Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Proyecto 1

Erik Regla
eregla09@alumnos.utalca.cl

16 de junio de 2020

1. Introducción

2. Estructura organizacional

2.1. Organigrama

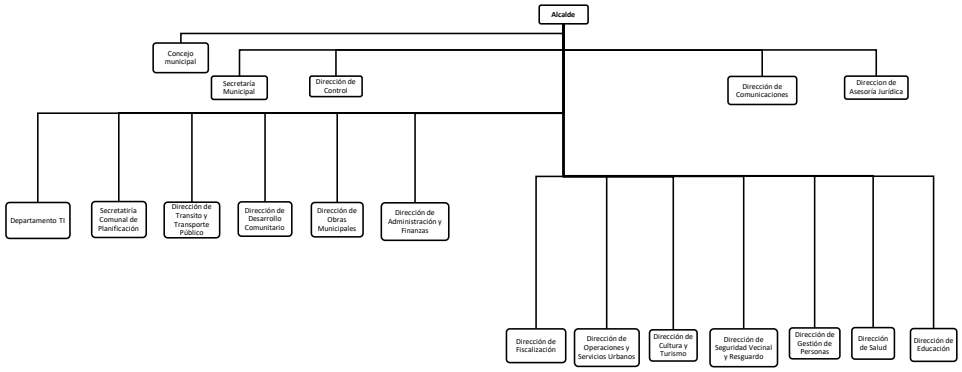

Figura 1: Organigrama

2.2. Rationale

El alcance de este trabajo abarca solo las siguientes divisiones:

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

    - Sección resolutiva
    - Sección administrativa
- **Departamento de certificación y archivo**. Perteneciente a la secretaría municipal. Este se compone de las siguientes oficinas:
    - Oficina de registro municipal de transferencias
    - Oficina de control de archivo y representación.
- **Departamento de asuntos concejo cosoc y otros**. Perteneciente a la secretaría municipal. Este se compone de las siguientes secciones:
    - Sección cosoc
    - Sección consejo municipal
- **Departamento de revisión de procesos de contratación pública**. Perteneciente a la dirección de control.
- **Departamento de auditoría operativa**. Perteneciente a la dirección de control.
- **Departamento Revisión de procesos de pago, bienes y servicios**. Perteneciente a la dirección de control.

Se establece para cada departamento la siguiente estructura base:

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

Se establece para cada oficina la siguiente estructura base:

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

Se establece para cada secretaría la siguiente estructura base:

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

3. Identificación de activos

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

3.1. Activos de carácter transversal

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

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

[1]https://www.cvedetails.com/cve/CVE-2013-1241/

Nombre	RTR_SECUN_001
Descripción	Router secundario Cisco 2901, utilizado de punto intermedio hacia la red interna
Categoría	Hardware TI
Ubicación	Sala de servidores - primer piso
Propietario	Departamento de TI
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[2]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	SWI_NODES_001
Descripción	Switch general Cisco Catalyst 2960, para nodo base del arbol de conectividad
Categoría	Hardware TI
Ubicación	Sala de servidores - primer piso
Propietario	Departamento de TI
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[3]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[2]https://www.cvedetails.com/cve/CVE-2017-3881/
[3]https://www.cvedetails.com/cve/CVE-2017-3881/

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

Nombre	OSS_WINDO_001
Descripción	Windows Server 2019 Datacenter Edition
Categoría	Sistemas Operativos
Ubicación	SRV_SHARE_001
Propietario	Departamento de TI
Valoración	Confidencialidad: 2 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Mas de 390 vulnerabilidades detectadas[4] Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

[4]https://www.cvedetails.com/product/50662/Microsoft-Windows-Server-2019.html?vendor_id=26

Nombre	EXE_EXCHA_001
Descripción	Módulo servidor para Microsoft Exchange 2016, para uso de correos corporativos de los funcionarios de la municipalidad.
Categoría	Software
Ubicación	SRV_SHARE_001
Propietario	Departamento de TI
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2018-8374[5]Tampering Vulnerability existente al momento de un fallo en la información de los perfiles. CVE-2018-8302[6]Ejecución de código remota debido al fallo de manipulación de objetos en memoria, resultante en control total. CVE-2018-8159[7] XSS resultante en elevación de privilegios por medio de requests web . CVE-2018-8154[8]Ejecución de código remota debido a la corrupción del manejo de objetos en memoria, resultante en control total. CVE-2018-8153[9] Spoofing . CVE-2018-8152[10] Elevación de privilegios . CVE-2018-8151[11] Corrupción de memoria . Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Posee información de alto interés para un grupo específico.

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

[5]https://www.cvedetails.com/cve/CVE-2018-8374/
[6]https://www.cvedetails.com/cve/CVE-2018-8302/
[7]https://www.cvedetails.com/cve/CVE-2018-8159/
[8]https://www.cvedetails.com/cve/CVE-2018-8154/
[9]https://www.cvedetails.com/cve/CVE-2018-8153/
[10]https://www.cvedetails.com/cve/CVE-2018-8152/
[11]https://www.cvedetails.com/cve/CVE-2018-8151/

Nombre	EXE_WPRES_001
Descripción	Servidor Wordpress 5.1 Beta3 para página institucional
Categoría	Software
Ubicación	SRV_SHARE_001
Propietario	Departamento de TI
Valoración	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2019-9787[12]Ejecución remota de código por medio de CRSRF. CVE-2019-16220[13]Sanitización de wp_validate manipula redirects. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	EXE_MYSQL_001
Descripción	Servidor MySQL 6.0.9 Beta3 para EXE_WPRES_001
Categoría	Software
Ubicación	SRV_SHARE_001
Propietario	Departamento de TI
Valoración	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2009-0819[14]Denegación de servicio. CVE-2008-7247[15]Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

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

[12]https://www.cvedetails.com/cve/CVE-2019-9787/
[13]https://www.cvedetails.com/cve/CVE-2019-16220/
[14]https://www.cvedetails.com/cve/CVE-2009-0819/
[15]https://www.cvedetails.com/cve/CVE-2008-7247/

Nombre	EXE_PHPSR_001
Descripción	Servidor PHP 7.3.6 para EXE_WPRES_001
Categoría	Software
Ubicación	SRV_SHARE_001
Propietario	Departamento de TI
Valoración	Confidencialidad: 1 Integridad: 3 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2019-11042[16]Buffer overflow causado por información EXIF. CVE-2008-7247[17]Buffer overflow causado por información EXIF. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

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

Nombre	EXE_MYSQL_002
Descripción	Servidor MySQL 6.0.9 Beta3 para EXE_ADMIN_002
Categoría	Software
Ubicación	SRV_SHARE_002
Propietario	Departamento de TI
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	CVE-2009-0819[18]Denegación de servicio. CVE-2008-7247[19]Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

[16]https://www.cvedetails.com/cve/CVE-2019-11042/
[17]https://www.cvedetails.com/cve/CVE-2008-7247/
[18]https://www.cvedetails.com/cve/CVE-2009-0819/
[19]https://www.cvedetails.com/cve/CVE-2008-7247/

Nombre	EXE_SQLTB_002
Descripción	Base de datos MySQL en EXE_MYSQL_002para EXE_ADMIN_002
Categoría	Software
Ubicación	SRV_SHARE_002
Propietario	Departamento de TI
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Está sujeta a vulnerabilidades de manera transitiva. Posee información de alto interés para un grupo específico.

Nombre	EXE_PHPSR_002
Descripción	Servidor PHP 7.3.6 para EXE_ADMIN_002
Categoría	Software
Ubicación	SRV_SHARE_002
Propietario	Departamento de TI
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	CVE-2019-11042[20]Buffer overflow causado por información EXIF. CVE-2008-7247[21]Buffer overflow causado por información EXIF. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

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

[20] https://www.cvedetails.com/cve/CVE-2019-11042/
[21] https://www.cvedetails.com/cve/CVE-2008-7247/

Nombre	EXE_MYSQL_003
Descripción	Servidor MySQL 6.0.9 Beta3 para EXE_ADMIN_003
Categoría	Software
Ubicación	SRV_SHARE_003
Propietario	Departamento de TI
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	CVE-2009-0819[22]Denegación de servicio. CVE-2008-7247[23]Bypass de restricciones RBAC. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

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

Nombre	EXE_PHPSR_003
Descripción	Servidor PHP 7.3.6 para EXE_ADMIN_003
Categoría	Software
Ubicación	SRV_SHARE_003
Propietario	Departamento de TI
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	CVE-2019-11042[24]Buffer overflow causado por información EXIF. CVE-2008-7247[25]Buffer overflow causado por información EXIF. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

[22]https://www.cvedetails.com/cve/CVE-2009-0819/
[23]https://www.cvedetails.com/cve/CVE-2008-7247/
[24]https://www.cvedetails.com/cve/CVE-2019-11042/
[25]https://www.cvedetails.com/cve/CVE-2008-7247/

3.2. 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.

3.2.1. Oficina de Partes Alcaldía

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

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

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

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

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

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

Nombre	NAS_OF001_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Partes Alcaldía
Categoría	Hardware TI
Ubicación	Oficina de Partes Alcaldía - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[26]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[26]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_OF001_001
Descripción	Oficina de Partes Alcaldía - Instancia física
Categoría	Infraestructura TI
Ubicación	Oficina de Partes Alcaldía - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.2. Oficina de Registro Municipal de Transferencias

Nombre	NTB_OF002_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
Propietario	Jefe de Oficina de Registro Municipal de Transferencias
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_OF002_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
Propietario	Secretario de Oficina de Registro Municipal de Transferencias
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

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

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

Nombre	NAS_OF002_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Registro Municipal de Transferencias
Categoría	Hardware TI
Ubicación	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[27]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[27]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_OF002_001
Descripción	Oficina de Registro Municipal de Transferencias - Instancia física
Categoría	Infraestructura TI
Ubicación	Oficina de Registro Municipal de Transferencias - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.3. Oficina de Control de Archivo y reorsentación

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

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

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

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

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

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

Nombre	NAS_OF003_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Oficina de Control de Archivo y reorsentación
Categoría	Hardware TI
Ubicación	Oficina de Control de Archivo y reorsentación - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de certificación y archivo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[28]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[28]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_OF003_001
Descripción	Oficina de Control de Archivo y reorsentación - Instancia física
Categoría	Infraestructura TI
Ubicación	Oficina de Control de Archivo y reorsentación - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.4. Sección Resolutiva

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

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

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

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

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

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

Nombre	NAS_SE001_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Sección Resolutiva
Categoría	Hardware TI
Ubicación	Sección Resolutiva - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[29]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[29]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_SE001_001
Descripción	Sección Resolutiva - Instancia física
Categoría	Infraestructura TI
Ubicación	Sección Resolutiva - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.5. Sección Administrativa

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

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

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

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

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

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

Nombre	NAS_SE002_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Sección Administrativa
Categoría	Hardware TI
Ubicación	Sección Administrativa - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[30]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[30]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_SE002_001
Descripción	Sección Administrativa - Instancia física
Categoría	Infraestructura TI
Ubicación	Sección Administrativa - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.6. Departamento de Asuntos Municipales

Nombre	SWI_DP001_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Asuntos Municipales - primer piso
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[31]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

[31]https://www.cvedetails.com/cve/CVE-2017-3881/

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

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

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

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

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

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

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

Nombre	NAS_DP001_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Asuntos Municipales
Categoría	Hardware TI
Ubicación	Departamento de Asuntos Municipales - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[32]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[32]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_DP001_001
Descripción	Departamento de Asuntos Municipales - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Asuntos Municipales - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.7. Departamento de Certificación y archivo

Nombre	SWI_DP002_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Certificación y Archivo - segundo piso
Propietario	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[33]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

[33]https://www.cvedetails.com/cve/CVE-2017-3881/

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

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

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

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

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

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

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

Nombre	NAS_DP002_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Certificación y Archivo
Categoría	Hardware TI
Ubicación	Departamento de Certificación y Archivo - segundo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Certificación y Archivo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[34]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

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

[34]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	OFI_DP002_001
Descripción	Departamento de Certificación y Archivo - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Certificación y Archivo - segundo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.8. Departamento de Asuntos Concejo Cosoc y

Nombre	SWI_DP003_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Concejo Cosoc y Otros.
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[35]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

[35]https://www.cvedetails.com/cve/CVE-2017-3881/

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

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

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

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

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

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

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

Nombre	NAS_DP003_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Asuntos Concejo Cosoc y Otros.
Categoría	Hardware TI
Ubicación	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Asuntos Concejo Cosoc y Otros.
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[36]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[36]https://www.cvedetails.com/cve/CVE-2017-7494/

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

Nombre	OFI_DP003_001
Descripción	Departamento de Asuntos Concejo Cosoc y Otros. - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.9. Departamento de Revisión de Procesos de Contratación

Nombre	SWI_DP004_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso
Propietario	Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[37]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[37]https://www.cvedetails.com/cve/CVE-2017-3881/

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

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

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

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

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

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

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

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

Nombre	NAS_DP004_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Revisión de Procesos de Contratación Pública
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[38]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[38]https://www.cvedetails.com/cve/CVE-2017-7494/

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

Nombre	OFI_DP004_001
Descripción	Departamento de Revisión de Procesos de Contratación Pública - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Revisión de Procesos de Contratación Pública - cuarto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.10. Departamento de Auditoría Operativa

Nombre	SWI_DP005_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Auditoría Operativa - quinto piso
Propietario	Departamento de TI - Encargado TI de Departamento de Auditoría Operativa
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[39]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[39]https://www.cvedetails.com/cve/CVE-2017-3881/

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

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

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

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

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

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

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

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

Nombre	NAS_DP005_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Auditoría Operativa
Categoría	Hardware TI
Ubicación	Departamento de Auditoría Operativa - quinto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Auditoría Operativa
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[40]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[40]https://www.cvedetails.com/cve/CVE-2017-7494/

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

Nombre	OFI_DP005_001
Descripción	Departamento de Auditoría Operativa - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Auditoría Operativa - quinto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.11. Dirección de Desarrollo Comunitario

Nombre	SWI_PP001_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Desarrollo Comunitario - sexto piso
Propietario	Departamento de TI - Encargado TI de Dirección de Desarrollo Comunitario
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[41]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[41] https://www.cvedetails.com/cve/CVE-2017-3881/

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

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

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

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

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

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

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

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

Nombre	NAS_PP001_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Desarrollo Comunitario
Categoría	Hardware TI
Ubicación	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Desarrollo Comunitario
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[42]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[42]https://www.cvedetails.com/cve/CVE-2017-7494/

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

Nombre	OFI_PP001_001
Descripción	Dirección de Desarrollo Comunitario - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Desarrollo Comunitario - sexto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

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

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

3.2.12. Dirección de Obras Municpales

Nombre	SWI_PP002_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Obras Municpales - séptimo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Obras Municpales
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[43]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[43]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP002_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Jefe de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP002_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Secretario de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP002_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Ejecutivo de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP002_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Encargado de TI de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP002_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP002_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP002_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP002_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP002_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Obras Municpales
Categoría	Hardware TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Obras Municpales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[44]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[44]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP002_001
Descripción	Armario de archivos para Dirección de Obras Municpales
Categoría	Infraestructura TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Jefe de Dirección de Obras Municpales
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP002_001
Descripción	Dirección de Obras Municpales - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP002_001
Descripción	Alarma de Dirección de Obras Municpales
Categoría	Control de entorno
Ubicación	Dirección de Obras Municpales - séptimo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP002_001
Descripción	Archivo de Dirección de Obras Municpales - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Obras Municpales - séptimo piso
Propietario	Jefe de Dirección de Obras Municpales
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.13. Dirección de Tránsito y Transporte Público

Nombre	SWI_PP003_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[45]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[45]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP003_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Jefe de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP003_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Secretario de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP003_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Ejecutivo de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP003_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Encargado de TI de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP003_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP003_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP003_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP003_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP003_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Tránsito y Transporte Público
Categoría	Hardware TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[46]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[46]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP003_001
Descripción	Armario de archivos para Dirección de Tránsito y Transporte Público
Categoría	Infraestructura TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Jefe de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP003_001
Descripción	Dirección de Tránsito y Transporte Público - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP003_001
Descripción	Alarma de Dirección de Tránsito y Transporte Público
Categoría	Control de entorno
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP003_001
Descripción	Archivo de Dirección de Tránsito y Transporte Público - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Tránsito y Transporte Público - octavo piso
Propietario	Jefe de Dirección de Tránsito y Transporte Público
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.14. Dirección de Administración y Finanzas

Nombre	SWI_PP004_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Administración y Finanzas - noveno piso
Propietario	Departamento de TI - Encargado TI de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[47]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[47]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP004_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Jefe de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP004_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Secretario de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP004_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Ejecutivo de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP004_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Encargado de TI de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP004_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP004_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP004_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP004_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP004_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Administración y Finanzas
Categoría	Hardware TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[48]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[48]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP004_001
Descripción	Armario de archivos para Dirección de Administración y Finanzas
Categoría	Infraestructura TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Jefe de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP004_001
Descripción	Dirección de Administración y Finanzas - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP004_001
Descripción	Alarma de Dirección de Administración y Finanzas
Categoría	Control de entorno
Ubicación	Dirección de Administración y Finanzas - noveno piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP004_001
Descripción	Archivo de Dirección de Administración y Finanzas - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Administración y Finanzas - noveno piso
Propietario	Jefe de Dirección de Administración y Finanzas
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.15. Dirección de Fiscalización

Nombre	SWI_PP005_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Fiscalización - décimo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Fiscalización
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[49]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[49]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP005_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Jefe de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP005_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Secretario de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP005_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Ejecutivo de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP005_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Encargado de TI de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP005_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP005_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP005_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP005_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP005_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Fiscalización
Categoría	Hardware TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Fiscalización
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[50]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[50]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP005_001
Descripción	Armario de archivos para Dirección de Fiscalización
Categoría	Infraestructura TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Jefe de Dirección de Fiscalización
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP005_001
Descripción	Dirección de Fiscalización - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP005_001
Descripción	Alarma de Dirección de Fiscalización
Categoría	Control de entorno
Ubicación	Dirección de Fiscalización - décimo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP005_001
Descripción	Archivo de Dirección de Fiscalización - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Fiscalización - décimo piso
Propietario	Jefe de Dirección de Fiscalización
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.16. Dirección de Operaciones y Servicios Urbanos

Nombre	SWI_PP006_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[51]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[51]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP006_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Jefe de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP006_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Secretario de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP006_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Ejecutivo de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP006_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Encargado de TI de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP006_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP006_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP006_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP006_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP006_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Operaciones y Servicios Urbanos
Categoría	Hardware TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[52]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	CAB_PP006_001
Descripción	Armario de archivos para Dirección de Operaciones y Servicios Urbanos
Categoría	Infraestructura TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Jefe de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP006_001
Descripción	Dirección de Operaciones y Servicios Urbanos - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[52]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	RNG_PP006_001
Descripción	Alarma de Dirección de Operaciones y Servicios Urbanos
Categoría	Control de entorno
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP006_001
Descripción	Archivo de Dirección de Operaciones y Servicios Urbanos - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Operaciones y Servicios Urbanos - onceavo piso
Propietario	Jefe de Dirección de Operaciones y Servicios Urbanos
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.17. Dirección de Cultura y Turismo

Nombre	SWI_PP007_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[53]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[53]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP007_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Jefe de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP007_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Secretario de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP007_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Ejecutivo de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP007_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Encargado de TI de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP007_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP007_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP007_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP007_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP007_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Cultura y Turismo
Categoría	Hardware TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[54]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[54]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP007_001
Descripción	Armario de archivos para Dirección de Cultura y Turismo
Categoría	Infraestructura TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Jefe de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP007_001
Descripción	Dirección de Cultura y Turismo - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP007_001
Descripción	Alarma de Dirección de Cultura y Turismo
Categoría	Control de entorno
Ubicación	Dirección de Cultura y Turismo - doceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP007_001
Descripción	Archivo de Dirección de Cultura y Turismo - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Cultura y Turismo - doceavo piso
Propietario	Jefe de Dirección de Cultura y Turismo
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.18. Dirección de Seguridad Vecinal y Resguardo

Nombre	SWI_PP008_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[55]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[55]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP008_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Jefe de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP008_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Secretario de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP008_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Ejecutivo de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP008_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Encargado de TI de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP008_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP008_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP008_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP008_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP008_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Seguridad Vecinal y Resguardo
Categoría	Hardware TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[56]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	CAB_PP008_001
Descripción	Armario de archivos para Dirección de Seguridad Vecinal y Resguardo
Categoría	Infraestructura TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Jefe de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP008_001
Descripción	Dirección de Seguridad Vecinal y Resguardo - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[56]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	RNG_PP008_001
Descripción	Alarma de Dirección de Seguridad Vecinal y Resguardo
Categoría	Control de entorno
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP008_001
Descripción	Archivo de Dirección de Seguridad Vecinal y Resguardo - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Seguridad Vecinal y Resguardo - treceavo piso
Propietario	Jefe de Dirección de Seguridad Vecinal y Resguardo
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.19. Dirección de Gestión de Personas

Nombre	SWI_PP009_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Gestión de Personas
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[57]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[57]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP009_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Jefe de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP009_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Secretario de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP009_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Ejecutivo de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP009_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Encargado de TI de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP009_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP009_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP009_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP009_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP009_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Gestión de Personas
Categoría	Hardware TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Gestión de Personas
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[58]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[58]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP009_001
Descripción	Armario de archivos para Dirección de Gestión de Personas
Categoría	Infraestructura TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Jefe de Dirección de Gestión de Personas
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP009_001
Descripción	Dirección de Gestión de Personas - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP009_001
Descripción	Alarma de Dirección de Gestión de Personas
Categoría	Control de entorno
Ubicación	Dirección de Gestión de Personas - catorceavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP009_001
Descripción	Archivo de Dirección de Gestión de Personas - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Gestión de Personas - catorceavo piso
Propietario	Jefe de Dirección de Gestión de Personas
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.20. Dirección de Salud

Nombre	SWI_PP0010_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Salud - décimo quinto piso
Propietario	Departamento de TI - Encargado TI de Dirección de Salud
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[59]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[59]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0010_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Jefe de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0010_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Secretario de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0010_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Ejecutivo de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0010_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Encargado de TI de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0010_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0010_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0010_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0010_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0010_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Salud
Categoría	Hardware TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Salud
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[60]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[60]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP0010_001
Descripción	Armario de archivos para Dirección de Salud
Categoría	Infraestructura TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Jefe de Dirección de Salud
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0010_001
Descripción	Dirección de Salud - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP0010_001
Descripción	Alarma de Dirección de Salud
Categoría	Control de entorno
Ubicación	Dirección de Salud - décimo quinto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0010_001
Descripción	Archivo de Dirección de Salud - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Salud - décimo quinto piso
Propietario	Jefe de Dirección de Salud
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.21. Dirección de Educación

Nombre	SWI_PP0011_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Educación - décimo sexto piso
Propietario	Departamento de TI - Encargado TI de Dirección de Educación
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[61]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[61]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0011_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Jefe de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0011_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Secretario de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0011_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Ejecutivo de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0011_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Encargado de TI de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0011_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0011_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0011_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0011_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0011_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Educación
Categoría	Hardware TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Educación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[62]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[62]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP0011_001
Descripción	Armario de archivos para Dirección de Educación
Categoría	Infraestructura TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Jefe de Dirección de Educación
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0011_001
Descripción	Dirección de Educación - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP0011_001
Descripción	Alarma de Dirección de Educación
Categoría	Control de entorno
Ubicación	Dirección de Educación - décimo sexto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0011_001
Descripción	Archivo de Dirección de Educación - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Educación - décimo sexto piso
Propietario	Jefe de Dirección de Educación
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.22. Secreataría Comunal de PLanificación

Nombre	SWI_PP0012_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso
Propietario	Departamento de TI - Encargado TI de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[63]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[63]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0012_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Jefe de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0012_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Secretario de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0012_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Ejecutivo de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0012_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Encargado de TI de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0012_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0012_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0012_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0012_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0012_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Secreataría Comunal de PLanificación
Categoría	Hardware TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[64]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	CAB_PP0012_001
Descripción	Armario de archivos para Secreataría Comunal de PLanificación
Categoría	Infraestructura TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Jefe de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0012_001
Descripción	Secreataría Comunal de PLanificación - Instancia física
Categoría	Infraestructura TI
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[64]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	RNG_PP0012_001
Descripción	Alarma de Secreataría Comunal de PLanificación
Categoría	Control de entorno
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0012_001
Descripción	Archivo de Secreataría Comunal de PLanificación - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Secreataría Comunal de PLanificación - décimo séptimo piso
Propietario	Jefe de Secreataría Comunal de PLanificación
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.23. Dirección de Asesoría Jurídica

Nombre	SWI_PP0013_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso
Propietario	Departamento de TI - Encargado TI de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[65]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[65]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0013_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Jefe de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0013_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Secretario de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0013_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Ejecutivo de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0013_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Encargado de TI de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0013_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0013_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0013_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0013_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0013_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Asesoría Jurídica
Categoría	Hardware TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[66]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[66]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP0013_001
Descripción	Armario de archivos para Dirección de Asesoría Jurídica
Categoría	Infraestructura TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Jefe de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0013_001
Descripción	Dirección de Asesoría Jurídica - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP0013_001
Descripción	Alarma de Dirección de Asesoría Jurídica
Categoría	Control de entorno
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0013_001
Descripción	Archivo de Dirección de Asesoría Jurídica - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Asesoría Jurídica - décimo octavo piso
Propietario	Jefe de Dirección de Asesoría Jurídica
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.24. Secretaría Municipal

Nombre	SWI_PP0014_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Secretaría Municipal - primer piso
Propietario	Departamento de TI - Encargado TI de Secretaría Municipal
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[67]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[67]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0014_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Jefe de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0014_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Secretario de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0014_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Ejecutivo de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0014_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Encargado de TI de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0014_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0014_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0014_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0014_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0014_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Secretaría Municipal
Categoría	Hardware TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Secretaría Municipal
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[68]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[68]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP0014_001
Descripción	Armario de archivos para Secretaría Municipal
Categoría	Infraestructura TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Jefe de Secretaría Municipal
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0014_001
Descripción	Secretaría Municipal - Instancia física
Categoría	Infraestructura TI
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP0014_001
Descripción	Alarma de Secretaría Municipal
Categoría	Control de entorno
Ubicación	Secretaría Municipal - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0014_001
Descripción	Archivo de Secretaría Municipal - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Secretaría Municipal - primer piso
Propietario	Jefe de Secretaría Municipal
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.25. Dirección de Control

Nombre	SWI_PP0015_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Control - cuarto piso
Propietario	Departamento de TI - Encargado TI de Dirección de Control
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[69]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[69]https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0015_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Jefe de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0015_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Secretario de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0015_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Ejecutivo de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0015_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Encargado de TI de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0015_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0015_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0015_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0015_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0015_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Control
Categoría	Hardware TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Control
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[70]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[70]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP0015_001
Descripción	Armario de archivos para Dirección de Control
Categoría	Infraestructura TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Jefe de Dirección de Control
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0015_001
Descripción	Dirección de Control - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP0015_001
Descripción	Alarma de Dirección de Control
Categoría	Control de entorno
Ubicación	Dirección de Control - cuarto piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0015_001
Descripción	Archivo de Dirección de Control - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Control - cuarto piso
Propietario	Jefe de Dirección de Control
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

3.2.26. Dirección de Comunicaciones

Nombre	SWI_PP0015_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso
Propietario	Departamento de TI - Encargado TI de Dirección de Comunicaciones
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[71]Ejecución arbitraria de código (resuelto). Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

[71] https://www.cvedetails.com/cve/CVE-2017-3881/

Nombre	NTB_PP0015_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Jefe de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0015_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Secretario de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0015_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Ejecutivo de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	NTB_PP0015_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Encargado de TI de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	EML_PP0015_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0015_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0015_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	EML_PP0015_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Robo de información digital. Pérdida de integridad física o lógica por intervención remota. Está sujeta a vulnerabilidades de manera transitiva.

Nombre	NAS_PP0015_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Dirección de Comunicaciones
Categoría	Hardware TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Dirección de Comunicaciones
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[72]Ejecución remota de código. Robo de información digital. Pérdida del equipo. Pérdida de integridad física o lógica por intervención remota. Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

[72]https://www.cvedetails.com/cve/CVE-2017-7494/

Nombre	CAB_PP0015_001
Descripción	Armario de archivos para Dirección de Comunicaciones
Categoría	Infraestructura TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Jefe de Dirección de Comunicaciones
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano. Posee información de alto interés para un grupo específico.

Nombre	OFI_PP0015_001
Descripción	Dirección de Comunicaciones - Instancia física
Categoría	Infraestructura TI
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Puede ser sujeto de desastres de origen natural. Puede ser sujeto de desastres de origen humano.

Nombre	RNG_PP0015_001
Descripción	Alarma de Dirección de Comunicaciones
Categoría	Control de entorno
Ubicación	Dirección de Comunicaciones - décimo noveno piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Pérdida de integridad física o lógica por intervención física. Pérdida de integridad física o lógica por intervención remota.

Nombre	ARC_PP0015_001
Descripción	Archivo de Dirección de Comunicaciones - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Dirección de Comunicaciones - décimo noveno piso
Propietario	Jefe de Dirección de Comunicaciones
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	No existen respaldos fisicos. No existen respaldos digitales. Pérdida de integridad física o lógica por intervención física. Posee un gran valor por reducción de especies.

4. Análisis de riesgos

5. Riesgos asociados a la atención de público

Título de Riesgo	Imposibilidad de obtener una hora de atención a público
Autor	Erik Regla
Fecha de Levantamiento	11/06/2020
Descripción	Al materializarse este riesgo, una persona natural queda imposibilitada de poder solicitar una hora para su atención, lo cual genera un cuello de botella.
Dueño del Activo	Jefe de Oficina de Asuntos Municipales.
Proceso	Obtención de hora de atención. Entrega de sugerencias. Entrega de reclamos. Solicitud de información.
Sub Área	Informaciones, Reclamos y Sugerencias.
Dependencia	Oficina de Asuntos Municipales.
Detalle de la Vulnerabilidad	Bla bla bla, el programa utilizado en bla bla... Debido a que la versión del sistema operativo utilizado tiene una gran cantidad de CVEs activos, existe la posibilidad de que un usuario malicioso intente generar un ataque de denegación de servicio dentro de la misma municipalidad.
Detalle de la amenaza	Bla bla bla, el programa utilizado en bla bla... Debido a que la versión del sistema operativo utilizado tiene una gran cantidad de CVEs activos, existe la posibilidad de que un usuario malicioso intente generar un ataque de denegación de servicio dentro de la misma municipalidad.
Respuesta	PREVENIR
Aprobación	Jefe de Oficina de Asuntos Municipales.

6. Riesgos asociados a plataformas o tecnologías generalizados dentro de la organización

Título de Riesgo	Denegación de servicio
Autor	Erik Regla
Fecha de Levantamiento	11/06/2020
Descripción	Al materializarse este riesgo, el sitio web de la municipalidad deja de quedar disponible para todo público.
Dueño del Activo	Jefe de Departamento de Tecnologías de la Información.
Proceso	Nivel general, Disponibilidad sitio web.
Sub Área	Dirección de Comunicaciones. Oficina de Asuntos Municipales. Departamento de Tecnologías de la Información.
Dependencia	Jefe de Departamento de Tecnologías de la Información.
Detalle de la Vulnerabilidad	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.
Detalle de la amenaza	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 simultaneamente, 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 desarolladas para uso interno.
Respuesta	CORREGIR
Aprobación	Jefe de Departamento de Tecnologías de la Información.

Título de Riesgo	Ejecución remota de código
Autor	Erik Regla
Fecha de Levantamiento	11/06/2020
Descripción	Al materializarse este riesgo, el atacante ejecuta código en el navegador del cliente sin previo consentimiento.
Dueño del Activo	Jefe de Departamento de Tecnologías de la Información.
Proceso	Nivel general, Disponibilidad sitio web.
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información.
Detalle de la Vulnerabilidad	La ejecución remota de código permite que un usuario no autorizado ejecute instrucciones en otro equipo.
Detalle de la amenaza	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.
Respuesta	PREVENIR
Aprobación	Jefe de Departamento de Tecnologías de la Información.

Título de Riesgo	Manipulación de redirecciones
Autor	Erik Regla
Fecha de Levantamiento	11/06/2020
Descripción	Al materializarse este riesgo, el atacante fuerza la redirección a un sitio externo.
Dueño del Activo	Jefe de Departamento de Tecnologías de la Información.
Proceso	Nivel general, Disponibilidad sitio web. Nivel general, Confiabilidad sitio web.
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información.
Detalle de la Vulnerabilidad	La ejecución remota de código permite que un usuario no autorizado ejecute instrucciones en otro equipo.
Detalle de la amenaza	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.
Respuesta	MITIGAR
Aprobación	Jefe de Departamento de Tecnologías de la Información.

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

7. Riesgos generales asociados a ingenería social

Título de Riesgo	Phishing
Autor	Erik Regla
Fecha de Levantamiento	11/06/2020
Descripción	Al materializarse este riesgo, un usuario ingresa información institucional a un sitio falso.
Dueño del Activo	Jefe de Departamento de Tecnologías de la Información.
Proceso	
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información.
Detalle de la Vulnerabilidad	Un usuario recibe un correo con un mensaje falso pero con apariencia visual creible, de esta manera para tentar al usuario a ejecutar alguna acción que pueda comprometer la seguridad, ya sea filtrando credenciales o información sensible.
Detalle de la amenaza	Un ataque de Phishing implica la personificación de otro individuo o entidad, la cual actua 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 tecnico.
Respuesta	PREVENIR
Aprobación	Jefe de Departamento de Tecnologías de la Información.

8. Riesgos generales asociados a activos estándares

9. Matriz de riesgos

10. Política de seguridad

Referencias