** **Contraseña restringía a etc…**

Atentamente: _____ **Firma:** _____**fecha**: 09/02/2024

Unidad Administrativa: _____

_____

En el supuesto de recabar datos personales sensibles, es necesario recabar el consentimiento expreso de la persona titular de los datos que se tratarán:

CONSENTIMIENTO EXPRESO
Ciudad de _____, Quintana Roo a _____ de ___ Por medio del presente y con fundamento en los artículos 9 y 17 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo y previo a haber leído y comprendido el aviso de privacidad, manifiesto expresamente mi consentimiento para que La Secretaría de la Contraloría del Estado "SECOES", _____(incorporar la finalidad) _____. _____ _____

FECHA ___/___/_____