



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

# **Seguridad Informática**

## Proyecto 1

Erik Regla  
eregla09@alumnos.otalca.cl

22 de junio de 2020

# Índice

<b>I</b>	<b>Resumen Ejecutivo</b>	<b>4</b>
<b>II</b>	<b>Introducción</b>	<b>5</b>
<b>III</b>	<b>Desarrollo</b>	<b>6</b>
<b>1.</b>	<b>Estructura organizacional</b>	<b>6</b>
1.1.	Organigrama . . . . .	6
1.2.	Rationale . . . . .	6
<b>2.</b>	<b>Identificación de activos</b>	<b>8</b>
2.1.	Contexto . . . . .	8
2.2.	Situación actual . . . . .	8
2.3.	Procesos . . . . .	8
2.3.1.	Sistema contabilidad gubernamental . . . . .	8
2.3.2.	Sistema de tesorería municipal . . . . .	9
2.4.	Sistema patentes comerciales . . . . .	10
2.5.	Sistema permisos de circulación . . . . .	10
2.6.	Activos de carácter transversal . . . . .	11
2.7.	Activos externalizados . . . . .	20
2.8.	Activos de carácter específico . . . . .	22
2.8.1.	Oficina de Partes Alcaldía . . . . .	23
2.8.2.	Oficina de Registro Municipal de Transferencias . . . . .	27
2.8.3.	Oficina de Control de Archivo y reorientación . . . . .	32
2.8.4.	Sección Resolutiva . . . . .	37
2.8.5.	Sección Administrativa . . . . .	42
2.8.6.	Departamento de Asuntos Municipales . . . . .	46
2.8.7.	Departamento de Certificación y archivo . . . . .	52
2.8.8.	Departamento de Cartografía . . . . .	58

2.8.9. Departamento de Revisión de Procesos de Contratación . . . . .	64
2.8.10. Departamento de Auditoría Operativa . . . . .	71
2.8.11. Dirección de revisión de Procesos de Pago, Bienes y Servicios . . . . .	77
2.8.12. Departamento de Tecnologías de la Información . . . . .	83
<b>3. Análisis de riesgos</b>	<b>90</b>
3.1. Riesgos asociados a factores no tecnológicos . . . . .	90
3.2. Riesgos asociados a procesos municipales . . . . .	95
3.3. Riesgos asociados a control del personal . . . . .	102
3.4. Riesgos asociados de índole técnica . . . . .	104
3.5. Riesgos generales asociados a ingeniería social . . . . .	116
<b>4. Matriz de riesgos</b>	<b>116</b>
<b>5. Políticas de seguridad</b>	<b>116</b>
5.1. Objetivos de la política . . . . .	116
5.2. Declaración de autoridad y alcance . . . . .	117
5.3. Política de uso aceptable . . . . .	117
5.4. Política de identificación y autenticación . . . . .	117
5.5. Política de acceso a internet . . . . .	117
5.6. Política de acceso . . . . .	118
5.7. Política de acceso remoto . . . . .	118
5.8. Políticas del manejo de incidentes . . . . .	118
<b>IV Conclusiones</b>	<b>120</b>
<b>V Bibliografía</b>	<b>121</b>

## Parte I

# Resumen Ejecutivo

La parte uno muestra un resumen ejecutivo de el esquema de este documento a fin de resumir la estructura de su contenido.

La parte dos presenta una introducción al problema a resolver.

La parte tres presenta el desarrollo del documento considerando las siguientes secciones:

- Estructura organizacional.
- Identificación de activos.
- Análisis de riesgos.
- Matriz de riesgos.
- Políticas de seguridad.

La parte cuatro presenta las conclusiones obtenidas de este trabajo.

La parte cinco presenta la bibliografía utilizada como referencia en este documento.

## **Parte II**

# **Introducción**

En este documento se realizará la ejecución de un análisis de riesgos para un municipio ficticio, el cual cuenta con una serie de problemas administrativos derivados de previas administraciones y direcciones del departamento de tecnologías de la información.

Para la creación de este municipio ficticio se ha utilizado como referencia la información real de municipios Chilenos, informes de contraloría y descripciones de procesos ya existentes en in intento de fidelizar el informe a la realidad diaria exagerando algunos atributos para poder darle asi contenido al informe – nuevamente, es ficticio.

Parte III

# Desarrollo

## 1. Estructura organizacional

### 1.1. Organigrama

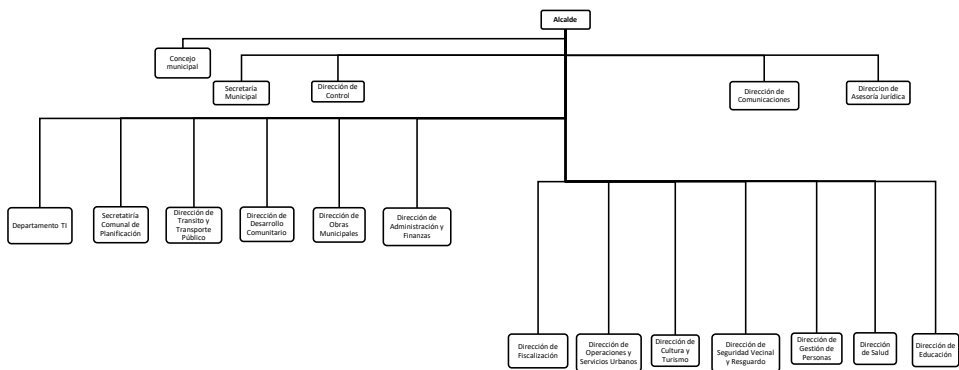


Figura 1: Organigrama

### 1.2. Rationale

El alcance de este trabajo abarca solo las siguientes divisiones:

- **Departamento de asuntos municipales.** Perteneciente a la secretaría municipal. Este se com-

pone de las siguientes oficinas:

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

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.

## **2. Identificación de activos**

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

### **2.2. Situación actual**

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

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

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

### **2.3. Procesos**

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

#### **2.3.1. Sistema contabilidad gubernamental**

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

---

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

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



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

Funciones de este sistema:

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

### **2.3.2. Sistema de tesorería municipal**

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

Funciones de este sistema:

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

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

## **2.4. Sistema patentes comerciales**

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

Funciones de este sistema:

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

## **2.5. Sistema permisos de circulación**

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

Funciones de este sistema:

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

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

## 2.6. Activos de carácter transversal

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

<b>Nombre</b>	RTR_PRINC_001
<b>Descripción</b>	Router principal Cisco 2901, gateway externo perteneciente a la municipalidad
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2013-1241 <sup>3</sup> Autenticación inválida en cabeceras del módulo ISM. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

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

<b>Nombre</b>	RTR_SECUN_001
<b>Descripción</b>	Router secundario Cisco 2901, utilizado de punto intermedio hacia la red interna
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>4</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

<b>Nombre</b>	SWLNODES_001
<b>Descripción</b>	Switch general Cisco Catalyst 2960, para nodo base del árbol de conectividad
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>5</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

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

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

<b>Nombre</b>	SRV_SHARE_001
<b>Descripción</b>	Dell PowerEdge R520 750W E5 2440
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

<b>Nombre</b>	OSS_WINDO_001
<b>Descripción</b>	Windows Server 2019 Datacenter Edition
<b>Categoría</b>	Sistemas Operativos
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 2 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Mas de 390 vulnerabilidades detectadas <sup>6</sup> Quiebre autenticación de llave seguridad. Dependencia de licencias. Ejecución de malwarepor falta de software AV. Dependencia de licencias. Desastres lógicos. Falta de encriptado. Carencia de licencias. Falta de protocolo de borrado de información.

---

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

<b>Nombre</b>	EXE_EXCHA_001
<b>Descripción</b>	Módulo servidor para Microsoft Exchange 2016, para uso de correos corporativos de los funcionarios de la municipalidad.
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	<p>CVE-2018-8374<sup>7</sup> Tampering Vulnerability existente al momento de un fallo en la información de los perfiles.</p> <p>CVE-2018-8302<sup>8</sup> Ejecución de código remota debido al fallo de manipulación de objetos en memoria, resultante en control total.</p> <p>CVE-2018-8159<sup>9</sup> XSS resultante en elevación de privilegios por medio de requests web .</p> <p>CVE-2018-8154<sup>10</sup> Ejecución de código remota debido a la corrupción del manejo de objetos en memoria, resultante en control total.</p> <p>CVE-2018-8153<sup>11</sup> Spoofing .</p> <p>CVE-2018-8152<sup>12</sup> Elevación de privilegios .</p> <p>CVE-2018-8151<sup>13</sup> Corrupción de memoria .</p> <p>Quiebre autenticación de llave seguridad.</p> <p>Desastres lógicos.</p> <p>Dependencia de licencias.</p> <p>Falta de encriptado.</p> <p>Carencia de licencias.</p> <p>Falta de protocolo de borrado de información.</p> <p>No existe plan de recuperación de desastres.</p> <p>Inexistencia de respaldos digitales.</p> <p>Falta de documentación e implantación de políticas para envío de correos masivos.</p>

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

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

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

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

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

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

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

<b>Nombre</b>	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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad. Transaccion rota.

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

<b>Nombre</b>	EXE_MYSQL_001
<b>Descripción</b>	Servidor MySQL 6.0.9 Beta3 para EXE_WPRES_001
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_001
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2009-0819 <sup>16</sup> Denegación de servicio. CVE-2008-7247 <sup>17</sup> Bypass de restricciones RBAC. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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

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

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

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

<b>Nombre</b>	EXE_SQLTB_001
<b>Descripción</b>	Base de datos MySQL en EXE_MYSQL_001 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>	Está sujeta a vulnerabilidades de manera transitiva.

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

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

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



<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 claro de las vulnerabilidades. Está sujeta a vulnerabilidades de manera transitiva. No existe plan de recuperación de desastres. Inexistencia de respaldos digitales. No interoperabilidad con estándar de norma técnica para los Órganos de la Administración del Estado. Transaccion rota. Falta de encriptado. Residuos de información. Dependencia de licencias. Ejecución de malware por falta de software AV. Denegación de servicio. Desastres de origen humano.

<b>Nombre</b>	EXE_MYSQL_002
<b>Descripción</b>	Servidor MySQL 6.0.9 Beta3 para EXE_ADMIN_002
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_002
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	CVE-2009-0819 <sup>20</sup> Denegación de servicio. CVE-2008-7247 <sup>21</sup> Bypass de restricciones RBAC. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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

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

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

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

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

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

<b>Nombre</b>	EXE_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 claro de las vulnerabilidades. Está sujeta a vulnerabilidades de manera transitiva. Quiebre autenticación de llave seguridad. Falta de encriptado. Dependencia de licencias. Falta de protocolo de borrado de información.

<b>Nombre</b>	EXE_MYSQL_003
<b>Descripción</b>	Servidor MySQL 6.0.9 Beta3 para EXE_ADMIN_003
<b>Categoría</b>	Software
<b>Ubicación</b>	SRV_SHARE_003
<b>Propietario</b>	Departamento de TI
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	CVE-2009-0819 <sup>24</sup> Denegación de servicio. CVE-2008-7247 <sup>25</sup> Bypass de restricciones RBAC. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

<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.

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

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

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

## 2.7. Activos externalizados

<b>Nombre</b>	EXT_PLATF_001
<b>Descripción</b>	Sistema de tesorería municipal
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 1
<b>Valoración</b>	Confidencialidad: 3 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Multas por servicios operaciones (como agua, luz). Pérdida de soporte de proyectos licitados. Fin de facturaciones. Desastres lógicos. Divulgación y copiado de informacion. Decretos de pago imputados a cuentas presupuestarias que no corresponden. Emisión de decretos de pago sin registrar datos y/o sin comprobantes. Recepción de pagos con cálculos de intereses y multas fuera de período. Mantenimiento preventivo externalizado ejecutado deficientemente. No existe plan de recuperación de desastres.

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

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

<b>Nombre</b>	EXT_PLATF_002
<b>Descripción</b>	Sistema de patentes comerciales
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 2
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	<p>Inexistencia de respaldos físicos.</p> <p>No interoperabilidad con estándar de norma técnica para los Órganos de la Administración del Estado.</p> <p>Falta de encriptado.</p> <p>Mantenimiento preventivo externalizado ejecutado deficientemente.</p> <p>Fin de facturaciones.</p> <p>Multas por servicios operaciones (como agua, luz).</p> <p>Pérdida de soporte de proyectos licitados.</p> <p>Soporte externo ejecutado de manera deficiente. Obtención y/o renovación de patentes municipales sin ingreso y/o acreditación de dataos del contribuyente, propiedad, sucursales y datos del servicio de impuestos internos.</p> <p>No existe plan de recuperación de desastres.</p>

<b>Nombre</b>	EXT_PLATF_003
<b>Descripción</b>	Sistema de Permisos de Circulación
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 3
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 2
<b>Vulnerabilidades y Amenazas</b>	<p>No interoperabilidad con estándar de norma técnica para los Órganos de la Administración del Estado.</p> <p>Integridad de información por estructura de datos.</p> <p>Inexistencia de respaldos digitales.</p> <p>No existe plan de recuperación de desastres.</p>

<b>Nombre</b>	EXT_PLATF_004
<b>Descripción</b>	Sistema de contabilidad gubernamental
<b>Categoría</b>	Software, base de datos transitiva
<b>Ubicación</b>	Sala de servidores - primer piso
<b>Propietario</b>	Empresa Externa 1
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Multas por servicios operaciones (como agua, luz). Pérdida de soporte de proyectos licitados. Fin de facturaciones. Divulgación y copiado de informacion. Emisión de cheque individual sin consultar datos en sistema de contabilidad gubernamental. No interoperabilidad con estándar de norma técnica para los Órganos de la Administración del Estado. Integridad de información por estructura de datos. Transaccion rota. Emisión de decretos de pago sin registrar datos y/o sin comprobantes. Falta de encriptado. Residuos de información. Mantenimiento preventivo externalizado ejecutado deficientemente. Denegación de servicio. Ejecución de malwarepor falta de software AV. Inexistencia de respaldos digitales. Falta de protocolo de borrado de información. Soporte externo ejecutado de manera deficiente. No existe plan de recuperación de desastres.

## 2.8. Activos de carácter específico

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

### 2.8.1. Oficina de Partes Alcaldía

<b>Nombre</b>	NTB_OF001_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Partes Alcaldía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.



<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_OF001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Partes Alcaldía
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Partes Alcaldía - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>28</sup> Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<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>	Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	OFL_OF001_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>	Desastres naturales. Desastres de origen humano.

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

<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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

### 2.8.2. Oficina de Registro Municipal de Transferencias

<b>Nombre</b>	NTB_OF002_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Registro Municipal de Transferencias
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_OF002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Registro Municipal de Transferencias
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>29</sup> Ejecución remota de código. Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<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>	Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	OFL_OF002_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>	Desastres naturales. 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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

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

<b>Nombre</b>	NTB_OF003_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Jefe de Oficina de Control de Archivo y reorientación
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.



<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>	Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de información. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transacción rota. Phishing. Falta de documentación e implementación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de información. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transacción rota. Phishing. Falta de documentación e implementación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de información. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transacción rota. Phishing. Falta de documentación e implementación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_OF003_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Control de Archivo y reorientación
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Oficina de Control de Archivo y reorientación - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de certificación y archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>30</sup> Ejecución remota de código. Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<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>	Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	OFL_OF003_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>	Desastres naturales. 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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

#### 2.8.4. Sección Resolutiva

<b>Nombre</b>	NTB_SE001_101
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Dirección de Sección Resolutiva
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_SE001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Sección Resolutiva
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>31</sup> Ejecución remota de código. Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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



<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>	Desastres naturales. Desastres de origen humano.

<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>	Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	RNG_SE001_001
<b>Descripción</b>	Alarma de Sección Resolutiva
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Sección Resolutiva - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

### 2.8.5. Sección Administrativa

<b>Nombre</b>	NTB_SE002_101
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Dirección de Sección Administrativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_SE002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Sección Administrativa
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Sección Administrativa - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>32</sup> Ejecución remota de código. Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<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>	Desastres naturales. Desastres de origen humano.

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

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

<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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

#### 2.8.6. Departamento de Asuntos Municipales

<b>Nombre</b>	SWLDP001_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>33</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.



<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_DP001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Asuntos Municipales
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Asuntos Municipales - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>34</sup> Ejecución remota de código. Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<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>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

<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>	Desastres naturales. Desastres de origen humano.

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

<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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

### 2.8.7. Departamento de Certificación y archivo

<b>Nombre</b>	SWLDP002_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>35</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.



<b>Nombre</b>	NAS_DP002_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Certificación y Archivo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Certificación y Archivo - segundo piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>36</sup> Ejecución remota de código. Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<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>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

<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>	Desastres naturales. Desastres de origen humano.

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

<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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

#### 2.8.8. Departamento de Cartografía

<b>Nombre</b>	SWLDP003_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>37</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<b>Nombre</b>	NTB_DP003_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_DP003_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_DP003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_DP003_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	EML_DP003_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_DP003_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_DP003_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_DP003_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_DP003_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Cartografía
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>38</sup> Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<b>Nombre</b>	CAB_DP003_001
<b>Descripción</b>	Armario de archivos para Departamento de Cartografía
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

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

<b>Nombre</b>	RNG_DP003_001
<b>Descripción</b>	Alarma de Departamento de Cartografía
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Cartografía - tercer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Quiebre autenticación de llave seguridad.

<b>Nombre</b>	ARC_DP003_001
<b>Descripción</b>	Archivo de Departamento de Cartografía - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Cartografía - tercer piso
<b>Propietario</b>	Jefe de Departamento de Cartografía
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

#### 2.8.9. Departamento de Revisión de Procesos de Contratación

<b>Nombre</b>	SWLDP004_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>39</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<sup>39</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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_DP004_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Revisión de Procesos de Contratación Pública
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>40</sup> Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<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>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

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

<b>Nombre</b>	OFLDP004_001
<b>Descripción</b>	Departamento de Revisión de Procesos de Contratación Pública - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Desastres naturales. 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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

### 2.8.10. Departamento de Auditoría Operativa

<b>Nombre</b>	SWLDP005_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>41</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	NTB_DP005_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

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

<b>Nombre</b>	NTB_DP005_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.



<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>	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<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>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_DP005_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Auditoría Operativa
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Auditoría Operativa - quinto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Auditoría Operativa
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>42</sup> Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<sup>42</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>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

<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>	Desastres naturales. 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>	Quiebre autenticación de llave seguridad.

<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>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

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

<b>Nombre</b>	SWLPP001_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>43</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

<b>Nombre</b>	NTB_PP001_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_PP001_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Secretario de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_PP001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Ejecutivo de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_PP001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Encargado de TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	EML_PP001_001
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_PP001_002
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Secretario de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.



<b>Nombre</b>	EML_PP001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Ejecutivo de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_PP001_003
<b>Descripción</b>	Cuenta de correo corporativa
<b>Categoría</b>	Activo de información tangible
<b>Ubicación</b>	EXE_EXCHA_001
<b>Propietario</b>	Encargado de TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_PP001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Desarrollo Comunitario
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>44</sup> Ejecución remota de código. Divulgación y copiado de información. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	CAB_PP001_001
<b>Descripción</b>	Armario de archivos para Dirección de Desarrollo Comunitario
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

<b>Nombre</b>	OFL_PP001_001
<b>Descripción</b>	Dirección de Desarrollo Comunitario - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Desastres naturales. Desastres de origen humano.

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

<b>Nombre</b>	RNG_PP001_001
<b>Descripción</b>	Alarma de Dirección de Desarrollo Comunitario
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Quiebre autenticación de llave seguridad.

<b>Nombre</b>	ARC_PP001_001
<b>Descripción</b>	Archivo de Dirección de Desarrollo Comunitario - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Dirección de Desarrollo Comunitario - sexto piso
<b>Propietario</b>	Jefe de Dirección de Desarrollo Comunitario
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

#### 2.8.12. Departamento de Tecnologías de la Información

<b>Nombre</b>	SWL_TI001_0001
<b>Descripción</b>	Switch general Cisco Catalyst 2960 para específico del departamento
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-3881 <sup>45</sup> Ejecución arbitraria de código (resuelto). Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<sup>45</sup><https://www.cvedetails.com/cve/CVE-2017-3881/>

<b>Nombre</b>	NTB_TI001_001
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_TI001_002
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Secretario de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_TI001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Ejecutivo de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	NTB_TI001_003
<b>Descripción</b>	Thinkpad T490 series, equipo corporativo
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Encargado de TI de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

<b>Nombre</b>	EML_TI001_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 Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_TI001_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 Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_TI001_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 Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	EML_TI001_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 Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing. Falta de documentación e implantación de políticas para envío de correos masivos.

<b>Nombre</b>	NAS_TI001_001
<b>Descripción</b>	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Tecnologías de la Información
<b>Categoría</b>	Hardware TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Departamento de TI - Encargado TI de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
<b>Vulnerabilidades y Amenazas</b>	CVE-2017-7494 <sup>46</sup> Ejecución remota de código. Divulgación y copiado de informacion. Pérdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

<b>Nombre</b>	CAB_TI001_001
<b>Descripción</b>	Armario de archivos para Departamento de Tecnologías de la Información
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Jefe de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

<b>Nombre</b>	OFL_TI001_001
<b>Descripción</b>	Departamento de Tecnologías de la Información - Instancia física
<b>Categoría</b>	Infraestructura TI
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Desastres naturales. Desastres de origen humano.

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



<b>Nombre</b>	RNG_TI001_001
<b>Descripción</b>	Alarma de Departamento de Tecnologías de la Información
<b>Categoría</b>	Control de entorno
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso - recurso estático
<b>Propietario</b>	Administración del edificio
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
<b>Vulnerabilidades y Amenazas</b>	Quiebre autenticación de llave seguridad.

<b>Nombre</b>	ARC_TI001_001
<b>Descripción</b>	Archivo de Departamento de Tecnologías de la Información - registro de documentos
<b>Categoría</b>	Activos tangibles / Activos intangibles
<b>Ubicación</b>	Departamento de Tecnologías de la Información - primer piso
<b>Propietario</b>	Jefe de Departamento de Tecnologías de la Información
<b>Valoración</b>	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
<b>Vulnerabilidades y Amenazas</b>	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

### 3. Análisis de riesgos

#### 3.1. Riesgos asociados a factores no tecnológicos

<b>Título de Riesgo</b>	Desastres naturales
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, distintas estructuras (departamentos) podrían verse dañadas parcial o totalmente.
<b>Dueño del Activo</b>	
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Departamento de Asuntos Municipales.
<b>Detalle de la Vulnerabilidad</b>	En caso de algun desastre de origen natural (terremoto, tsunami, pandemia), la infraestructura puede sufrir daños por consecuencia directa o transitiva a esta.
<b>Detalle de la amenaza</b>	Dado que Chile está ubicado en una zona potencialmente sísmica, la integridad de los recursos físicos se encuentra en un peligro constante.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Multas por Servicios Básicos (Agua, luz)
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, una multa o una infracción a algún proceso de pago de un servicio puede interrumpirlo
<b>Dueño del Activo</b>	
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Contabilidad gubernamental Procesos de mantención de infraestructura y servicios
<b>Dependencia</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de revisión de procesos de contratación pública
<b>Detalle de la Vulnerabilidad</b>	El no pago de un servicio o incurrir en multas debido a un problema administrativo o burocrático.
<b>Detalle de la amenaza</b>	Una multa o infracción puede generar la suspensión de un servicio básico lo cual puede causar la interrupción de los servicios de la municipalidad.
<b>Respuesta</b>	
<b>Aprobación</b>	

<b>Título de Riesgo</b>	Pérdidas de soporte de proyectos licitados
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, un proyecto externalizado deja de tener soporte opeartivo.
<b>Dueño del Activo</b>	Empresas externas
<b>Proceso</b>	Afecta a todos los procesos terciarizados
<b>Sub Área</b>	Departamento de revisión de procesos de contratación pública Departamento de auditoria operativa Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Departamento de Tecnologías de la Información. Alcalde.
<b>Detalle de la Vulnerabilidad</b>	Los contratos de licitación incluyen contratos de soporte por un periodo relativamente extendido de tiempo. Sin embargo, puede darse el caso que el desarrollo es demasiado caro para seguirlo manteniendo, una nueva licitación fracase o bien la empresa rompa relaciones con la municipalidad.
<b>Detalle de la amenaza</b>	En caso de una pérdida de soporte el equipo interno de TI queda a ciegas respecto a como administrar o normalizar una situación sobre el software licitado. En caso de ser un SaSS, la normativa vigente especifica que la fuente debe estar alojada dentro de un servidor municipal, sin embargo esto no garantiza un soporte efectivo.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Fin de facturaciones
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, los procesos de facturación terminan lo cual puede ser causal para una empresa para bajar la calidad de su soporte
<b>Dueño del Activo</b>	Jefe de Departamento revisión de procesos de pago, bienes y servicios
<b>Proceso</b>	Empresas externas
<b>Sub Área</b>	Departamento de revisión de procesos de contratación pública Departamento de auditoria operativa Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Alcalde. Departamento revisión de procesos de pago, bienes y servicios
<b>Detalle de la Vulnerabilidad</b>	Una baja en la calidad del servicio puede dejar expuestos los sistemas desarrollados por terceros.
<b>Detalle de la amenaza</b>	Dada la indiosincracia del Chileno y de las empresas Chilenas, las relaciones contractuales se vuelven mas distantes una vez se ejecuta el último periodo de facturación. Adicionalmente, esto se puede producir por un atraso. En cualquiera de los dos casos, incluso si por ley esta la empresa licitada obligada a mantener la calidad del servicio, esto podría no ser así ya que no hay fiscalización durante el proceso.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Alcalde.

<b>Título de Riesgo</b>	Desastres lógicos
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, surgen errores lógicos en el componente afectado.
<b>Dueño del Activo</b>	
<b>Proceso</b>	Integridad de datos.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Se define como un desastre lógico a algun error propagado por un determinado motivo el cual es causado por un error humano no premeditado ni predecible el cual implica una pérdida total de la integridad de los datos.
<b>Detalle de la amenaza</b>	Este tipo de errores puede ser causado por un sinfin de procesos, desde un desarrollo defectuoso por terceros, errores de hardware, etc.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Divulgación y copiado de informacion.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, la información confidencial del municipio queda expuesta a terceros.
<b>Dueño del Activo</b>	Alcalde
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Alcalde
<b>Detalle de la Vulnerabilidad</b>	La información propia del municipio puede ser copiada, transportada y/o divulgada por cualquier médio, permitiendo su uso malicioso.
<b>Detalle de la amenaza</b>	Comunmente asociado a pérdida de credenciales o ruptura de autenticación, este riesgo también se puede dar con empresas
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	candados de seguridad.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	No hay candados de seguridad para poder restringir la movilidad del dispositivo
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Seguridad de infraestructura
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Los candados de seguridad permiten anclar dispositivos como notebooks hacia una mesa de manera relativamente segura. Al no tener dichos candados, estos dispositivos son fáciles de sustraer.
<b>Detalle de la amenaza</b>	Al no tener mecanismos para restringir la movilidad de los equipos, estos se vuelven susceptibles a su sustracción de las dependencias por terceras personas, poniendo en riesgo la confidencialidad de los datos.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

### 3.2. Riesgos asociados a procesos municipales

<b>Título de Riesgo</b>	Falta de documentación e implantación de políticas para envío de correos masivos.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	No hay política de envíos masivos de correo.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Departamento de Asuntos Municipales.
<b>Dependencia</b>	Alcalde
<b>Detalle de la Vulnerabilidad</b>	No hay políticas de envío masivo de correos a nivel de servidor, de usuario o de política general. Debido a esto, no es posible regular los correos salientes.
<b>Detalle de la amenaza</b>	Al no existir regulación de los correos salientes, los correos de la municipalidad se vuelven objetivo fácil de phishing. Esto es ya que si no se estandariza el envío de correos (por ejemplo, utilizando una lista), se da a entender que cualquier correo puede ejecutar esta acción, lo cual la vuelve más creíble. De la misma manera, al no haber regulaciones permite que cualquier usuario pueda ejecutar estas acciones las cuales pueden tener consecuencias graves para la credibilidad de la municipalidad.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Alcalde Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Falta de punto de contacto.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	No existe punto de contacto por parte de la municipalidad.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Departamento de Asuntos Municipales.
<b>Dependencia</b>	Alcalde
<b>Detalle de la Vulnerabilidad</b>	No existen índices ni puntos de contacto a la municipalidad para efectos de trámites civiles.
<b>Detalle de la amenaza</b>	Al no existir puntos de contacto, la atención por parte al cliente se ve afectada, saturando a los ejecutivos lo cual lleva a cuellos de botella dentro de la operación normal de la municipalidad.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Roles no definidos.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	No existen roles definidos de usuario.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	No existen roles definidos de usuario respecto a los permisos sobre cada plataforma mas alla de la autenticación interna de cada uno.
<b>Detalle de la amenaza</b>	El no restringir los accesos a nivel de usuario (de la nube interna/hibrida) puede provocar brechas de seguridad debido a la no restriccion de permisos.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Falta de monitoreo.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, los dispositivos afectados pueden desarrollar comportamientos anómalos .
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Administracion de red y plataforma
<b>Sub Área</b>	Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	De no monitorearse servicios o dispositivos no se puede dar atención a una posible explotación (o aparición) fortuita de fallos.
<b>Detalle de la amenaza</b>	Actualmente no existen políticas que determinen una conducta o protocolo de monitoreo de los recursos internos.
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.



<b>Título de Riesgo</b>	Obtención y/o renovación de permisos de circulación sin ingreso o acreditación física y online de datos sobre propietario, placa patente única, seguro obligatorio, revisión técnica y/o multas impagas.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sistema de permisos de circulación ejecuta operaciones sin necesidad inmediata ni forzada de ingresar datos.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Registro comunal de permisos de circulación
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Registro comunal de permisos de circulación
<b>Dependencia</b>	Empresa Externa 3
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido aun fallo interno del sistema externalizado de permisos de circulación, emite decretos de pago inválidos o con información errónea.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Obtención y/o renovación de permisos de circulación sin ingreso o acreditación física y online de datos sobre propietario, placa patente única, seguro obligatorio, revisión técnica y/o multas impagas.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sistema de permisos de circulación ejecuta operaciones sin necesidad inmediata ni forzada de ingresar datos.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Registro comunal de permisos de circulación
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Registro comunal de permisos de circulación
<b>Dependencia</b>	Empresa Externa 3
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido aun fallo interno del sistema externalizado de permisos de circulación, emite decretos de pago inválidos o con información errónea.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Obtención y/o renovación de patentes municipales sin ingreso y/o acreditación de datos del contribuyente, propiedad, sucursales y datos del servicio de impuestos internos.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sistema de patentes comerciales ejecuta operaciones sin necesidad inmediata ni forzada de ingresar datos.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Patentes municipales
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Patentes municipales
<b>Dependencia</b>	Empresa Externa 2
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido aun fallo interno del sistema externalizado de patentes municipales, emite decretos de pago inválidos o con información errónea.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Emisión de decretos de pago sin registrar datos y/o sin comprobantes.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sistema de tesorería municipal o el sistema externalizado de contabilidad gubernamental pueden emitir decretos sin requerir la información.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Contabilidad gubernamental
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de revisión de procesos de contratación pública
<b>Dependencia</b>	Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido aun fallo interno del sistema externalizado de contabilidad gubernamental, emite decretos de pago inválidos o con información errónea.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Decretos de pago imputados a cuentas presupuestarias que no corresponden.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sistema de tesorería municipal puede emitir cheques a terceros con cargo a la municipalidad.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Contabilidad gubernamental
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de revisión de procesos de contratación pública
<b>Dependencia</b>	Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido aun fallo interno del sistema externalizado de contabilidad gubernamental, emite decretos de pago inválidos o con información errónea.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Emisión de cheque individual sin consultar datos en sistema de contabilidad gubernamental.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el sistema de contabilidad gubernamental puede emitir cheques a terceros con cargo a la municipalidad.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Contabilidad gubernamental
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios
<b>Dependencia</b>	Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido aun fallo interno del sistema externalizado de contabilidad gubernamental, este pueda ser utilizado para la extracción de fondos de manera ilícita.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Recepción de pagos con cálculos de intereses y multas fuera de período
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, es posible ingresar un pago con cálculos erróneos en el sistema, los cuales se ven reflejados posteriormente en el sistema interno de contabilidad.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Sistemas computacionales por internet y sistemas sociales Administración de sistemas de egresos, recursos humanos y remuneraciones Contabilidad gubernamental Trámites de oficina de partes Patentes municipales
<b>Sub Área</b>	Departamento de Asuntos Municipales. Departamento de revisión de procesos de contratación pública Departamento de revisión de procesos de pago, bienes y servicios
<b>Dependencia</b>	Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Es posible que debido a un fallo interno del sistema externalizado para pagos de la tesorería municipal puedan ejecutarse pagos sin respetar los cálculos establecidos para la contabilidad de multas y demases.
<b>Detalle de la amenaza</b>	Al estar externalizado el servicio, no hay control sobre el funcionamiento interno de esta plataforma, en especial considerando su estatus de plataforma legada.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

### 3.3. Riesgos asociados a control del personal

<b>Título de Riesgo</b>	Quiebre autenticación de tarjeta magnética
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, las llaves magnéticas que utilizadas como barrera para personal no autorizado quedan sin efecto.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Seguridad de infraestructura
<b>Sub Área</b>	Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	De ser quebrada la autenticación de las tarjetas magnéticas utilizadas para acceder a las salas de servidores, la integridad completa de los dispositivos queda comprometida.
<b>Detalle de la amenaza</b>	Este tipo de amenazas se presenta principalmente por un factor físico dada la dificultad de intervenir las cerraduras magnéticas. Copias de las tarjetas, duplicaciones, generaciones de maestros son algunas de las amenazas posibles las cuales pueden ser ejecutadas si existe una brecha de información respecto a la infraestructura de las cerraduras, la pérdida de una tarjeta o el robo de esta.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Copia de llaves
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, las llaves físicas que utilizadas como barrera para personal no autorizado quedan sin efecto.
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Seguridad de infraestructura Seguridad del personal
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Alcalde
<b>Detalle de la Vulnerabilidad</b>	Al efectuarse una copia física de las llaves, la seguridad que estas proveen queda inutilizable. Por tanto ya no es posible contar con la seguridad de control de personal que estas ofrecen.
<b>Detalle de la amenaza</b>	El acceso físico no es solo relevante por el compromiso de infraestructura que este pueda poseer, si no por la rapidez con la que esta puede generar problemas alternos (como la propagación de la misma copia) y a su vez deja en peligro al personal ya que seguridad no puede desempeñar correctamente sus funciones.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Quiebre autenticación de llave de seguridad
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, la información de autenticación queda comprometida a terceras partes
<b>Dueño del Activo</b>	Miguel Jorquera
<b>Proceso</b>	Integridad de datos.
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Alcalde
<b>Detalle de la Vulnerabilidad</b>	El compromiso de autenticación de un usuario compromete en su totalidad todos los niveles de seguridad permitidos, poniendo en riesgo la confidencialidad, integridad y disponibilidad de información y servicios.
<b>Detalle de la amenaza</b>	Puede ocurrir al dejar contraseñas escritas en medios físicos como post-it, almacenadas dentro de archivos planos en unidades extraíbles o en equipos personales, etc.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

### 3.4. Riesgos asociados de índole técnica

<b>Título de Riesgo</b>	No interoperabilidad con estándar de norma técnica para los Órganos de la Administración del Estado.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, los datos son corrompidos debido a un mal diseño de alguna estructura de datos subyacente a la aplicación.
<b>Dueño del Activo</b>	Empresa Externa 1 Empresa Externa 2 Empresa Externa 3
<b>Proceso</b>	Registro comunal de permisos de circulación Contabilidad gubernamental Patentes municipales
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de auditoria operativa Departamento de revisión de procesos de contratación pública
<b>Dependencia</b>	Empresa Externa 1 Empresa Externa 2 Empresa Externa 3
<b>Detalle de la Vulnerabilidad</b>	Un manejo deficiente de las estructuras de datos involucradas en el desarrollo de las aplicaciones o de las bases de datos puede llevar a corrupcion de los datos debido a múltiples factores.
<b>Detalle de la amenaza</b>	Actualmente la municipalidad externaliza gran parte de los servicios informaticos como tambien la mantención de muchos de sus equipos. Debido a esto, en caso de que uno de los proveedores entregue un servicio desarrollado de manera deficiente, resulta en un incremento de la probabilidad de un evento de perdida de datos.
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.



<b>Título de Riesgo</b>	No interoperabilidad con estándar de norma técnica para los Órganos de la Administración del Estado.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, los datos son corrompidos debido a un mal diseño de alguna estructura de datos subyacente a la aplicación.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Un manejo deficiente de las estructuras de datos involucradas en el desarrollo de las aplicaciones o de las bases de datos puede llevar a corrupción de los datos debido a múltiples factores.
<b>Detalle de la amenaza</b>	Actualmente la municipalidad externaliza gran parte de los servicios informáticos como también la mantención de muchos de sus equipos. Debido a esto, en caso de que uno de los proveedores entregue un servicio desarrollado de manera deficiente, resulta en un incremento de la probabilidad de un evento de pérdida de datos .
<b>Respuesta</b>	CORREGIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Integridad de información por estructura de datos.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, los datos son corrompidos debido a un mal diseño de alguna estructura de datos subyacente a la aplicación.
<b>Dueño del Activo</b>	Empresa Externa 1 Empresa Externa 2 Empresa Externa 3
<b>Proceso</b>	Registro comunal de permisos de circulación Contabilidad gubernamental
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de Asuntos Municipales. Departamento de auditoria operativa Departamento de revisión de procesos de contratación pública
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Un manejo deficiente de las estructuras de datos involucradas en el desarrollo de las aplicaciones o de las bases de datos puede llevar a corrupcion de los datos debido a múltiples factores.
<b>Detalle de la amenaza</b>	Actualmente la municipalidad externaliza gran parte de los servicios informaticos como tambien la mantención de muchos de sus equipos. Debido a esto, en caso de que uno de los proveedores entregue un servicio desarrollado de manera deficiente, resulta en un incremento de la probabilidad de un evento de perdida de datos .
<b>Respuesta</b>	COMPENSAR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

<b>Título de Riesgo</b>	Dependencia de licencias.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, la carencia de una licencia podría limitar la disponibilidad de un servicio que dependa de esta.
<b>Dueño del Activo</b>	Dominio General
<b>Proceso</b>	Afecta a todos los procesos en general
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Detalle de la Vulnerabilidad</b>	Para el caso de software que opera con licencias (Office 365 por ejemplo), la no disponibilidad de las mismas puede ocasionar problemas al momento de utilizar otros servicios
<b>Detalle de la amenaza</b>	Actualmente debido al convenio con Microsoft vigente por parte del gobierno actual, muchos softwares están a merced de que estas licencias estén disponibles. Sin embargo, la no caducidad no tiene relación alguna con las licencias asignadas, ya que dependiendo del tier involucrado en las licencias asignadas, son los servicios disponibles.
<b>Respuesta</b>	PREVENIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información. , Jefe de Departamento revisión de procesos de pago, bienes y servicios , Jefe de Departamento de revisión de procesos de contratación pública

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

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

<b>Título de Riesgo</b>	Falta de encriptado.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, es posible leer la información directamente desde el medio en que se encuentra sin ninguna barrera de seguridad
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información. , Empresa Externa 1
<b>Proceso</b>	Resguardo de información personal. Resguardo de información institucional. Contabilidad gubernamental Administración municipal
<b>Sub Área</b>	Todas.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Una auditoría realizada por contraloría reveló que no existe encriptación de los datos almacenados digitalmente salvo en la capa de transporte.
<b>Detalle de la amenaza</b>	La falta de encriptación puede producir fuga de información sensible.
<b>Respuesta</b>	CORREGIR TRANSFERIR si es externalizado
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Residuos de información.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, información que haya sido borrada sigue disponible dentro de una base de datos sin ser detectada
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Contabilidad gubernamental Administración municipal
<b>Sub Área</b>	Departamento revisión de procesos de pago, bienes y servicios Departamento de revisión de procesos de contratación pública Departamento de Asuntos Municipales.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Una auditoría realizada por contraloría reveló que no existen protocolos de eliminación de la información de manera interna y esta tampoco forma parte de los servicios contratados.
<b>Detalle de la amenaza</b>	Al no existir un protocolo de eliminación de información claro, es altamente probable que la información no pueda ser eliminada de manera efectiva ya sea de plataformas, dispositivos, medios extraíbles, etc. Este problema aplica también a los archivos físicos que no cuenten con respaldo y que dentro de las operaciones vigentes consideren su eliminación.
<b>Respuesta</b>	MITIGAR TRANSFERIR si es externalizado
<b>Aprobación</b>	Alcalde

<b>Título de Riesgo</b>	Mantenimiento preventivo externalizado ejecutado deficientemente.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	12/06/2020
<b>Descripción</b>	Al materializarse este riesgo, las plataformas sujetas a manteniendo por parte de una empresa externa podrían quedar expuestas a vulnerabilidades
<b>Dueño del Activo</b>	Empresas externas
<b>Proceso</b>	Resguardo de información personal. Resguardo de información institucional. Fiabilidad de plataforma
<b>Sub Área</b>	Departamento de Asuntos Municipales. Departamento revisión de procesos de pago, bienes y servicios Departamento de auditoria operativa
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. , Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Mantenciones negligentes, omitidas, incompletas.
<b>Detalle de la amenaza</b>	Una mantención negligente de las plataformas puede llevar a un uso malicioso de estas, las cuales pueden perjudicar enormemente el servicio entregado por la municipalidad como también poner en riesgo los datos disponibles en esta. Actualmente debido a la normativa actual, todas las aplicaciones están alojadas en servidores de la municipalidad, sin embargo, no implica que el código esté necesariamente abierto o que el personal propio del departamento de tecnologías pueda tener el conocimiento suficiente sobre este para tomar control completo.
<b>Respuesta</b>	TRANSFERIR
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.



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

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

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

<b>Título de Riesgo</b>	Ejecución de malware por falta de software AV.
<b>Autor</b>	Erik Regla
<b>Fecha de Levantamiento</b>	11/06/2020
<b>Descripción</b>	Al materializarse este riesgo, el servidor principal de la municipalidad queda comprometido.
<b>Dueño del Activo</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Proceso</b>	Contabilidad gubernamental Administración de red y plataforma
<b>Sub Área</b>	Jefe de Departamento de Tecnologías de la Información.
<b>Dependencia</b>	Jefe de Departamento de Tecnologías de la Información. Empresa Externa 1
<b>Detalle de la Vulnerabilidad</b>	Ataques por ransomware, gusanos, trojanos, etc.
<b>Detalle de la amenaza</b>	Debido al alto número de vulnerabilidades presentes en el sistema operativo, es posible que la materialización de un riesgo en un equipo de una red adyacente pueda propagar procesos de terceros y estos comprometan el servidor principal.
<b>Respuesta</b>	CORREGIR TRANSFERIR si es externalizado
<b>Aprobación</b>	Jefe de Departamento de Tecnologías de la Información.

### 3.5. Riesgos generales asociados a ingeniería social

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

## 4. Matriz de riesgos

La matriz de riesgos está agregada adjunta al proyecto.

## 5. Políticas de seguridad

### 5.1. Objetivos de la política

Esta política está diseñada para ayudar al proceso de estandarización y saneamiento de los problemas detectados durante la realización de este informe. Se espera que estas políticas sean leídas por el personal administrativo y general para informarse de los requisitos obligatorios para proteger la información del municipio.

Estas políticas están disponibles en nuestro sitio web oficial de la municipalidad como también son entregadas como documento adjunto al contrato de trabajo y debe ser entregada una copia firmada para notificar la lectura y aceptación de estas políticas.

## **5.2. Declaración de autoridad y alcance**

Esta política es diseñada por parte del Departamento de Tecnologías de la Información del municipio para velar por la seguridad de TI desde un punto de vista general. Se espera que esta política establezca un lineamiento base respecto al uso de recursos y dispositivos a lo largo de la organización con tal de reducir el impacto de las vulnerabilidades de origen humano.

Dentro de esta política no se especificarán aspectos detallados sobre las contrataciones, mecanismos de licitación, mecanismos de auditoria ni ningún otro aspecto administrativo salvo el uso correcto de bienes y servicios por parte de los funcionarios, sin embargo, esta política base no excluye del efecto de otras políticas vigentes dentro de cada departamento, oficina y secretaria.

## **5.3. Política de uso aceptable**

- El usuario tiene prohibido extraer información de su dispositivo personal a otro medio físico.
- El usuario no puede utilizar aplicaciones externas o fuera del ecosistema utilizado por la organización.
- No esta permitido realizar cambios al sistema operativo, hardware o estructura interna del dispositivo institucional entregado .

## **5.4. Política de identificación y autenticación**

- Para poder ingresar a sus dispositivos será necesaria la utilización de una contraseña segura, alfanumérica con al menos un caracter especial de un largo no menor a 10 caracteres, como también debera utilizar en conjunto autenticación de doble factor biométrico.
- Todos los dispositivos no deben presentar medios para poder establecer cambios al sistema operativo ni a su entorno.
- Todos los dispositivos deben contar con encendido automático cada cierto número de horas.

## **5.5. Política de acceso a internet**

- Todas las conexiones hacia los recursos de la empresa deben ser realizadas por medio de una VPN y por medio de conexión cableada mediante Ethernet.
- No está permitido el uso de redes inalámbricas, salvo la institucional, la cual para su uso se requiere un certificado el cual es provisto por el departamento de tecnologías de la información.
- No está permitido el acceso a sitios no autorizados u de ocio por medio de la red institucional.

## **5.6. Política de acceso**

- Para poder iniciar sesión en los recursos en línea de la empresa es necesario proveer de la contraseña de la cuenta corporativa y una verificación de dos pasos por medio de Office365 S2-E5.
- Las conexiones a recursos de la empresa solo pueden ser ejecutadas por medio de las aplicaciones stand-alone correspondientes.
- Todos los accesos a equipos corporativos deben hacerse por medio de Active Directory.

## **5.7. Política de acceso remoto**

- El acceso remoto solo está permitido por medio de el uso conjunto de una VPN y la red institucional.
- Las conexiones a recursos de la empresa solo pueden ser ejecutadas por medio de las aplicaciones stand-alone correspondientes.
- En caso de situaciones de fuerza mayor, las restricciones anteriores pueden ser levantadas y/o controladas.

## **5.8. Políticas del manejo de incidentes**

En caso de robo o pérdida del equipo:

- Se debe dar anuncio inmediato a el Departamento de Tecnologías de la Información para iniciar el procedimiento de traza y de ser necesario de borrado de información.
- El Departamento de Tecnologías de la Información debe dar anuncio inmediato del evento a las autoridades pertinentes e iniciar los trámites necesarios para la obtención del equipo. El individuo afectado también deberá concurrir junto con el Departamento de Tecnologías de la Información para tales efectos.
- La gerencia deberá gestionar la entrega de un nuevo dispositivo en un plazo no mayor a 5 días hábiles e iniciará un procedimiento de eliminación e inhabilitación remota por medio del encendido automático.

En caso de mal uso:

- En caso de detectarse mal uso el Departamento de Tecnologías de la Información deberá emitir una carta de amonestación a la persona, la cual deberá acusar su recibo con su jefe directo. Esta carta solo será entregada como máximo tres veces, luego de esto será considerado una violación al código de seguridad de la empresa.
- En caso de reiteradas violaciones al código de conducta, el caso será derivado a la gerencia de recursos humanos para sus respectivas medidas o sanciones que estimen pertinentes.

En caso de ser víctima de un ataque informático u sospecha del mismo:

- La persona afectada deberá dar cuenta al Departamento de Tecnologías de la Información de sus actividades y sospechas para que este pueda investigar en el problema.
- Se deberá hacer un security assesment para poder identificar los posibles afectados y comenzar con mitigaciones.
- De ser necesario afectado deberá hacer entrega de sus equipos digitales para ser examinados por el Departamento de Tecnologías de la Información y esclarecer el origen del problema y sus mitigaciones.
- El Departamento de Tecnologías de la Información deberá pasado el proceso de examen entregar los equipos limpios a su usuario para que este pueda retomar sus funciones.
- El incidente deberá ser archivado dentro de los registros del Departamento de Tecnologías de la Información. Dependiendo de la gravedad del incidente, este reporte puede ser elevado a otras unidades de la organización o bien a entes gubernamentales en acuerdo a la ley de protección de datos vigente actualmente en el país.

**Parte IV**

## **Conclusiones**



**Parte V**

# **Bibliografía**

**Referencias**