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

Seguridad Informática

Proyecto 1

Erik Regla
eregla09@alumnos.utalca.cl

10 de junio de 2020

1. Introducción

2. Estructura organizacional

El alcance de este trabajo abarca solo las siguientes divisiones:

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

3.2. Activos de carácter específico

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

[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	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[12]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.

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.

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

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	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[13]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.

[13]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	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[14]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.

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

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.

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	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[15]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.

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.

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

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	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[16]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.

[16]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.

SWI_DP001 Switch general Cisco Catalyst 2960 para específico del departamento Hardware TI Departamento de Asuntos Municipales - primer piso Departamento de TI - Encargado TI de Departamento de Asuntos Municipales 155 CVE-2017-3881[17]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.

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

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.

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[18]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.

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

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.

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.

SWI_DP002 Switch general Cisco Catalyst 2960 para específico del departamento Hardware TI Departamento de Certificación y Archivo - segundo piso Departamento de TI - Encargado TI de Departamento de Certificación y Archivo 155 CVE-2017-3881[19]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.

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

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.

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[20]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.

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.

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

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.

SWI_DP003 Switch general Cisco Catalyst 2960 para específico del departamento Hardware TI Departamento de Asuntos Concejo Cosoc y Otros. - tercer piso Departamento de TI - Encargado TI de Departamento de Asuntos Concejo Cosoc y Otros. 155 CVE-2017-3881[21]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.

[21]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[22]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.

[22]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.

SWI_DP004 Switch general Cisco Catalyst 2960 para específico del departamento Hardware TI Departamento de Revisión de Procesos de Contratación Pública - cuarto piso Departamento de TI - Encargado TI de Departamento de Revisión de Procesos de Contratación Pública 155 CVE-2017-3881[23]Ejecución arbitraria de código (resuelto).
Pérdida del equipo.
Pérdida de integridad física o lógica por intervención física.

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

Pérdida 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_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[24]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.

[24]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.

SWI_DP005 Switch general Cisco Catalyst 2960 para específico del departamento Hardware TI Departamento de Auditoría Operativa - quinto piso Departamento de TI - Encargado TI de Departamento de Auditoría Operativa 155 CVE-2017-3881[25]Ejecución arbitraria de código (resuelto).

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

Pérdida del equipo.
Pérdida de integridad física o lógica por intervención física.
Pérdida 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_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[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_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.

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

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.

SWI_DP006 Switch general Cisco Catalyst 2960 para específico del departamento Hardware TI Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso Departamento de TI - Encargado TI de Departamento de Revisión de Pagos de Bienes y Servicios 155 CVE-2017-3881[27]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_DP006_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
Propietario	Jefe de Departamento de Revisión de Pagos de Bienes y Servicios
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.

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

Nombre	NTB_DP006_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
Propietario	Secretario de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
Propietario	Ejecutivo de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
Propietario	Encargado de TI de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Revisión de Pagos de Bienes y Servicios
Categoría	Hardware TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Revisión de Pagos de Bienes y Servicios
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.

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

Nombre	CAB_DP006_001
Descripción	Armario de archivos para Departamento de Revisión de Pagos de Bienes y Servicios
Categoría	Infraestructura TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - sexto piso - recurso estático
Propietario	Jefe de Departamento de Revisión de Pagos de Bienes y Servicios
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_DP006_001
Descripción	Departamento de Revisión de Pagos de Bienes y Servicios - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - 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_DP006_001
Descripción	Alarma de Departamento de Revisión de Pagos de Bienes y Servicios
Categoría	Control de entorno
Ubicación	Departamento de Revisión de Pagos de Bienes y Servicios - 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.

4. Análisis de riesgos

5. Matriz de riesgos

6. Política de seguridad

Referencias

[1] Bill McDaniel. *An Algorithm for Error Correcting Cyclic Redundance Checks*. https://www.drdobbs.com/an-algorithm-for-error-correcting-cyclic/184401662, 2002.

[2] Linux Man pages. *gpg(1) - Linux man page*. https://linux.die.net/man/1/gpg.

[3] VeraCrypt. *Documentation*. https://www.veracrypt.fr/en/Documentation.html.

[4] Koopman, Philip and Chakravarty, T. *Cyclic redundancy code (CRC) polynomial selection for embedded networks*. 10.1109/DSN.2004.1311885. 2004.