



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

# **Seguridad Informática**

## Proyecto 1

Erik Regla  
eregla09@alumnos.otalca.cl

10 de junio de 2020

## 1. Introducción

## 2. Estructura organizacional

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

  

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

<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-2018-8302 <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-2018-8302/>

<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_003 para 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.

<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.

<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.

<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.

<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.

<b>Nombre</b>	OFL_SE001_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.

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

<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.

  

<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.

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

<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.

<b>Nombre</b>	OFL_SE002_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.

<b>Nombre</b>	SWLDP001
<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.

<b>Nombre</b>	SWLDP002
<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.

<b>Nombre</b>	SWLDP003
<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.

  

<b>Nombre</b>	SWL_DP004
<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.

  

<b>Nombre</b>	SWLDP005
<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.

<b>Nombre</b>	SWLDP006
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Revisión de Pagos de Bienes y Servicios
<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_DP006_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Revisión de Pagos de Bienes y Servicios
<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_DP006_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Revisión de Pagos de Bienes y Servicios
<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_DP006_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Revisión de Pagos de Bienes y Servicios
<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_DP006_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Revisión de Pagos de Bienes y Servicios
<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_DP006_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 Pagos de Bienes y Servicios
<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_DP006_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 Pagos de Bienes y Servicios
<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_DP006_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 Pagos de Bienes y Servicios
<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_DP006_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 Pagos de Bienes y Servicios
<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_DP006_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Revisión de Pagos de Bienes y Servicios
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Revisión de Pagos de Bienes y Servicios
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>42</sup> Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

  

<b>Nombre</b>	CAB_DP006_001
<b>Descripción</b>	Armario de archivos para Departamento de Revisión de Pagos de Bienes y Servicios
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Revisión de Pagos de Bienes y Servicios
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

<b>Nombre</b>	OFLDP006_001
<b>Descripción</b>	Departamento de Revisión de Pagos de Bienes y Servicios - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - 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_DP006_001
<b>Descripción</b>	Alarma de Departamento de Revisión de Pagos de Bienes y Servicios
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - 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_DP006_001
<b>Descripción</b>	Archivo de Departamento de Revisión de Pagos de Bienes y Servicios - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso
<b>Propietario</b>	Jefe de Departamento de Revisión de Pagos de Bienes y Servicios
<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

## 5. Matriz de riesgos

## 6. Política de seguridad

### Referencias

- [1] Bill McDaniel. *An Algorithm for Error Correcting Cyclic Redundance Checks*. <https://www.drdoobs.com/an-algorithm-for-error-correcting-cyclic/184401662>, 2002.
- [2] Linux Man pages. *gpg(1) - Linux man page*. <https://linux.die.net/man/1/gpg>.
- [3] VeraCrypt. *Documentation*. <https://www.veracrypt.fr/en/Documentation.html>.
- [4] Koopman, Philip and Chakravarty, T. *Cyclic redundancy code (CRC) polynomial selection for embedded networks*. 10.1109/DSN.2004.1311885. 2004.