



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

# **Seguridad Informática**

## Proyecto 1

Erik Regla  
eregl09@alumnos.otalca.cl

17 de junio de 2020

## 1. Introducción

## 2. Estructura organizacional

### 2.1. Organigrama

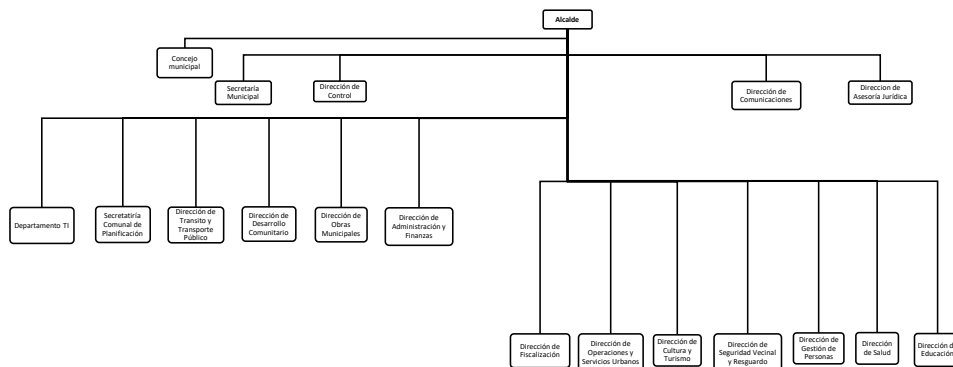


Figura 1: Organigrama

### 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 asuntos concejo cosoc y otros.** Perteneciente a la secretaría municipal. Este se compone de las siguientes secciones:
  - Sección cosoc
  - Sección consejo municipal
- **Departamento de revisión de procesos de contratación pública.** Perteneciente a la dirección de control.
- **Departamento de auditoría operativa.** Perteneciente a la dirección de control.
- **Departamento Revisión de procesos de pago, bienes y servicios.** Perteneciente a la dirección de control.

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

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.

#### 3.1. Activos de carácter transversal

A continuación se listan los activos de caracter 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>1</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>1</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>2</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>3</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>2</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<sup>3</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>4</sup> Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<sup>4</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>	CVE-2018-8374 <sup>5</sup> Tampering Vulnerability existente al momento de un fallo en la información de los perfiles. CVE-2018-8302 <sup>6</sup> Ejecución de código remota debido al fallo de manipulación de objetos en memoria, resultante en control total. CVE-2018-8159 <sup>7</sup> XSS resultante en elevación de privilegios por medio de requests web . CVE-2018-8154 <sup>8</sup> Ejecución de código remota debido a la corrupción del manejo de objetos en memoria, resultante en control total. CVE-2018-8153 <sup>9</sup> Spoofing . CVE-2018-8152 <sup>10</sup> Elevación de privilegios . CVE-2018-8151 <sup>11</sup> Corrupción de memoria . Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Posee información de alto interés para un grupo específico.

<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>	No existen respaldos físicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física.

<sup>5</sup><https://www.cvedetails.com/cve/CVE-2018-8374/>

<sup>6</sup><https://www.cvedetails.com/cve/CVE-2018-8302/>

<sup>7</sup><https://www.cvedetails.com/cve/CVE-2018-8159/>

<sup>8</sup><https://www.cvedetails.com/cve/CVE-2018-8154/>

<sup>9</sup><https://www.cvedetails.com/cve/CVE-2018-8153/>

<sup>10</sup><https://www.cvedetails.com/cve/CVE-2018-8152/>

<sup>11</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>12</sup> Ejecución remota de código por medio de CRSRF. CVE-2019-16220 <sup>13</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>14</sup> Denegación de servicio. CVE-2008-7247 <sup>15</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>12</sup><https://www.cvedetails.com/cve/CVE-2019-9787/>

<sup>13</sup><https://www.cvedetails.com/cve/CVE-2019-16220/>

<sup>14</sup><https://www.cvedetails.com/cve/CVE-2009-0819/>

<sup>15</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>16</sup> Buffer overflow causado por información EXIF. CVE-2008-7247 <sup>17</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>18</sup> Denegación de servicio. CVE-2008-7247 <sup>19</sup> Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

<sup>16</sup><https://www.cvedetails.com/cve/CVE-2019-11042/>

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

<sup>18</sup><https://www.cvedetails.com/cve/CVE-2009-0819/>

<sup>19</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>20</sup> Buffer overflow causado por información EXIF. CVE-2008-7247 <sup>21</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>20</sup><https://www.cvedetails.com/cve/CVE-2019-11042/>

<sup>21</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>22</sup> Denegación de servicio. CVE-2008-7247 <sup>23</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>24</sup> Buffer overflow causado por información EXIF. CVE-2008-7247 <sup>25</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>22</sup><https://www.cvedetails.com/cve/CVE-2009-0819/>

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

<sup>24</sup><https://www.cvedetails.com/cve/CVE-2019-11042/>

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

### 3.2. 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.

#### 3.2.1. 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>26</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>26</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.

### 3.2.2. 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>27</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>27</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.

### 3.2.3. 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>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_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>28</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.

### 3.2.4. 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>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_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>29</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.

### 3.2.5. 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>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_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>30</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.

### 3.2.6. 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>31</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>31</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>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_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>32</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.

### 3.2.7. 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>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_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>33</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>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_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>34</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.

### 3.2.8. Departamento de Asuntos Concejo Cosoc y

<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 Asuntos Concejo Cosoc y Otros. - tercer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Concejo Cosoc y Otros.
<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_DP003_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Asuntos Concejo Cosoc y Otros.
<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_DP003_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros.
<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 Asuntos Concejo Cosoc y Otros.
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Concejo Cosoc y Otros.
<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.

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

<b>Nombre</b>	CAB_DP003_001
<b>Descripción</b>	Armario de archivos para Departamento de Asuntos Concejo Cosoc y Otros.
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Asuntos Concejo Cosoc y Otros.
<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.

<b>Nombre</b>	OFLDP003_001
<b>Descripción</b>	Departamento de Asuntos Concejo Cosoc y Otros. - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - 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 Asuntos Concejo Cosoc y Otros.
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - 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 Asuntos Concejo Cosoc y Otros. - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso
<b>Propietario</b>	Jefe de Departamento de Asuntos Concejo Cosoc y Otros.
<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.

### 3.2.9. 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>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.

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

<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.

<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>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.

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

<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.

<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.

### 3.2.10. 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>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.

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

<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.

<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>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.

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



<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.

<b>Nombre</b>	OFL_DP005_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.

### 3.2.11. Dirección de Desarrollo Comunitario

<b>Nombre</b>	SWLPP001_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>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.

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

<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.

<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>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.

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

<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.

<b>Nombre</b>	OFL_PP001_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.

### 3.2.12. Dirección de Obras Municipales

<b>Nombre</b>	SWL_PP002_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Obras Municipales
<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.

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

<b>Nombre</b>	NTB_PP002_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Obras 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_PP002_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Obras 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_PP002_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Obras 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_PP002_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Obras 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_PP002_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 Obras 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_PP002_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 Obras 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_PP002_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 Obras 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_PP002_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 Obras 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_PP002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Obras Municipales
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Obras Municipales
<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.

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

<b>Nombre</b>	CAB_PP002_001
<b>Descripción</b>	Armario de archivos para Dirección de Obras Municipales
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Obras 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.

<b>Nombre</b>	OFL_PP002_001
<b>Descripción</b>	Dirección de Obras Municipales - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo 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_PP002_001
<b>Descripción</b>	Alarma de Dirección de Obras Municipales
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo 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_PP002_001
<b>Descripción</b>	Archivo de Dirección de Obras Municipales - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Obras Municipales - séptimo piso
<b>Propietario</b>	Jefe de Dirección de Obras 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.

### 3.2.13. Dirección de Tránsito y Transporte Público

<b>Nombre</b>	SWL_PP003_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Tránsito y Transporte Público
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>45</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>45</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP003_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Tránsito y Transporte Público
<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_PP003_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Tránsito y Transporte Público
<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_PP003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Tránsito y Transporte Público
<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_PP003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Tránsito y Transporte Público
<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_PP003_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 Tránsito y Transporte Público
<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_PP003_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 Tránsito y Transporte Público
<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_PP003_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 Tránsito y Transporte Público
<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_PP003_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 Tránsito y Transporte Público
<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_PP003_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Tránsito y Transporte Público
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Tránsito y Transporte Público
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>46</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.

<sup>46</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP003_001
<b>Descripción</b>	Armario de archivos para Dirección de Tránsito y Transporte Público
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Tránsito y Transporte Público
<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.

<b>Nombre</b>	OFL_PP003_001
<b>Descripción</b>	Dirección de Tránsito y Transporte Público - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo 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_PP003_001
<b>Descripción</b>	Alarma de Dirección de Tránsito y Transporte Público
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo 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_PP003_001
<b>Descripción</b>	Archivo de Dirección de Tránsito y Transporte Público - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Tránsito y Transporte Público - octavo piso
<b>Propietario</b>	Jefe de Dirección de Tránsito y Transporte Público
<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.

### 3.2.14. Dirección de Administración y Finanzas

<b>Nombre</b>	SWLPP004_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Administración y Finanzas
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>47</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>47</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP004_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Administración y Finanzas
<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_PP004_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Administración y Finanzas
<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_PP004_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Administración y Finanzas
<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_PP004_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Administración y Finanzas
<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_PP004_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 Administración y Finanzas
<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_PP004_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 Administración y Finanzas
<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_PP004_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 Administración y Finanzas
<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_PP004_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 Administración y Finanzas
<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_PP004_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Administración y Finanzas
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Administración y Finanzas
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>48</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.

<sup>48</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP004_001
<b>Descripción</b>	Armario de archivos para Dirección de Administración y Finanzas
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Administración y Finanzas
<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.

<b>Nombre</b>	OFL_PP004_001
<b>Descripción</b>	Dirección de Administración y Finanzas - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno 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_PP004_001
<b>Descripción</b>	Alarma de Dirección de Administración y Finanzas
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno 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_PP004_001
<b>Descripción</b>	Archivo de Dirección de Administración y Finanzas - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Administración y Finanzas - noveno piso
<b>Propietario</b>	Jefe de Dirección de Administración y Finanzas
<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.

### 3.2.15. Dirección de Fiscalización

<b>Nombre</b>	SWL_PP005_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Fiscalización
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>49</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>49</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP005_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Fiscalización
<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_PP005_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Fiscalización
<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_PP005_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Fiscalización
<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_PP005_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Fiscalización
<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_PP005_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 Fiscalización
<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_PP005_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 Fiscalización
<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_PP005_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 Fiscalización
<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_PP005_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 Fiscalización
<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_PP005_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Fiscalización
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Fiscalización
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>50</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.

<sup>50</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP005_001
<b>Descripción</b>	Armario de archivos para Dirección de Fiscalización
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Fiscalización
<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.

<b>Nombre</b>	OFL_PP005_001
<b>Descripción</b>	Dirección de Fiscalización - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Fiscalización - décimo 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_PP005_001
<b>Descripción</b>	Alarma de Dirección de Fiscalización
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Fiscalización - décimo 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_PP005_001
<b>Descripción</b>	Archivo de Dirección de Fiscalización - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Fiscalización - décimo piso
<b>Propietario</b>	Jefe de Dirección de Fiscalización
<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.

### 3.2.16. Dirección de Operaciones y Servicios Urbanos

<b>Nombre</b>	SWL_PP006_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Operaciones y Servicios Urbanos
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>51</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>51</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP006_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Operaciones y Servicios Urbanos
<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_PP006_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Operaciones y Servicios Urbanos
<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_PP006_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Operaciones y Servicios Urbanos
<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_PP006_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Operaciones y Servicios Urbanos
<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_PP006_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 Operaciones y Servicios Urbanos
<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_PP006_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 Operaciones y Servicios Urbanos
<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_PP006_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 Operaciones y Servicios Urbanos
<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_PP006_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 Operaciones y Servicios Urbanos
<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_PP006_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Operaciones y Servicios Urbanos
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Operaciones y Servicios Urbanos
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>52</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_PP006_001
<b>Descripción</b>	Armario de archivos para Dirección de Operaciones y Servicios Urbanos
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Operaciones y Servicios Urbanos
<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.

<b>Nombre</b>	OFLPP006_001
<b>Descripción</b>	Dirección de Operaciones y Servicios Urbanos - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo 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.

<sup>52</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	RNG_PP006_001
<b>Descripción</b>	Alarma de Dirección de Operaciones y Servicios Urbanos
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo 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_PP006_001
<b>Descripción</b>	Archivo de Dirección de Operaciones y Servicios Urbanos - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Operaciones y Servicios Urbanos - onceavo piso
<b>Propietario</b>	Jefe de Dirección de Operaciones y Servicios Urbanos
<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.

### 3.2.17. Dirección de Cultura y Turismo

<b>Nombre</b>	SWL_PP007_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Cultura y Turismo
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>53</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>53</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>



<b>Nombre</b>	NTB_PP007_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Cultura y Turismo
<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_PP007_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Cultura y Turismo
<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_PP007_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Cultura y Turismo
<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_PP007_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Cultura y Turismo
<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_PP007_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 Cultura y Turismo
<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_PP007_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 Cultura y Turismo
<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_PP007_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 Cultura y Turismo
<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_PP007_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 Cultura y Turismo
<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_PP007_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Cultura y Turismo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Cultura y Turismo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>54</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.

<sup>54</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP007_001
<b>Descripción</b>	Armario de archivos para Dirección de Cultura y Turismo
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Cultura y Turismo
<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.

<b>Nombre</b>	OFL_PP007_001
<b>Descripción</b>	Dirección de Cultura y Turismo - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo 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_PP007_001
<b>Descripción</b>	Alarma de Dirección de Cultura y Turismo
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo 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_PP007_001
<b>Descripción</b>	Archivo de Dirección de Cultura y Turismo - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Cultura y Turismo - doceavo piso
<b>Propietario</b>	Jefe de Dirección de Cultura y Turismo
<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.

### 3.2.18. Dirección de Seguridad Vecinal y Resguardo

<b>Nombre</b>	SWL_PP008_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Seguridad Vecinal y Resguardo
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>55</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>55</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP008_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Seguridad Vecinal y Resguardo
<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_PP008_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Seguridad Vecinal y Resguardo
<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_PP008_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Seguridad Vecinal y Resguardo
<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_PP008_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Seguridad Vecinal y Resguardo
<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_PP008_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 Seguridad Vecinal y Resguardo
<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_PP008_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 Seguridad Vecinal y Resguardo
<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_PP008_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 Seguridad Vecinal y Resguardo
<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_PP008_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 Seguridad Vecinal y Resguardo
<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_PP008_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Seguridad Vecinal y Resguardo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Seguridad Vecinal y Resguardo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>56</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_PP008_001
<b>Descripción</b>	Armario de archivos para Dirección de Seguridad Vecinal y Resguardo
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Seguridad Vecinal y Resguardo
<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.

<b>Nombre</b>	OFLPP008_001
<b>Descripción</b>	Dirección de Seguridad Vecinal y Resguardo - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo 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.

<sup>56</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	RNG_PP008_001
<b>Descripción</b>	Alarma de Dirección de Seguridad Vecinal y Resguardo
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo 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_PP008_001
<b>Descripción</b>	Archivo de Dirección de Seguridad Vecinal y Resguardo - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Seguridad Vecinal y Resguardo - treceavo piso
<b>Propietario</b>	Jefe de Dirección de Seguridad Vecinal y Resguardo
<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.

### 3.2.19. Dirección de Gestión de Personas

<b>Nombre</b>	SWL_PP009_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Gestión de Personas
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>57</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>57</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP009_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Gestión de Personas
<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_PP009_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Gestión de Personas
<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_PP009_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Gestión de Personas
<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_PP009_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Gestión de Personas
<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_PP009_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 Gestión de Personas
<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_PP009_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 Gestión de Personas
<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_PP009_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 Gestión de Personas
<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_PP009_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 Gestión de Personas
<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_PP009_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Gestión de Personas
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Gestión de Personas
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>58</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.

<sup>58</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP009_001
<b>Descripción</b>	Armario de archivos para Dirección de Gestión de Personas
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Gestión de Personas
<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.

<b>Nombre</b>	OFL_PP009_001
<b>Descripción</b>	Dirección de Gestión de Personas - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo 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_PP009_001
<b>Descripción</b>	Alarma de Dirección de Gestión de Personas
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo 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_PP009_001
<b>Descripción</b>	Archivo de Dirección de Gestión de Personas - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Gestión de Personas - catorceavo piso
<b>Propietario</b>	Jefe de Dirección de Gestión de Personas
<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.

### 3.2.20. Dirección de Salud

<b>Nombre</b>	SWLPP0010_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Salud
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>59</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>59</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP0010_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Salud
<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_PP0010_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Salud
<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_PP0010_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Salud
<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_PP0010_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Salud
<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_PP0010_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 Salud
<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_PP0010_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 Salud
<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_PP0010_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 Salud
<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_PP0010_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 Salud
<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_PP0010_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Salud
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Salud
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>60</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.

<sup>60</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP0010_001
<b>Descripción</b>	Armario de archivos para Dirección de Salud
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Salud
<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.

<b>Nombre</b>	OFL_PP0010_001
<b>Descripción</b>	Dirección de Salud - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Salud - décimo 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_PP0010_001
<b>Descripción</b>	Alarma de Dirección de Salud
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Salud - décimo 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_PP0010_001
<b>Descripción</b>	Archivo de Dirección de Salud - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Salud - décimo quinto piso
<b>Propietario</b>	Jefe de Dirección de Salud
<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.

### 3.2.21. Dirección de Educación

<b>Nombre</b>	SWLPP0011_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Educación
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>61</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>61</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP0011_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Educación
<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_PP0011_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Educación
<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_PP0011_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Educación
<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_PP0011_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Educación
<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_PP0011_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 Educación
<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_PP0011_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 Educación
<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_PP0011_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 Educación
<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_PP0011_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 Educación
<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_PP0011_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Educación
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Educación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>62</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.

<sup>62</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP0011_001
<b>Descripción</b>	Armario de archivos para Dirección de Educación
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Educación
<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.

<b>Nombre</b>	OFL_PP0011_001
<b>Descripción</b>	Dirección de Educación - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Educación - décimo 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_PP0011_001
<b>Descripción</b>	Alarma de Dirección de Educación
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Educación - décimo 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_PP0011_001
<b>Descripción</b>	Archivo de Dirección de Educación - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Educación - décimo sexto piso
<b>Propietario</b>	Jefe de Dirección de Educación
<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.

### 3.2.22. Secretaría Comunal de PPlanificación

<b>Nombre</b>	SWLPP0012_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Secretaría Comunal de PPlanificación
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>63</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>63</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP0012_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso - recurso estático
<b>Propietario</b>	Jefe de Secretaría Comunal de PPlanificación
<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_PP0012_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso - recurso estático
<b>Propietario</b>	Secretario de Secretaría Comunal de PPlanificación
<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_PP0012_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Secretaría Comunal de PPlanificación
<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_PP0012_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Secretaría Comunal de PPlanificación
<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_PP0012_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 Secretaría Comunal de PPlanificación
<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_PP0012_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 Secretaría Comunal de PPlanificación
<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_PP0012_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 Secretaría Comunal de PPlanificación
<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_PP0012_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 Secretaría Comunal de PPlanificación
<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_PP0012_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Secretaría Comunal de PPlanificación
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Secretaría Comunal de PPlanificación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>64</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_PP0012_001
<b>Descripción</b>	Armario de archivos para Secretaría Comunal de PPlanificación
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso - recurso estático
<b>Propietario</b>	Jefe de Secretaría Comunal de PPlanificación
<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.

<b>Nombre</b>	OFLPP0012_001
<b>Descripción</b>	Secretaría Comunal de PPlanificación - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo 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.

<sup>64</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	RNG_PP0012_001
<b>Descripción</b>	Alarma de Secretaría Comunal de PPlanificación
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo 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_PP0012_001
<b>Descripción</b>	Archivo de Secretaría Comunal de PPlanificación - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Secretaría Comunal de PPlanificación - décimo séptimo piso
<b>Propietario</b>	Jefe de Secretaría Comunal de PPlanificación
<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.

### 3.2.23. Dirección de Asesoría Jurídica

<b>Nombre</b>	SWL_PP0013_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Asesoría Jurídica
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>65</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>65</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP0013_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Asesoría Jurídica
<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_PP0013_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Asesoría Jurídica
<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_PP0013_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Asesoría Jurídica
<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_PP0013_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Asesoría Jurídica
<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_PP0013_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 Asesoría Jurídica
<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_PP0013_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 Asesoría Jurídica
<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_PP0013_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 Asesoría Jurídica
<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_PP0013_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 Asesoría Jurídica
<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_PP0013_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Asesoría Jurídica
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Asesoría Jurídica
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>66</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.

<sup>66</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP0013_001
<b>Descripción</b>	Armario de archivos para Dirección de Asesoría Jurídica
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Asesoría Jurídica
<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.

<b>Nombre</b>	OFL_PP0013_001
<b>Descripción</b>	Dirección de Asesoría Jurídica - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo 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_PP0013_001
<b>Descripción</b>	Alarma de Dirección de Asesoría Jurídica
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo 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_PP0013_001
<b>Descripción</b>	Archivo de Dirección de Asesoría Jurídica - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Asesoría Jurídica - décimo octavo piso
<b>Propietario</b>	Jefe de Dirección de Asesoría Jurídica
<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.

### 3.2.24. Secretaría Municipal

<b>Nombre</b>	SWL_PP0014_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Municipal - primer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Secretaría Municipal
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>67</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>67</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP0014_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Municipal - primer piso - recurso estático
<b>Propietario</b>	Jefe de Secretaría Municipal
<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_PP0014_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Municipal - primer piso - recurso estático
<b>Propietario</b>	Secretario de Secretaría Municipal
<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_PP0014_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Municipal - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Secretaría Municipal
<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_PP0014_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Municipal - primer piso - recurso estático
<b>Propietario</b>	Encargado de TI de Secretaría Municipal
<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_PP0014_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 Secretaría Municipal
<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_PP0014_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 Secretaría Municipal
<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_PP0014_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 Secretaría Municipal
<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_PP0014_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 Secretaría Municipal
<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_PP0014_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Secretaría Municipal
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Secretaría Municipal - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Secretaría Municipal
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>68</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.

<sup>68</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP0014_001
<b>Descripción</b>	Armario de archivos para Secretaría Municipal
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Secretaría Municipal - primer piso - recurso estático
<b>Propietario</b>	Jefe de Secretaría Municipal
<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.

<b>Nombre</b>	OFL_PP0014_001
<b>Descripción</b>	Secretaría Municipal - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Secretaría Municipal - 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_PP0014_001
<b>Descripción</b>	Alarma de Secretaría Municipal
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Secretaría Municipal - 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_PP0014_001
<b>Descripción</b>	Archivo de Secretaría Municipal - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Secretaría Municipal - primer piso
<b>Propietario</b>	Jefe de Secretaría Municipal
<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.

### 3.2.25. Dirección de Control

<b>Nombre</b>	SWLPP0015_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Control - cuarto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Control
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>69</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>69</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>



<b>Nombre</b>	NTB_PP0015_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Control - cuarto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Control
<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_PP0015_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Control - cuarto piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Control
<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_PP0015_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Control - cuarto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Control
<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_PP0015_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Control - cuarto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Control
<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_PP0015_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 Control
<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_PP0015_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 Control
<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_PP0015_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 Control
<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_PP0015_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 Control
<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_PP0015_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Control
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Control - cuarto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Control
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>70</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.

<sup>70</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>

<b>Nombre</b>	CAB_PP0015_001
<b>Descripción</b>	Armario de archivos para Dirección de Control
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Control - cuarto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Control
<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.

<b>Nombre</b>	OFL_PP0015_001
<b>Descripción</b>	Dirección de Control - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Control - 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_PP0015_001
<b>Descripción</b>	Alarma de Dirección de Control
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Control - 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_PP0015_001
<b>Descripción</b>	Archivo de Dirección de Control - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Control - cuarto piso
<b>Propietario</b>	Jefe de Dirección de Control
<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.

### 3.2.26. Dirección de Comunicaciones

<b>Nombre</b>	SWLPP0015_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Comunicaciones
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>71</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>71</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_PP0015_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Comunicaciones
<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_PP0015_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Comunicaciones
<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_PP0015_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Comunicaciones
<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_PP0015_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Comunicaciones
<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_PP0015_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 Comunicaciones
<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_PP0015_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 Comunicaciones
<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_PP0015_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 Comunicaciones
<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_PP0015_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 Comunicaciones
<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_PP0015_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Comunicaciones
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Comunicaciones
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>72</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.

<sup>72</sup><https://www.cvedetails.com/cve/CVE-2017-7494/>



<b>Nombre</b>	CAB_PP0015_001
<b>Descripción</b>	Armario de archivos para Dirección de Comunicaciones
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Comunicaciones
<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.

<b>Nombre</b>	OFL_PP0015_001
<b>Descripción</b>	Dirección de Comunicaciones - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno 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_PP0015_001
<b>Descripción</b>	Alarma de Dirección de Comunicaciones
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno 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_PP0015_001
<b>Descripción</b>	Archivo de Dirección de Comunicaciones - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Comunicaciones - décimo noveno piso
<b>Propietario</b>	Jefe de Dirección de Comunicaciones
<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

Remuneraciones Registro comunal de permisos de circulación Licencias de conducir Patentes municipales Control de bienes Adquisición y control de bodegas Contabilidad gubernamental Banco de datos propiedades comunales Oficina de partes Departamento Tecnologías Juzgados de policía local Administración red departamente licencias de conducir administracion red departamente de juzgados de policia local partes empadronados departamento de seguridad ciudadana administración red departamente patentes municipales y tesorería administración red del departamente de seguridad ciudadana administración de dirección de obras municipales administración de sistemas de egresos, recursos humanos y remuneraciones plataforma de egresos administracion de sistemas de desarrollo comunitario sistemas computaciones por internet y sistemas sociales mantencion y administración de cartografia digital

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>	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 sitio web.
<b>Sub Área</b>	Dirección de Comunicaciones. Oficina de Asuntos Municipales. Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<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 MYQSL 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 sitio web.
<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 sitio web. Nivel general, Confiabilidad sitio web.
<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 en servidor principal
<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**