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

Seguridad Informática

Proyecto 1

Erik Regla
eregla09@alumnos.utalca.cl

21 de junio de 2020

1. Introducción

2. Estructura organizacional

2.1. Organigrama

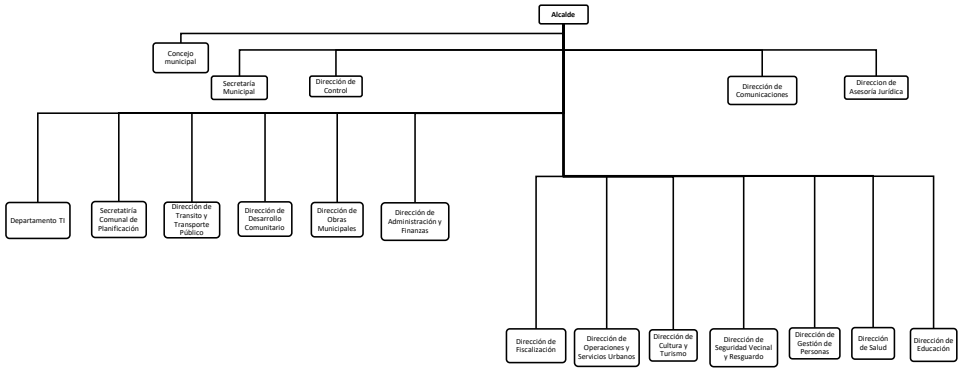

Figura 1: Organigrama

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 cartografía**.
- **Departamento de revisión de procesos de contratación pública**
- **Departamento de auditoría operativa**
- **Departamento Revisión de procesos de pago, bienes y servicios**

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

3.1. Contexto[1]

3.2. Situación actual

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

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

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

3.3. Procesos

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

3.3.1. Sistema contabilidad gubernamental

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

[1] 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.

[2] https://digital.gob.cl/doc/Guia_de_desarrollo_de_software_para_el_Estado.pdf

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

Funciones de este sistema:

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

3.3.2. Sistema de tesoreria municipal

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

Funciones de este sistema:

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

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

3.4. Sistema patentes comerciales

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

Funciones de este sistema:

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

3.5. Sistema permisos de circulación

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

Funciones de este sistema:

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

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

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[3]Autenticación inválida en cabeceras del módulo ISM. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

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[4]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

[3]https://www.cvedetails.com/cve/CVE-2013-1241/
[4]https://www.cvedetails.com/cve/CVE-2017-3881/

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[5]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

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	Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. Quiebre autenticación de tarjeta magnética. Falta de monitoreo.

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

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[6] Quiebre autenticación de llave seguridad. Dependencia de licencias. Ejecución de malwarepor falta de software AV. Desastres lógicos. Falta de encriptado. Carencia de licencias. Falta de protocolo de borrado de información.

[6]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[7]Tampering Vulnerability existente al momento de un fallo en la información de los perfiles. CVE-2018-8302[8]Ejecución de código remota debido al fallo de manipulación de objetos en memoria, resultante en control total. CVE-2018-8159[9] XSS resultante en elevación de privilegios por medio de requests web . CVE-2018-8154[10]Ejecución de código remota debido a la corrupción del manejo de objetos en memoria, resultante en control total. CVE-2018-8153[11] Spoofing . CVE-2018-8152[12] Elevación de privilegios . CVE-2018-8151[13] Corrupción de memoria . Quiebre autenticación de llave seguridad. Desastres lógicos. Falta de encriptado. Carencia de licencias. Falta de protocolo de borrado de información. No existe plan de recuperación de desastres. Inexistencia de respaldos digitales. Falta de documentación e implantación de políticas para envío de correos masivos.

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

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	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad. Transaccion rota.

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[14]Ejecución remota de código por medio de CRSRF. CVE-2019-16220[15]Sanitización de wp_validate manipula redirects. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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[16]Denegación de servicio. CVE-2008-7247[17]Bypass de restricciones RBAC. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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

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.

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[18]Buffer overflow causado por información EXIF. CVE-2008-7247[19]Buffer overflow causado por información EXIF. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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

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

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[20]Denegación de servicio. CVE-2008-7247[21]Bypass de restricciones RBAC. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

[20]https://www.cvedetails.com/cve/CVE-2009-0819/
[21]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.

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[22]Buffer overflow causado por información EXIF. CVE-2008-7247[23]Buffer overflow causado por información EXIF. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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 claro de las vulnerabilidades. Está sujeta a vulnerabilidades de manera transitiva. Quiebre autenticación de llave seguridad. Falta de encriptado. Falta de protocolo de borrado de información.

[22]https://www.cvedetails.com/cve/CVE-2019-11042/
[23]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[24]Denegación de servicio. CVE-2008-7247[25]Bypass de restricciones RBAC. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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.

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[26]Buffer overflow causado por información EXIF. CVE-2008-7247[27]Buffer overflow causado por información EXIF. Quiebre autenticación de llave seguridad. Quiebre autenticación de llave seguridad.

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

3.6. Activos externalizados

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

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

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

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

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

3.6.1. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[28]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

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	Desastres naturales. Desastres de origen humano.

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	Desastres naturales. 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	Quiebre autenticación de llave seguridad.

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

3.6.2. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[29]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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

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	Quiebre autenticación de llave seguridad.

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

3.6.3. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[30]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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

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	Quiebre autenticación de llave seguridad.

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

3.6.4. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[31]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

[31]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	Quiebre autenticación de llave seguridad.

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

3.6.5. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[32]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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	Desastres naturales. Desastres de origen humano.

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

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	Quiebre autenticación de llave seguridad.

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

3.6.6. 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[33]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[33]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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[34]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[34]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	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

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	Desastres naturales. 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	Quiebre autenticación de llave seguridad.

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

3.6.7. 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[35]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[35]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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[36]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

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

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	Desastres naturales. 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	Quiebre autenticación de llave seguridad.

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

3.6.8. Departamento de Cartografía

Nombre	SWI_DP003_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Cartografía - tercer piso
Propietario	Departamento de TI - Encargado TI de Departamento de Cartografía
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[37]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

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

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

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

Nombre	NTB_DP003_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Cartografía - tercer piso - recurso estático
Propietario	Encargado de TI de Departamento de Cartografía
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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 Cartografía
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

Nombre	EML_DP003_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Departamento de Cartografía
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

Nombre	EML_DP003_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Departamento de Cartografía
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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 Cartografía
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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

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

Nombre	OFI_DP003_001
Descripción	Departamento de Cartografía - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Cartografía - tercer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Desastres naturales. Desastres de origen humano.

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

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

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

3.6.9. 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[39]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[39]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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[40]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

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

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	Desastres naturales. 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	Quiebre autenticación de llave seguridad.

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

3.6.10. 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[41]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[42]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

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	Desastres naturales. Desastres de origen humano.

[42]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	Quiebre autenticación de llave seguridad.

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

3.6.11. Dirección de revisión de Procesos de Pago, Bienes y Servicios

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[43]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[43]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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. 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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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	Divulgación y copiado de informacion. Quiebre autenticación de llave seguridad. Está sujeta a vulnerabilidades de manera transitiva. Roles no definidos. Quiebre autenticación de llave seguridad. Transaccion rota. Phishing.

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[44]Ejecución remota de código. Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[44]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	Desastres naturales. Desastres de origen humano. No existe plan de recuperación de desastres.

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	Desastres naturales. 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	Quiebre autenticación de llave seguridad.

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

4. Análisis de riesgos

1 Empresa Externa 1 2 Empresa Externa 2 3 Empresa Externa 3

Remuneraciones Registro comunal de permisos de circulación Licencias de conducir Patentes municipalesControl de bienes Adquisisión y control de bodegas Banco de datos propiedas comunales Oficina de partes DepartamentoTecnologiasJuzgados de polícia local mantencion y administración de cartografia digital

Administracion red departamente licencias de conducir administracion red departamento de juzgados de policia local partes empadronados departamento de seguridad ciudadana administración red departamento patentes municpales y tesorería administración red del departamento de seguridad ciudadana administración de dirección de obras municipales plataforma de egresos administracion de sistemas de desarrollo comunitario sistemas computaciones por internet y sistemas sociales

administración de sistemas de egresos, recursos humanos y remuneraciones ** Contabilidad gubernamental **

5. Riesgos asociados a factores no tecnológicos

6. Riesgos asociados a procesos municpales

7. Riesgos asociados procesos de atención municipal

8. Riesgos asociados a control del personal

9. Riesgos asociados de índole técnica

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

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

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

Título de Riesgo	Residuos de información
Autor	Erik Regla
Fecha de Levantamiento	12/06/2020
Descripción	Al materializarse este riesgo, información que haya sido borrada sigue disponible dentro de una base de datos sin ser detectada
Dueño del Activo	Jefe de Departamento de Tecnologías de la Información.
Proceso	Resguardo de información personal. Resguardo de información institucional.
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
Detalle de la Vulnerabilidad	Una auditoria realizada por contraloría reveló que no existen protocolos de eliminación de la información de manera interna y esta tampoco forma parte de los servicios contratados.
Detalle de la amenaza	Al no existir un protocolo de eliminado de información claro, es altamente probable que la información no pueda ser eliminada de manera efectiva ya sea de plataformas, dispositivos, medios extraibles, etc. Este problema aplica también a los archivos físicos que no cuenten con respaldo y que dentro de las operaciones vigentes consideren su eliminación.
Respuesta	CORREGIR
Aprobación	Alcalde

Título de Riesgo	Residuos de información
Autor	Erik Regla
Fecha de Levantamiento	12/06/2020
Descripción	Al materializarse este riesgo, información que haya sido borrada sigue disponible dentro de una base de datos sin ser detectada
Dueño del Activo	Jefe de Departamento de Tecnologías de la Información.
Proceso	Resguardo de información personal. Resguardo de información institucional.
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
Detalle de la Vulnerabilidad	Una auditoria realizada por contraloría reveló que no existen protocolos de eliminación de la información de manera interna y esta tampoco forma parte de los servicios contratados.
Detalle de la amenaza	Al no existir un protocolo de eliminado de información claro, es altamente probable que la información no pueda ser eliminada de manera efectiva ya sea de plataformas, dispositivos, medios extraibles, etc. Este problema aplica también a los archivos físicos que no cuenten con respaldo y que dentro de las operaciones vigentes consideren su eliminación.
Respuesta	CORREGIR
Aprobación	Alcalde

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

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 del servicio.
Sub Área	Departamento de Tecnologías de la Información.
Dependencia	Jefe de Departamento de Tecnologías de la Información. , Empresas externas
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 del servicio.
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 del servicio. Nivel general, Confiabilidad del servicio.
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 malwarepor falta de software AV
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.

10. 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.

11. Matriz de riesgos

12. Política de seguridad

Referencias