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

Seguridad Informática

Proyecto 1

Erik Regla
eregla09@alumnos.utalca.cl

22 de junio de 2020

Índice

Parte I

ResumenEjecutivo

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

La parte dos presenta una introducción al problema a resolver.

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

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

La parte cuatro presenta las conclusiones obtenidas de este trabajo.

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

Parte II

Introducción

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

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

Parte III

Desarrollo

1. Estructura organizacional

1.1. Organigrama

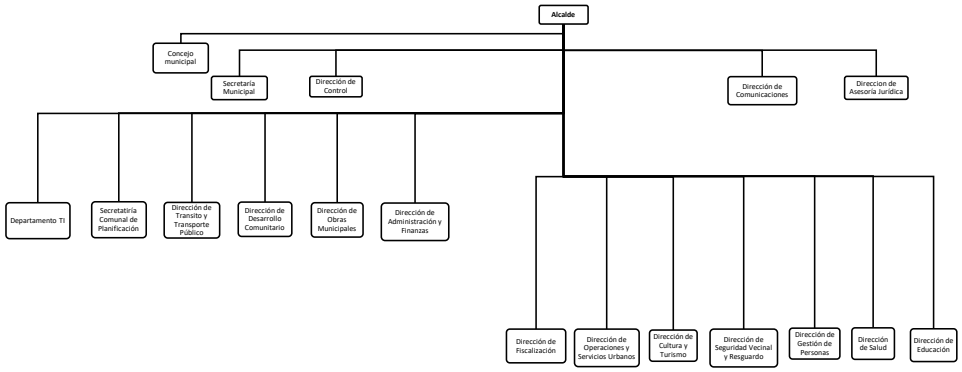

Figura 1: Organigrama

1.2. Rationale

El alcance de este trabajo abarca solo las siguientes divisiones:

- **Departamento de asuntos municipales**

- **Departamento de certificación y archivo**
- **Departamento de cartografía**.
- **Departamento de revisión de procesos de contratación pública**
- **Departamento de auditoría operativa**
- **Departamento Revisión de procesos de pago, bienes y servicios**
- **Departamento Tenologías de la Información**

Se establece para cada departamento la siguiente estructura base:

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

Se establece para cada oficina la siguiente estructura base:

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

Se establece para cada secretaría la siguiente estructura base:

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

2. Identificación de activos

2.1. Contexto[1]

2.2. Situación actual

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

[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.

- 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-

2.3. 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:

2.3.1. 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 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).

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

- Confección de órdenes de pago.
- Ingreso y contabilización de documentos contables, rendiciones decuentas.

2.3.2. 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.

2.4. Sistema patentes comerciales

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

Funciones de este sistema:

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

2.5. Sistema permisos de circulación

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

Funciones de este sistema:

- Generación de giro para pago de permisos de circulación.
- Generación de duplicado de permisos de circulación.
- Emisión de giros de fondos a terceros
- Bloqueo por sistema de placas patentes.
- Consultas de pagos años anteriores, de registro de multas, deincorporaciones y de traslados.
- Generación de giros de sellos.
- Mantención de traslado.
- Asignación de código de S.I.I.
- Anulación de giros mal emitidos

2.6. Activos de carácter transversal

A continuación se listan los activos de 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. Dependencia de licencias. 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. Dependencia de licencias. 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. Dependencia de licencias. 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.

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

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. Dependencia de licencias. Falta de protocolo de borrado de información.

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.

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

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.

2.7. 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. Emisión de decretos de pago sin registrar datos y/o sin comprobantes. Recepción de pagos con cálculos de intereses y multas fuera de período. Mantenimiento preventivo externalizado ejecutado deficientemente. No existe plan de recuperación de desastres.

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

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. Emisión de decretos de pago sin registrar datos y/o sin comprobantes. Falta de encriptado. Residuos de información. Mantenimiento preventivo externalizado ejecutado deficientemente. Denegación de servicio. Ejecución de malwarepor falta de software AV. Inexistencia de respaldos digitales. Falta de protocolo de borrado de información. Soporte externo ejecutado de manera deficiente. No existe plan de recuperación de desastres.

2.8. Activos de carácter específico

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

2.8.1. 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[28]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

Nombre	NTB_DP001_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Asuntos Municipales - primer piso - recurso estático
Propietario	Jefe de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

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

Nombre	NTB_DP001_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Asuntos Municipales - primer piso - recurso estático
Propietario	Secretario de Departamento de Asuntos Municipales
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	Divulgación y copiado de informacion. Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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

[29]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.

2.8.2. 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[30]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[30]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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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[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_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.

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

Nombre	RNG_DP002_001
Descripción	Alarma de Departamento de Certificación y Archivo
Categoría	Control de entorno
Ubicación	Departamento de Certificación y Archivo - segundo piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	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.

2.8.3. 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[32]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[32]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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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

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

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.

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.

2.8.4. 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[34]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[34]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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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[35]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.

[35]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.

2.8.5. 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[36]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. candados de seguridad.

[36]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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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

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

Nombre	CAB_DP005_001
Descripción	Armario de archivos para Departamento de Auditoría Operativa
Categoría	Infraestructura TI
Ubicación	Departamento de Auditoría Operativa - quinto piso - recurso estático
Propietario	Jefe de Departamento de Auditoría Operativa
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	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.

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.

2.8.6. 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[38]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

[38]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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. candados de seguridad.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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. Falta de documentación e implantación de políticas para envío de correos masivos.

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[39]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_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.

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

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.

2.8.7. Departamento de Tecnologías de la Información

Nombre	SWI_TI001_0001
Descripción	Switch general Cisco Catalyst 2960 para específico del departamento
Categoría	Hardware TI
Ubicación	Departamento de Tecnologías de la Información - primer piso
Propietario	Departamento de TI - Encargado TI de Departamento de Tecnologías de la Información
Valoración	Confidencialidad: 1 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	CVE-2017-3881[40]Ejecución arbitraria de código (resuelto). Perdida o robo. Quiebre autenticación de llave seguridad. Desastres naturales. Desastres de origen humano.

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

Nombre	NTB_TI001_001
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Jefe de Departamento de Tecnologías de la Información
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. candados de seguridad.

Nombre	NTB_TI001_002
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Secretario de Departamento de Tecnologías de la Información
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. candados de seguridad.

Nombre	NTB_TI001_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Ejecutivo de Departamento de Tecnologías de la Información
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. candados de seguridad.

Nombre	NTB_TI001_003
Descripción	Thinkpad T490 series, equipo corporativo
Categoría	Hardware TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Encargado de TI de Departamento de Tecnologías de la Información
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. candados de seguridad.

Nombre	EML_TI001_001
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Jefe de Departamento de Tecnologías de la Información
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. Falta de documentación e implantación de políticas para envío de correos masivos.

Nombre	EML_TI001_002
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Secretario de Departamento de Tecnologías de la Información
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. Falta de documentación e implantación de políticas para envío de correos masivos.

Nombre	EML_TI001_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Ejecutivo de Departamento de Tecnologías de la Información
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. Falta de documentación e implantación de políticas para envío de correos masivos.

Nombre	EML_TI001_003
Descripción	Cuenta de correo corporativa
Categoría	Activo de información tangible
Ubicación	EXE_EXCHA_001
Propietario	Encargado de TI de Departamento de Tecnologías de la Información
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. Falta de documentación e implantación de políticas para envío de correos masivos.

Nombre	NAS_TI001_001
Descripción	Cisco NSS324 NAS, NAS local para equipo de la Departamento de Tecnologías de la Información
Categoría	Hardware TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Departamento de TI - Encargado TI de Departamento de Tecnologías de la Información
Valoración	Confidencialidad: 4 Integridad: 5 Disponibilidad: 3
Vulnerabilidades y Amenazas	CVE-2017-7494[41]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_TI001_001
Descripción	Armario de archivos para Departamento de Tecnologías de la Información
Categoría	Infraestructura TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Jefe de Departamento de Tecnologías de la Información
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_TI001_001
Descripción	Departamento de Tecnologías de la Información - Instancia física
Categoría	Infraestructura TI
Ubicación	Departamento de Tecnologías de la Información - primer piso - recurso estático
Propietario	Administración del edificio
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 5
Vulnerabilidades y Amenazas	Desastres naturales. Desastres de origen humano.

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

Nombre	RNG_TI001_001
Descripción	Alarma de Departamento de Tecnologías de la Información
Categoría	Control de entorno
Ubicación	Departamento de Tecnologías de la Información - 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_TI001_001
Descripción	Archivo de Departamento de Tecnologías de la Información - registro de documentos
Categoría	Activos tangibles / Activos intangibles
Ubicación	Departamento de Tecnologías de la Información - primer piso
Propietario	Jefe de Departamento de Tecnologías de la Información
Valoración	Confidencialidad: 5 Integridad: 5 Disponibilidad: 4
Vulnerabilidades y Amenazas	Inexistencia de respaldos físicos. Inexistencia de respaldos digitales. . Quiebre autenticación de llave seguridad.

3. Análisis de riesgos

3.1. Riesgos asociados a factores no tecnológicos

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

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

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

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

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

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

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

3.2. Riesgos asociados a procesos municpales

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

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

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

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

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

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

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

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

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

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

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

3.3. Riesgos asociados a control del personal

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

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

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

3.4. Riesgos asociados de índole técnica

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

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

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

Título de Riesgo	Dependencia de licencias.
Autor	Erik Regla
Fecha de Levantamiento	12/06/2020
Descripción	Al materializarse este riesgo, la carencia de una licencia podría limitar la disponibilidad de un servicio que dependa de esta.
Dueño del Activo	Dominio General
Proceso	Afecta a todos los procesos en general
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información.
Detalle de la Vulnerabilidad	Para el caso de software que opera con licencias (Office 365 por ejemplo), la no disponibilidad de las mismas puede ocasionar problemas al momento de utilizar otros servicios
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 estén disponibles. Sin embargo, la no caducidad no tiene relación alguna con las licencias asignadas, ya que dependiendo del tier involucrado en las licencias asignadas, son los servicios disponibles.
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	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 seguridad o bien interrupciones en la disponibilidad de un servicio.
Dueño del Activo	Dominio General
Proceso	Disponibilidad del servicio.
Sub Área	Administracion municipal Afecta a los procesos de envio y recepción de correo
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. Resguardo de información personal. Resguardo de información institucional. Contabilidad gubernamental Administracion municipal
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	CORREGIR TRANSFERIR si es externalizado
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. , Empresa Externa 1
Proceso	Resguardo de información personal. Resguardo de información institucional. Contabilidad gubernamental Administracion municipal
Sub Área	Todas.
Dependencia	Jefe de Departamento de Tecnologías de la Información. , Empresa Externa 1
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 TRANSFERIR si es externalizado
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	Contabilidad gubernamental Administracion municipal
Sub Área	Departamento revisión de procesos de pago, bienes y servicios Departamento de revisión de procesos de contratación pública Departamento de Asuntos Municipales.
Dependencia	Jefe de Departamento de Tecnologías de la Información. , Empresa Externa 1
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	MITIGAR TRANSFERIR si es externalizado
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. , Empresa Externa 1
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	TRANSFERIR
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	Contabilidad gubernamental Jefe de Dirección de Administración y Finanzas
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	MITIGAR TRANSFERIR si es externalizado
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	MITIGAR
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	Contabilidad gubernamental Administracion de red y plataforma
Sub Área	Jefe de Departamento de Tecnologías de la Información.
Dependencia	Jefe de Departamento de Tecnologías de la Información. Empresa Externa 1
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	CORREGIR TRANSFERIR si es externalizado
Aprobación	Jefe de Departamento de Tecnologías de la Información.

3.5. 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	Afecta a los procesos de envio y recepción de correo
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 creíble, 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 actúa como emisor de un mensaje el cual puede ser de interés del usuario. En este caso la apuesta es que el lector del correo hará caso del call to action antes de verificar la veracidad del contenido, por lo que este tipo de ataques está dirigido a un público no técnico.
Respuesta	PREVENIR
Aprobación	Jefe de Departamento de Tecnologías de la Información.

4. Matriz de riesgos

La matriz de riesgos está agregada adjunta al proyecto.

5. Políticas de seguridad

5.1. Objetivos de la política

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

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

5.2. Declaración de autoridad y alcance

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

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

5.3. Política de uso aceptable

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

5.4. Política de identificación y autenticación

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

5.5. Política de acceso a internet

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

5.6. Política de acceso

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

5.7. Política de acceso remoto

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

5.8. Políticas del manejo de incidentes

En caso de robo o pérdida del equipo:

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

En caso de mal uso:

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

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

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

Parte IV

Conclusiones

Parte V
Bibliografía

Referencias