



UNIVERSIDAD DE TALCA  
FACULTAD DE INGENIERÍA  
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

# **Seguridad Informática**

## Proyecto 1

Erik Regla  
eregl09@alumnos.otalca.cl

18 de junio de 2020

## 1. Introducción

## 2. Estructura organizacional

### 2.1. Organigrama

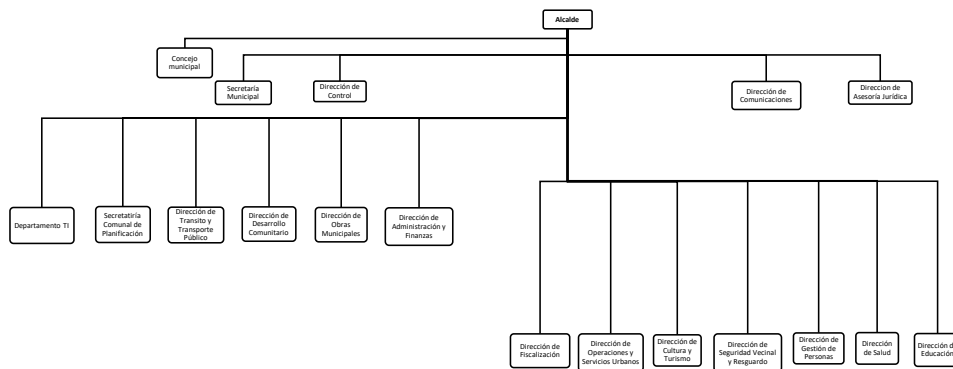


Figura 1: Organigrama

### 2.2. Rationale

El alcance de este trabajo abarca solo las siguientes divisiones:

- **Departamento de asuntos municipales.** Perteneciente a la secretaría municipal. Este se compone de las siguientes oficinas:
  - Oficina de partes alcaldía

- Sección resolutive
- Sección administrativa
- **Departamento de certificación y archivo.** Perteneciente a la secretaría municipal. Este se compone de las siguientes oficinas:
  - Oficina de registro municipal de transferencias
  - Oficina de control de archivo y representación.
- **Departamento de cartografía.**
- **Departamento de revisión de procesos de contratación pública**
- **Departamento de auditoría operativa**
- **Departamento Revisión de procesos de pago, bienes y servicios**

Se establece para cada departamento la siguiente estructura base:

- Un(a) Jefe(a) de departamento.
- Un(a) Secretario(a) general de departamento.
- Uno o más ejecutivos de departamento.
- Un encargado de TI del departamento.

Se establece para cada oficina la siguiente estructura base:

- Un(a) Jefe(a) de oficina.
- Un(a) Secretario(a) general.
- Uno o más ejecutivos de oficina.

Se establece para cada secretaría la siguiente estructura base:

- Un(a) Secretario(a) general.
- Uno o más ejecutivos de oficina.

### **3. Identificación de activos**

#### **3.1. Contexto<sup>1</sup>**

#### **3.2. Situación actual**

Durante noviembre del mes pasado, gracias a un informe de contraloría se han detectado las siguientes falencias en relación a los servicios contratados a empresas externas, ya que no se consideran cláusulas respecto a las siguientes operaciones:

- Controles para asegurar la protección contra software malicioso
- Procedimientos para determinar si ha ocurrido algún compromiso en los datos municipales
- Plan de contingencia para accesos indebidos, siniestros físicos y lógicos
- Restricciones de copiado y divulgación de la información municipal
- Devolución o destrucción de la información y bienes, amparado por las regulaciones locales y término de la relación contractual.
- Posibilidad de auditar módulos del sistema administrativo municipal y los datos

Respecto a estos problemas, el alcalde ha mencionado que durante este año se deben de solucionar - parte del objetivo de este trabajo-

#### **3.3. Procesos**

Debido a que por ordenanzas del estado es necesario justificar el uso de recursos, la municipalidad hace uso de externalizaciones para la mayoría de sus recursos de software, siendo solo desarrollados o mantenidos de manera in-house las plataformas legadas o las que requieren atención crítica. Si bien el objetivo de la municipalidad es externalizar el desarrollo, gracias a los lineamientos descritos el año 2018<sup>2</sup>, los sistemas son alojados de manera interna y administrados internamente. Sin embargo, aún hay un par de sistemas legados, los cuales serán listados a continuación:

##### **3.3.1. Sistema contabilidad gubernamental**

Este sistema fue desarrollado por la Empresa Externa 1 durante el año 2010, por lo cual no está ligado directamente a la normativa de apertura de código digital. Las fuentes de esta plataforma

---

<sup>1</sup>Durante la identificación de activos esta se ha limitado a activos que puedan presentar riesgos de seguridad de la información, ignorando los activos humanos y los activos de servicios de TI ya que escapan a situaciones bajo el control directo y supervisión de el equipo de TI. Adicionalmente está especificado en la especificación del proyecto que dichos factores no deben de ser incluidos.

<sup>2</sup>[https://digital.gob.cl/doc/Guia\\_de\\_desarrollo\\_de\\_software\\_para\\_el\\_Estado.pdf](https://digital.gob.cl/doc/Guia_de_desarrollo_de_software_para_el_Estado.pdf)

están cerradas y la base de datos solo permite acceso al motor y su contenido pero no a la instancia de máquina virtual donde se aloja.

Funciones de este sistema:

- Sistema contabilidad gubernamental.
- Ingreso de cuentas contables, programas y centro de costos.
- Ingreso de tablas para el funcionamiento del sistema (meses, áreas, tipo de comprobantes contables, tipo de documentos, tabla centro costos, programas, parámetros y proveedores).
- Ingreso de presupuesto inicial y modificaciones presupuestarias.
- Ingreso de obligaciones (contratos, orden de compra, adjudicaciones y factibilidades).
- Ingreso de devengados por proveedor (facturas).
- Confección de órdenes de pago.
- Ingreso y contabilización de documentos contables, rendiciones de cuentas.

### **3.3.2. Sistema de tesorería municipal**

Este es el sistema legado de mayor longevidad presente externalizado por la Empresa Externa 2, el cual data del año 1999. Sin embargo, debido a que el contrato con la empresa externa incluye actualizaciones continuas de la plataforma, esta se ha podido mantener vigente hasta el día de hoy sin mayores cambios visibles. De acuerdo a un informe de auditoría de contraloría realizado el año pasado, esta plataforma presenta problemas de interoperabilidad con los sistemas existentes, por lo cual un nuevo contrato es esperado de firmarse este año para iniciar un nuevo desarrollo de esta.

Funciones de este sistema:

- Boletas de garantía.
  - Mantención de garantías.
  - Consulta documento en garantía.
  - Ingreso de contratos
- Egresos.
  - Emisión de cheques de distintas cuentas corrientes.
  - Emisión de listados de información, como cuenta corriente de proveedor.
  - Generación de listado de conciliaciones bancarias y retenciones de impuesto.
  - Contabilización de movimientos contables
- Ingresos.

- Apertura y cierre de cajas.
- Anulación de ingresos.
- Cuadraturas de cajas.
- Contabilización de ingresos.
- Conciliación de ingresos.
- Pagos a través de Internet.
- Emisión informes varios.
- Consulta de recaudación por cajas.

### **3.4. Sistema patentes comerciales**

Este sistema acaba de ser contratado a la Empresa Externa 3 hace no mas de dos meses y su aprobación de uso fue entregada hace tres días atrás. Para mantener el uso con el archivo antiguo de la municipalidad, todos los registros físicos fueron migrados a sus versiones digitales para poder ser utilizados desde la nueva plataforma.

Funciones de este sistema:

- Consulta de patentes.
- Listar patentes CIPA, según tipo.
- Administrar solicitud de patente.
- Mantención del maestro de patentes.
- Cálculo de patentes.
- Anulación de patentes y/o giros.

### **3.5. Sistema permisos de circulación**

Este es el segundo sistema externalizado a la Empresa Externa 1 y está en la misma situación que el sistema anteriormente mencionado para las patentes comerciales.

Funciones de este sistema:

- Generación de giro para pago de permisos de circulación.
- Generación de duplicado de permisos de circulación.
- Emisión de giros de fondos a terceros
- Bloqueo por sistema de placas patentes.
- Consultas de pagos años anteriores, de registro de multas, de incorporaciones y de traslados.

- Generación de giros de sellos.
- Mantención de traslado.
- Asignación de código de S.I.I.
- Anulación de giros mal emitidos

### 3.6. Activos de carácter transversal

A continuación se listan los activos de carácter transversal, quiere decir, cuyo uso se extiende por más de una sola oficina.

<b>Nombre</b>	RTR_PRINC_001
<b>Descripción</b>	Router principal Cisco 2901, gateway externo perteneciente a la municipalidad
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2013-1241 <sup>3</sup> Autenticación inválida en cabeceras del módulo ISM. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

---

<sup>3</sup><https://www.cvedetails.com/cve/CVE-2013-1241/>

<b>Nombre</b>	RTR_SECUN_001
<b>Descripción</b>	Router secundario Cisco 2901, utilizado de punto intermedio hacia la red interna
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>4</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	SWLNODES_001
<b>Descripción</b>	Switch general Cisco Catalyst 2960, para nodo base del arbol de conectividad
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>5</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>4</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<sup>5</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>



<b>Nombre</b>	SRV_SHARE_001
<b>Descripción</b>	Dell PowerEdge R520 750W E5 2440
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	OSS_WINDO_001
<b>Descripción</b>	Windows Server 2019 Datacenter Edition
<b>Categoría</b>	Sistemas Operativos
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 2 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Mas de 390 vulnerabilidades detectadas <sup>6</sup> Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. La disponibilidad del recurso depende de sus licencias. Este recurso no posee antivirus.

<sup>6</sup>[https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor\\_id=26](https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor_id=26)

<b>Nombre</b>	EXE_EXCHA_001
<b>Descripción</b>	Módulo servidor para Microsoft Exchange 2016, para uso de correos corporativos de los funcionarios de la municipalidad.
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	<p>CVE-2018-8374<sup>7</sup> Tampering Vulnerability existente al momento de un fallo en la información de los perfiles.</p> <p>CVE-2018-8302<sup>8</sup> Ejecución de código remota debido al fallo de manipulación de objetos en memoria, resultante en control total.</p> <p>CVE-2018-8159<sup>9</sup> XSS resultante en elevación de privilegios por medio de requests web .</p> <p>CVE-2018-8154<sup>10</sup> Ejecución de código remota debido a la corrupción del manejo de objetos en memoria, resultante en control total.</p> <p>CVE-2018-8153<sup>11</sup> Spoofing .</p> <p>CVE-2018-8152<sup>12</sup> Elevación de privilegios .</p> <p>CVE-2018-8151<sup>13</sup> Corrupción de memoria .</p> <p>Pérdida de integridad física o lógica por intervención física.</p> <p>Pérdida de integridad física o lógica por intervención remota.</p> <p>Posee información de alto interés para un grupo específico.</p>

<b>Nombre</b>	ARC_LOCAL_001
<b>Descripción</b>	Archivo general de la municipalidad - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Archivo - Primer piso
<b>Propietario</b>	Departamento de Certificación y Archivos
<b>Valoración</b>	Confidencialidad: 5 Integridad: 4 Disponibilidad: 2
<b>Vulnerabilidades y Amenazas</b>	<p>No existen respaldos físicos.</p> <p>No existen respaldos digitales.</p> <p>Pérdida de integridad física o lógica por intervención física.</p> <p>Este recurso no cuenta con registro transaccional.</p>

<sup>7</sup><https://www.cvedetails.com/cve/CVE-2018-8374/>

<sup>8</sup><https://www.cvedetails.com/cve/CVE-2018-8302/>

<sup>9</sup><https://www.cvedetails.com/cve/CVE-2018-8159/>

<sup>10</sup><https://www.cvedetails.com/cve/CVE-2018-8154/>

<sup>11</sup><https://www.cvedetails.com/cve/CVE-2018-8153/>

<sup>12</sup><https://www.cvedetails.com/cve/CVE-2018-8152/>

<sup>13</sup><https://www.cvedetails.com/cve/CVE-2018-8151/>

<b>Nombre</b>	EXE_WPRES_001
<b>Descripción</b>	Servidor Wordpress 5.1 Beta3 para página institucional
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2019-9787 <sup>14</sup> Ejecución remota de código por medio de CRSRF. CVE-2019-16220 <sup>15</sup> Sanitización de wp_validate manipula redirects. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	EXE_MYSQL_001
<b>Descripción</b>	Servidor MySQL 6.0.9 Beta3 para EXE_WPRES_001
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2009-0819 <sup>16</sup> Denegación de servicio. CVE-2008-7247 <sup>17</sup> Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	EXE_SQLTB_001
<b>Descripción</b>	Base de datos MySQL en EXE_MYSQL_001para EXE_WPRES_001
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Está sujeta a vulnerabilidades de manera transitiva. Posee información de alto interés para un grupo específico.

<sup>14</sup><https://www.cvedetails.com/cve/CVE-2019-9787/>

<sup>15</sup><https://www.cvedetails.com/cve/CVE-2019-16220/>

<sup>16</sup><https://www.cvedetails.com/cve/CVE-2009-0819/>

<sup>17</sup><https://www.cvedetails.com/cve/CVE-2008-7247/>

<b>Nombre</b>	EXE_PHPSR_001
<b>Descripción</b>	Servidor PHP 7.3.6 para EXE_WPRES_001
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2019-11042 <sup>18</sup> Buffer overflow causado por información EXIF. CVE-2008-7247 <sup>19</sup> Buffer overflow causado por información EXIF. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	EXE_ADMIN_002
<b>Descripción</b>	Servidor con aplicativo de administración propia para municipio
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_002
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	No se tiene conocimiento de las vulnerabilidades. Está sujeta a vulnerabilidades de manera transitiva. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	EXE_MYSQL_002
<b>Descripción</b>	Servidor MySQL 6.0.9 Beta3 para EXE_ADMIN_002
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_002
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	CVE-2009-0819 <sup>20</sup> Denegación de servicio. CVE-2008-7247 <sup>21</sup> Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<sup>18</sup><https://www.cvedetails.com/cve/CVE-2019-11042/>

<sup>19</sup><https://www.cvedetails.com/cve/CVE-2008-7247/>

<sup>20</sup><https://www.cvedetails.com/cve/CVE-2009-0819/>

<sup>21</sup><https://www.cvedetails.com/cve/CVE-2008-7247/>

<b>Nombre</b>	EXE_SQLTB_002
<b>Descripción</b>	Base de datos MySQL en EXE_MYSQL_002 para EXE_ADMIN_002
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_002
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Está sujeta a vulnerabilidades de manera transitiva. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	EXE_PHPSR_002
<b>Descripción</b>	Servidor PHP 7.3.6 para EXE_ADMIN_002
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_002
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	CVE-2019-11042 <sup>22</sup> Buffer overflow causado por información EXIF. CVE-2008-7247 <sup>23</sup> Buffer overflow causado por información EXIF. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	EXE_ADMIN_003
<b>Descripción</b>	Servidor con aplicativo de administración para archivo de municipio
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_003
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	No se tiene conocimiento de las vulnerabilidades. Está sujeta a vulnerabilidades de manera transitiva. Posee información de alto interés para un grupo específico.

<sup>22</sup><https://www.cvedetails.com/cve/CVE-2019-11042/>

<sup>23</sup><https://www.cvedetails.com/cve/CVE-2008-7247/>

<b>Nombre</b>	EXE_MYSQL_003
<b>Descripción</b>	Servidor MySQL 6.0.9 Beta3 para EXE_ADMIN_003
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_003
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	CVE-2009-0819 <sup>24</sup> Denegación de servicio. CVE-2008-7247 <sup>25</sup> Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	EXE_SQLTB_003
<b>Descripción</b>	Base de datos MySQL en EXE_MYSQL_003para EXE_ADMIN_003
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_003
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Está sujeta a vulnerabilidades de manera transitiva. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	EXE_PHPSR_003
<b>Descripción</b>	Servidor PHP 7.3.6 para EXE_ADMIN_003
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_003
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	CVE-2019-11042 <sup>26</sup> Buffer overflow causado por información EXIF. CVE-2008-7247 <sup>27</sup> Buffer overflow causado por información EXIF. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<sup>24</sup><https://www.cvedetails.com/cve/CVE-2009-0819/>

<sup>25</sup><https://www.cvedetails.com/cve/CVE-2008-7247/>

<sup>26</sup><https://www.cvedetails.com/cve/CVE-2019-11042/>

<sup>27</sup><https://www.cvedetails.com/cve/CVE-2008-7247/>

### 3.7. Activos externalizados

<b>Nombre</b>	EXT_PLATF_001
<b>Descripción</b>	Sistema de tesorería municipal
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 1
<b>Valoración</b>	Confidencialidad: 3 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Este componente pudo pasar pruebas de pentesting satisfactoriamente. No existe interoperación con estandar de norma técnica para los Organos de la administración del estado. La información no está encriptada. Este recurso está externalizado. Este recurso tiene mantenimiento preventivo externalizado. Este recurso no cuenta con registro transaccional.

<b>Nombre</b>	EXT_PLATF_002
<b>Descripción</b>	Sistema de patentes comerciales
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 2
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos fisicos. No existe interoperación con estandar de norma técnica para los Organos de la administración del estado. La información no está encriptada. Este recurso está externalizado. Este recurso tiene mantenimiento preventivo externalizado.

<b>Nombre</b>	EXT_PLATF_003
<b>Descripción</b>	Sistema de Permisos de Circulación
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 3
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 2
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos digitales. No existe interoperación con estandar de norma técnica para los Organos de la administración del estado. La información no está encriptada. Este recurso está externalizado. Este recurso no cuenta con protocolos de recuperación de desastres.

<b>Nombre</b>	EXT_PLATF_004
<b>Descripción</b>	Sistema de contabilidad gubernamental
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 1
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Posee un gran valor por reducción de especies. Posee información de alto interés para un grupo específico. Este componente pudo pasar pruebas de pentesting satisfactoriamente. No existe interoperación con estandar de norma técnica para los Organos de la administración del estado. La información no está encriptada. Este recurso está externalizado. Este recurso tiene mantenimiento preventivo externalizado. Este recurso no cuenta con registro transaccional.

### 3.8. Activos de carácter específico

A continuación se listan los activos de carácter específico, quiere decir, cuyo uso es solo de un oficina, departamento o sección en particular.



### 3.8.1. Oficina de Partes Alcaldía

<b>Nombre</b>	NTB_OF001_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_OF001_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Secretario de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_OF001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_OF001_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_OF001_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_OF001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_OF001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Partes Alcaldía
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>28</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_OF001_001
<b>Descripción</b>	Armario de archivos para Oficina de Partes Alcaldía
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>28</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLOF001_001
<b>Descripción</b>	Oficina de Partes Alcaldía - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_OF001_001
<b>Descripción</b>	Alarma de Oficina de Partes Alcaldía
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_OF001_001
<b>Descripción</b>	Archivo de Oficina de Partes Alcaldía - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso
<b>Propietario</b>	Jefe de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.2. Oficina de Registro Municipal de Transferencias

<b>Nombre</b>	NTB_OF002.001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_OF002.002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Secretario de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_OF002_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_OF002_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_OF002_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_OF002_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_OF002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Registro Municipal de Transferencias
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>29</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_OF002_001
<b>Descripción</b>	Armario de archivos para Oficina de Registro Municipal de Transferencias
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>29</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLOF002_001
<b>Descripción</b>	Oficina de Registro Municipal de Transferencias - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_OF002_001
<b>Descripción</b>	Alarma de Oficina de Registro Municipal de Transferencias
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_OF002_001
<b>Descripción</b>	Archivo de Oficina de Registro Municipal de Transferencias - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso
<b>Propietario</b>	Jefe de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.



### 3.8.3. Oficina de Control de Archivo y reorientación

<b>Nombre</b>	NTB_OF003_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_OF003_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Secretario de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_OF003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_OF003_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_OF003_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_OF003_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_OF003_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Control de Archivo y reorientación
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de certificación y archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>30</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_OF003_001
<b>Descripción</b>	Armario de archivos para Oficina de Control de Archivo y reorientación
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>30</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLOF003_001
<b>Descripción</b>	Oficina de Control de Archivo y reorientación - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_OF003_001
<b>Descripción</b>	Alarma de Oficina de Control de Archivo y reorientación
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_OF003_001
<b>Descripción</b>	Archivo de Oficina de Control de Archivo y reorientación - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso
<b>Propietario</b>	Jefe de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.4. Sección Resolutiva

<b>Nombre</b>	NTB_SE001_101
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Dirección de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_SE001_101
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Secretario de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_SE001_201
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_SE001_101
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Dirección de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_SE001_101
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_SE001_201
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_SE001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Sección Resolutiva
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>31</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_SE001_001
<b>Descripción</b>	Armario de archivos para Sección Resolutiva
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Jefe de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>31</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLSE001_001
<b>Descripción</b>	Sección Resolutiva - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_SE001_001
<b>Descripción</b>	Alarma de Sección Resolutiva
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_SE001_001
<b>Descripción</b>	Archivo de Sección Resolutiva - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Sección Resolutiva - primer piso
<b>Propietario</b>	Jefe de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.



### 3.8.5. Sección Administrativa

<b>Nombre</b>	NTB_SE002_101
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Dirección de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_SE002_101
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Secretario de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_SE002_201
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_SE002_101
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Dirección de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_SE002_101
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_SE002_201
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_SE002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Sección Administrativa
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>32</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_SE002_001
<b>Descripción</b>	Armario de archivos para Sección Administrativa
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Jefe de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>32</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLSE002_001
<b>Descripción</b>	Sección Administrativa - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_SE002_001
<b>Descripción</b>	Alarma de Sección Administrativa
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_SE002_001
<b>Descripción</b>	Archivo de Sección Administrativa - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Sección Administrativa - primer piso
<b>Propietario</b>	Jefe de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.6. Departamento de Asuntos Municipales

<b>Nombre</b>	SWLDP001_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>33</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP001_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>33</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_DP001_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_DP001_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP001_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_DP001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Asuntos Municipales
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>34</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_DP001_001
<b>Descripción</b>	Armario de archivos para Departamento de Asuntos Municipales
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>34</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>



<b>Nombre</b>	OFLDP001_001
<b>Descripción</b>	Departamento de Asuntos Municipales - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_DP001_001
<b>Descripción</b>	Alarma de Departamento de Asuntos Municipales
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_DP001_001
<b>Descripción</b>	Archivo de Departamento de Asuntos Municipales - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso
<b>Propietario</b>	Jefe de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.7. Departamento de Certificación y archivo

<b>Nombre</b>	SWLDP002_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>35</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP002_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>35</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_DP002_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP002_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP002_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_DP002_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP002_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP002_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP002_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_DP002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Certificación y Archivo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>36</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_DP002_001
<b>Descripción</b>	Armario de archivos para Departamento de Certificación y Archivo
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>36</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLDP002_001
<b>Descripción</b>	Departamento de Certificación y Archivo - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_DP002_001
<b>Descripción</b>	Alarma de Departamento de Certificación y Archivo
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_DP002_001
<b>Descripción</b>	Archivo de Departamento de Certificación y Archivo - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso
<b>Propietario</b>	Jefe de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.8. Departamento de Cartografía

<b>Nombre</b>	SWLDP003_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>37</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP003_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>37</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_DP003_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.



<b>Nombre</b>	EML_DP003_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP003_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP003_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP003_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_DP003_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Cartografía
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>38</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_DP003_001
<b>Descripción</b>	Armario de archivos para Departamento de Cartografía
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>38</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLDP003_001
<b>Descripción</b>	Departamento de Cartografía - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_DP003_001
<b>Descripción</b>	Alarma de Departamento de Cartografía
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_DP003_001
<b>Descripción</b>	Archivo de Departamento de Cartografía - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Cartografía - tercer piso
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.9. Departamento de Revisión de Procesos de Contratación

<b>Nombre</b>	SWLDP004_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>39</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP004_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>39</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_DP004_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP004_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP004_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_DP004_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP004_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP004_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP004_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_DP004_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Revisión de Procesos de Contratación Pública
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>40</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_DP004_001
<b>Descripción</b>	Armario de archivos para Departamento de Revisión de Procesos de Contratación Pública
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>40</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>



<b>Nombre</b>	OFLDP004_001
<b>Descripción</b>	Departamento de Revisión de Procesos de Contratación Pública - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_DP004_001
<b>Descripción</b>	Alarma de Departamento de Revisión de Procesos de Contratación Pública
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_DP004_001
<b>Descripción</b>	Archivo de Departamento de Revisión de Procesos de Contratación Pública - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso
<b>Propietario</b>	Jefe de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.10. Departamento de Auditoría Operativa

<b>Nombre</b>	SWLDP005_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>41</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP005_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>41</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_DP005_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP005_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_DP005_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	EML_DP005_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP005_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP005_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_DP005_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_DP005_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Auditoría Operativa
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>42</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_DP005_001
<b>Descripción</b>	Armario de archivos para Departamento de Auditoría Operativa
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>42</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLDP005_001
<b>Descripción</b>	Departamento de Auditoría Operativa - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_DP005_001
<b>Descripción</b>	Alarma de Departamento de Auditoría Operativa
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_DP005_001
<b>Descripción</b>	Archivo de Departamento de Auditoría Operativa - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso
<b>Propietario</b>	Jefe de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

### 3.8.11. Dirección de revisión de Procesos de Pago, Bienes y Servicios

<b>Nombre</b>	SWL_PP001_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>43</sup> Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_PP001_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<sup>43</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP001_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_PP001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	NTB_PP001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.



<b>Nombre</b>	EML_PP001_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_PP001_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_PP001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	EML_PP001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

<b>Nombre</b>	NAS_PP001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Desarrollo Comunitario
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>44</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<b>Nombre</b>	CAB_PP001_001
<b>Descripción</b>	Armario de archivos para Dirección de Desarrollo Comunitario
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

<sup>44</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	OFLPP001_001
<b>Descripción</b>	Dirección de Desarrollo Comunitario - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

<b>Nombre</b>	RNG_PP001_001
<b>Descripción</b>	Alarma de Dirección de Desarrollo Comunitario
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<b>Nombre</b>	ARC_PP001_001
<b>Descripción</b>	Archivo de Dirección de Desarrollo Comunitario - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

## 4. Análisis de riesgos

1 Empresa Externa 1 2 Empresa Externa 2 3 Empresa Externa 3

Remuneraciones Registro comunal de permisos de circulación Licencias de conducir Patentes municipales Control de bienes Adquisición y control de bodegas Banco de datos propiedades comunales Oficina de partes Departamento Tecnologías Juzgados de policía local mantención y administración de cartografía digital

Administracion red departamente licencias de conducir administracion red departamento de juzgados de policia local partes empadronados departamento de seguridad ciudadana administraci3n red departamente patentes municipales y tesorería administraci3n red del departamento de seguridad ciudadana administraci3n de direcci3n de obras municipales plataforma de egresos administracion de sistemas de desarrollo comunitario sistemas computaciones por internet y sistemas sociales

administraci3n de sistemas de egresos, recursos humanos y remuneraciones \*\* Contabilidad gubernamental \*\*

5. Riesgos asociados a factores no tecnológicos
6. Riesgos asociados a procesos municipales
7. Riesgos asociados procesos de atención municipal
8. Riesgos asociados a control del personal
9. Riesgos asociados de índole técnica

<b>Título de Riesgo</b>	Dependencia de licencias
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, la invalidación de una licencia podría provocar problemas de seguridad o bien interrupciones en la disponibilidad de un servicio.
<b>Dueño del Activo</b>	Dominio General
<b>Proceso</b>	Disponibilidad del servicio.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	Para el caso de software que opera con licencias (Office 365 por ejemplo), la caducidad de las mismas puede generar interrupciones o bien dejar de dar soporte a nuevas amenazas
<b>Detalle de la amenaza</b>	Actualmente debido al convenio con Microsoft vigente por parte del gobierno actual, muchos softwares están a merced de que estas licencias no caduquen. Esto podría producirse por múltiples factores, no disponibilidad del retailer, cambio de versiones, no soporte de cambios, olvido de pagos, etc.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información. , Jefe de Departamento revisión de procesos de pago, bienes y servicios , Jefe de Departamento de revisión de procesos de contratación pública

<b>Título de Riesgo</b>	Transaccion rota
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, es posible leer la información directamente desde el medio en que se encuentra sin ninguna barrera de seguridad
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Integridad de datos.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	Actualmente no hay ningún mecanismo de respaldo para operaciones de índole transaccional, lo cual puede provocar pérdidas de información.
<b>Detalle de la amenaza</b>	Al no haber un registro de comunicaciones llevadas a cabo de manera transaccional, en el momento de existir peticiones a los distintos servicios que puedan provocar un conflicto, este puede resultar en inconsistencias, corrupción y pérdida de datos. Sin embargo, Dado que los riesgos son mínimos de por el momento y no ha ocurrido no se le da mayor importancia, a excepción del sistema de pago.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Falta de encriptado
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, es posible leer la información directamente desde el medio en que se encuentra sin ninguna barrera de seguridad
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Resguardo de información personal. Resguardo de información institucional.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	Una auditoria realizada por contraloría reveló que no existe encriptación de los datos almacenados digitalmente salvo en la capa de transporte.
<b>Detalle de la amenaza</b>	La falta de encriptación puede producir fuga de información sensible.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Residuos de información
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, información que haya sido borrada sigue disponible dentro de una base de datos sin ser detectada
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Resguardo de información personal. Resguardo de información institucional.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	Una auditoria realizada por contraloría reveló que no existen protocolos de eliminación de la información de manera interna y esta tampoco forma parte de los servicios contratados.
<b>Detalle de la amenaza</b>	Al no existir un protocolo de eliminado de información claro, es altamente probable que la información no pueda ser eliminada de manera efectiva ya sea de plataformas, dispositivos, medios extraíbles, etc. Este problema aplica también a los archivos físicos que no cuenten con respaldo y que dentro de las operaciones vigentes consideren su eliminación.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Residuos de información
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, información que haya sido borrada sigue disponible dentro de una base de datos sin ser detectada
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Resguardo de información personal. Resguardo de información institucional.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	Una auditoria realizada por contraloría reveló que no existen protocolos de eliminación de la información de manera interna y esta tampoco forma parte de los servicios contratados.
<b>Detalle de la amenaza</b>	Al no existir un protocolo de eliminado de información claro, es altamente probable que la información no pueda ser eliminada de manera efectiva ya sea de plataformas, dispositivos, medios extraíbles, etc. Este problema aplica también a los archivos físicos que no cuenten con respaldo y que dentro de las operaciones vigentes consideren su eliminación.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Alcalde



<b>Título de Riesgo</b>	Mantenimiento preventivo externalizado ejecutado deficientemente
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, las plataformas sujetas a manteniendo por parte de una empresa externa podrían quedar expuestas a vulnerabilidades
<b>Dueño del Activo</b>	Empresas externas
<b>Proceso</b>	Resguardo de información personal. Resguardo de información institucional. Fiabilidad de plataforma
<b>Sub Área</b>	Departamento de Asuntos Municipales. Departamento revisión de procesos de pago, bienes y servicios Departamento de auditoria operativa
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	Mantenciones negligentes, omitidas, incompletas.
<b>Detalle de la amenaza</b>	Una mantención negligente de las plataformas puede llevar a un uso malicioso de estas, las cuales pueden perjudicar enormemente el servicio entregado por la municipalidad como también poner en riesgo los datos disponibles en esta. Actualmente debido a la normativa actual, todas las aplicaciones están alojadas en servidores de la municipalidad, sin embargo, no implica que el código esté necesariamente abierto o que el personal propio del departamento de tecnologías pueda tener el conocimiento suficiente sobre este para tomar control completo.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Denegación de servicio
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	11/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sitio web de la municipalidad deja de quedar disponible para todo público.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Nivel general, Disponibilidad del servicio.
<b>Sub Área</b>	Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
<b>Detalle de la Vulnerabilidad</b>	La denegación de servicio es un tipo de ataque cuyo fin es eliminar temporal o parcialmente la disponibilidad de un servicio, usualmente por medios como ICMP Flood.
<b>Detalle de la amenaza</b>	Si bien la aplicación está funcionando con las últimas versiones de PHP y de MYSQL disponibles, la infraestructura al ser local y no contar con un WAF, no hay filtro respecto a las peticiones que son resueltas en el servidor. Debido a esto, en caso de llegar un número importante de peticiones las cuales no pudiesen resolverse simultáneamente, podría ocurrir un problema de overflow de memoria colapsando el proceso. Cabe destacar que esto también puede ocurrir de manera orgánica en situaciones de alta demanda. Y debido a los acuerdos internos de desarrollo estandarizado, está presente en todas las plataformas desarrolladas para uso interno.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Ejecución remota de código
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	11/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el atacante ejecuta código en el navegador del cliente sin previo consentimiento.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Nivel general, Disponibilidad del servicio.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	La ejecución remota de código permite que un usuario no autorizado ejecute instrucciones en otro equipo.
<b>Detalle de la amenaza</b>	Esta amenaza está atribuida a CVE-2019-9787, el cual especifica una vulnerabilidad sobre la ejecución remota de código por medio de CRSRF. Este tipo de ataque fuerza al usuario a ejecutar código utilizando sus credenciales ya cargadas en la aplicación.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Manipulación de redirecciones
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	11/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el atacante fuerza la redirección a un sitio externo.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Nivel general, Disponibilidad del servicio. Nivel general, Confiabilidad del servicio.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	La ejecución remota de código permite que un usuario no autorizado ejecute instrucciones en otro equipo.
<b>Detalle de la amenaza</b>	Esta amenaza está atribuida a CVE-2019-16220, el cual especifica una vulnerabilidad sobre la ejecución remota de código por medio de CRSRF. Este tipo de ataque fuerza al usuario a ejecutar código utilizando sus credenciales ya cargadas en la aplicación.
<b>Respuesta</b>	MITIGAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Ejecución de malware por falta de software AV
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	11/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el servidor principal de la municipalidad queda comprometido.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Ataques por randomware, gusanos, trojanos, etc.
<b>Detalle de la amenaza</b>	Debido al alto número de vulnerabilidades presentes en el sistema operativo, es posible que la materialización de un riesgo en un equipo de una red adyacente pueda propagar procesos de terceros y estos comprometan el servidor principal.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

## 10. Riesgos generales asociados a ingeniería social

<b>Título de Riesgo</b>	Phishing
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	11/06/2020
<b>Descripción</b>	Al materializarse este riesgo, un usuario ingresa información institucional a un sitio falso.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Un usuario recibe un correo con un mensaje falso pero con apariencia visual creíble, de esta manera para tentar al usuario a ejecutar alguna acción que pueda comprometer la seguridad, ya sea filtrando credenciales o información sensible.
<b>Detalle de la amenaza</b>	Un ataque de Phishing implica la personificación de otro individuo o entidad, la cual actúa como emisor de un mensaje el cual puede ser de interés del usuario. En este caso la apuesta es que el lector del correo hará caso del call to action antes de verificar la veracidad del contenido, por lo que este tipo de ataques está dirigido a un público no técnico.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

## 11. Matriz de riesgos

## 12. Política de seguridad

## Referencias