Servicio de Salud
Magallanes

Ministerio de Salud

RESOLUCION EXENTA Nº 10457

Punta Arenas, 26 OCT. 2018

VISTOS: Los antecedentes respectivos, Memo N° 35/23.10.2018 del Jefe Regional TIC; Lo dispuesto en la ley N°19.880 que establece Bases de los Procedimientos Administrativos; en el Decreto con Fuerza de ley N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del Decreto Ley N°2763, de 1979 y de las leyes N°18.933 y N°18.469; en el Decreto Supremo N°136, de 2004, del Ministerio de Salud, que aprueba Reglamento Orgánico del Ministerio de Salud; en la ley N°19.799 sobre documentos electrónicos, forma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo N°83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos: en la ley N°19.233 sobre delitos informáticos: en la Norma Chilena NCh-ISO 27002 Of.2013; y 10 manifestado en la Resolución Exenta N° 1161 del 04.10.2016 que Aprueba el Sistema de Seguridad de la Información.

C O N S I D E R A N D O

Que, la necesidad de contar con adecuadas políticas de seguridad de la información, destinadas a proteger los recursos de información y la tecnología utilizada para su procesamiento. Todo, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo que permita alcanzar niveles de integridad, confidencialidad y disponibilidad, con todos los activos de información relevantes para la institución, como un principio clave en la gestión de procesos, y en uso de las facultades que me confiere el Articulo quincuagésimo noveno de la Ley N° 19.882 en su texto modificado por la Ley N° 20.955 y el Art. N° 80 de la Ley N° 18.834, dicto la siguiente:

R E S O L U C I O N:

1. APRUEBESE, a contar del 27 de Agosto del año 2018 y hasta nueva disposición, "**Política de Seguridad la Gestión de Activos"** de la Dirección de Servicio de Salud Magallanes y sus establecimientos dependientes.

2.- Entiéndase como parte integrante de esta Resolución dicha Política, que a continuación se indica.

Política de Seguridad en la Gestión de Activos.

Preparado por:	Andrés Martínez Chamorro.		
Revisado por	Equipo TIC del Servicio de Salud Magallanes		
Aprobado por:	Pablo Alexis Cona Romero	**Fecha de Aprobación:**	10-07-2018
		Fecha de Publicación:	11-07-2018
		Vigente desde:	11-07-2018
		Vigente Hasta:	Nueva Revisión.

Control de versiones

Versión	Fecha de Vigencia	Aprobado por	Fecha publicación	Firma	Comentario
1.0	27-03-2014	Mauricio Díaz Cárdenas	27-03-2014		
2.0	03-2016	Pablo Cona Romero	11-07-2018		Revisión crítica de la 1ra versión. Todas las secciones.

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Cualquier pregunta o comentario sobre esta Política de Seguridad de Información dirigirla al Departamento TIC.

1. OBJETIVOS DE LA SEGURIDAD EN LA GESTION DE ACTIVOS DE LA INFORMACION EN LA DSSM.

1.1 OBJETIVO GENERAL:

Establecer una protección adecuada de los recursos de información de la Dirección del Servicio de Salud Magallanes (DSSM) y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información, a través de un Sistema de Gestión de Seguridad de la Información (SGSI).

1.2 OBJETIVOS ESPECÍFICOS:

- Identificar todos los activos importantes asociados a cada sistema de información de la DSSM, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

- Analizar los riesgos que afectan a los recursos de la información de esta Institución frente a posibles amenazas, ya sean internas o externas.

- Clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la Organización y establecer las medidas oportunas para reducir el impacto esperado hasta un nivel aceptable.

- Diseñar e implementar medidas que permitan mitigar los riesgos de procesamiento, conservación y transmisión de la información que sean identificados, del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo, sin perder de vista el enfoque de la gestión por procesos institucionales.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información, y de esta forma minimizar la ocurrencia de hechos contingentes de posibles amenazas en los medios de almacenamiento y procesamiento.

- Generar planes de continuidad operacional ante hechos contingentes que interrumpan la operación del sistema de seguridad de la información.

- Mantener la Política de Seguridad de gestión de activos del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

- Evaluar y coordinar la implementación de controles específicos de seguridad se la información para los activos de esta organización, sean preexistente o nuevos.

2. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Para que estos objetivos sean efectivos, resulta necesaria la implementación de esta Política de Seguridad de Gestión de Activos formando parte activa de la cultura organizacional de la Dirección del Servicio Magallanes, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento con lo cual se ayudará a la preservación y acceso a la información local y la interacción segura con sistemas externos.

Esta Política se aplica a todos los funcionarios de la Dirección del Servicio de Salud Magallanes (planta, contrata, reemplazos y suplencias), personal a honorarios y personal externo que preste servicios, (proveedores, compra de servicios, etc). Que tengan accesos privilegiado a la información, además de contemplar todos los controles contenidos en la NCh-IS027001.0f2009.

La presenta política considera todos los activos de Información que se requiera proteger. en cada institución, considerando la información en sí, en todas sus formas y representaciones, los procesos relacionados, los sistemas, redes, tecnologías en general y el personal involucrado en su operación, manipulación y protección.

3. MARCO NORMATIVO POLITICAS SEGURIDAD DE LA GESTIÓN DE ACTIVOS.

La política de la seguridad de la información considera el siguiente marco legal:

- Política de Seguridad de la Información DSSM.
- Norma ISO/IEC 27002:2013, puntos A.5, A.5.1.1, A.6, A.6.1.1, A.8, A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11, A.11.2.7
- NCh-IS027001.0f2013; Tecnologías de la Información – Técnicas de Seguridad sistemas de gestión de la seguridad de la información.
- NCh-IS027002.0f2013; Tecnologías de la Información - Código de prácticas para la gestión de la seguridad de la información.
- Ley N° 19.628, agosto de 1999. Sobre protección de la vida privada y datos personales. Ministerio Secretaria General de la Presidencia.
- Ley N° 20.285, sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.
- Ley N° 20.285, de transparencia o acceso a la información pública.
- Ley N° 19.653, sobre probidad administrativa aplicable de los órganos de la administración del Estado.
- Instructivo para el manejo de inventarios en el nivel central del Ministerio de Salud (Resolución Exenta N°12, del 9 de enero de 2009).
- D.F.L N°29 que fija texto refundido, coordinado y sistematizados de la Ley N° 18.834, sobre estatuto Administrativo.
- Decreto N°41, de 2012, del Ministerio de Salud, que aprueba reglamento sobre fichas clínicas:
    - Regular el contenido, almacenamiento, administración, protección y eliminación de fichas clínicas de manera de resguardar el correcto empleo, disponibilidad y confidencialidad de las mismas.

- Resolución Exenta N° 1161, que aprueba sistemas de seguridad de la información de las Subsecretarías de la Salud Pública y Redes Asistenciales.
- Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad incluidas en el portal del CSIRT del Ministerio del Interior:
    - https://www.csirt.gob.cl/decretos
    - https://www.csirt.gob.cl/leyes

4. MARCO GENERAL DE LAS POLITICAS SEGURIDAD DE LA INFORMACIÓN.

La Política General de Seguridad de la Información ha sido elaborada en concordancia con la legislación vigente en el país, considerando además su compatibilidad con las prácticas sugeridas en la NCh 27002 Of.2013.

La Dirección se compromete a realizar las acciones que estén a su alcance para permitir la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

5. DEFINICIONES

Información: la información es la interpretación que se da a un conjunto de datos, pudiendo residir está en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos de la DSSM, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

Información Pública: toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente

Información reservada (conocimiento reservado) : son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

La información secreta (solamente a quien le atañe la información debe conocerlo): son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales.

Seguridad de la Información: es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

Activo de Información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Podemos distinguir 3 tipos de activos:

a) La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, etc.).

b) Los Equipos/Sistemas que la soportan.

c) Las Personas que la utilizan. Los activos poseen valor para la organización, y necesitan por tanto ser protegidos adecuadamente, para que no se vea perjudicado.

6. ROLES Y RESPONSABILIDADES

6.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI): es el cuerpo integrado por representantes de todas las áreas sustantivas del DSSM, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

El Comité de Seguridad de la Información (CSI), tiene los siguientes objetivos:

- Revisar y proponer al Director(a) del Servicio de Salud, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fueran convenientes y apropiadas elaboradas por el Encargado de Seguridad de la Información para la Dirección del Servicio de Salud Magallanes.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de esta Institución frente a posibles amenazas, sean internas o externas.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de esta Organización.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Recomendar roles y responsabilidad específicos que se relacionen con la Seguridad de la Información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de esta Organización, sean preexistente o nuevos.
- Apoyar en las funciones del Encargado de Seguridad de la Información.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Dirección del Servicio de Salud Magallanes, como así, coordinar el proceso de administración de la continuidad de las actividades.

6.1.2 ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

Se describe a modo de resumen algunas de las funciones del cargo actual:

- **Políticas de Seguridad:**
  - Tener a su cargo el desarrollo de las políticas de seguridad al interior de la organización y el control de su implementación, y velar por su correcta aplicación.
  - Generar en conjunto con el Comité de Seguridad de la Información, los controles, registros e indicadores que implementen las políticas.
  - Verificar el cumplimiento de estas políticas.
- **Organización de Seguridad:**
  - Establecer responsabilidades asociadas a la protección de los activos y procesos específicos:
  - Identificar y definir claramente los activos y procesos asociados a cada sistema individual.
  - Debe definirse el administrador responsable por cada activo o proceso de seguridad y los detalles de esta responsabilidad deben estar documentados.
  - Los niveles de autorización deben estar claramente definidos y documentados
  - Crear el equipo de respuesta ante incidentes y comité de Seguridad que de soporte a las políticas establecidas.

- **Gestión de Activos:**
  - Inventariar y clasificar de acuerdo a su grado de sensibilidad los activos que desean ser protegidos.
  - Establecer medidas apropiadas para su protección.

6.1.3 PROPIETARIO DE LA INFORMACIÓN: Es el Jefe o Encargado de la Unidad Organizacional o apoyo correspondiente, responsable de la protección y uso de la información. EI propietario de la información es responsable de clasificación de la misma y es responsable del mantenimiento y actualización de dicha clasificación.

También debe participar en la definición de los lineamientos y controles necesarios, así como de su monitoreo con el apoyo del Jefe Regional TIC, en especial con el encargado de la información, para estar en cumplimiento con las normativas y objetivos de la DSSM.

6.1.4 USUARIO DE LA INFORMACIÓN: Es el conjunto de funcionarios (planta, contrata, reemplazos y suplencia) personal a honorarios y/o externas (proveedores, compra de servicios, tratamiento por encargo, servicios externalizados, etc), que con la debida autorización del propietario de la información, puede consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento.

- Los usuarios finales solo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitaran su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.
- Las principales responsabilidades de los usuarios de información son:
  - Utilizar la información solo para el propósito para el que recibió autorización de uso.
  - Conocer las políticas y procedimiento de Seguridad de la Información que se han institucionalizado.
  - Cumplir con los controles establecidos en las políticas y procedimientos definidos en el SGSI y que están relacionadas a su quehacer habitual.
  - Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

7. MATERIAS TRATADAS.

Las materias tratadas en el documento están relacionas con la seguridad de la información en la gestión de activos, abordadas en las siguientes temáticas:

- Identificar los activos de la Dirección del Servicio de Salud Magallanes y definir las responsabilidades de protección pertinentes.
- Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.
- Reflejar la sensibilidad de los activos en un modelo de Niveles de Clasificación de los activos.
- Prevenir todo uso no autorizado de los activos de información y sus medios de almacenamiento, como divulgación, modificación, eliminación o destrucción.

8. LINEAMIENTOS ESTRATEGICOS.

8.1 GESTIONAR LA SEGURIDAD EN EL TRATAMIENTO DE ACTIVOS.

- Se integran los requisitos y lineamientos respecto a la Gestión de Activos, ya señalados en la Política General de Seguridad de la Información.
- Para lograr mantener un proceso de Gestión de Mejora Continua en la protección de la seguridad de los activos de Información, se usara el modelo DEMING o POCA (Plan; Do; Check; Act), materializado en las secciones a continuación:
    - Lineamientos de Planificación.
    - Lineamientos de Implementación.
    - Lineamientos de Revisión y Mejora.

8.2 LINEAMIENTOS DE PLANICFICACIÓN.

8.2.1 SEGURIDAD ASOCIADA EN SERVICIOS DE TERCEROS.

- Activos de Información:
    - Los procesos y sus activos, son la base de la evaluación de riesgos, que sustenta los controles de seguridad necesarios para la protección de dichos activos, ya que al igual que otros recursos valiosos de la institución, merecen o requieren protección contra diversas amenazas y peligros.

- Dichos activos, se asocian a la información en sí, en todas sus formas y representaciones, los procesos relacionados, los sistemas, redes y el personal involucrado en su operación, manipulación y protección.

- Ejemplos de activos:

Activos	Tipo de activos	Responsable del activo
Hardware y Sotfware	Software	Dependencia TIC según corresponda
	Base de datos	
	Hardware	
	Equipos informáticos	
	Sistemas	
Otros.	Documentos expedientes	Jefe de División, departamento y/o Unidad donde se desarrolla el proceso
	Infraestructura (edificios, equipamiento, etc)	Jefe de División, departamento y/o Unidad donde se desarrolla el proceso
	Personas	Jefe de División, departamento y/o Unidad donde se desarrolla el proceso

- Activos de Información:
  - La información y muchos otros activos de información tienen un ciclo de vida en la organización y al interior de sus propios procesos de negocio.
  - Se deben reconocer las diferentes etapas por las que pasa un activo, desde por ejemplo: su creación, adquisición u origen, transformación, pasando por almacenamiento, procesamiento, uso y transmisión, hasta su eventual decaimiento, eliminación o destrucción.
  - El valor del activo y los riesgos asociados pueden variar a lo largo de su vida útil.

8.2.2 LINEAMIENTOS INSTITUCIONALES EN GESTIÓN DE ACTIVOS.

- La institución debe identificar los lineamientos necesarios para proteger sus activos de información de amenazas en este ámbito, estableciendo controles normativos al respecto. Para ello debe analizar al menos los siguientes conjuntos de lineamientos:

    - Inventario de activos de Información
    - Propiedad de los activos de información
    - Uso aceptable de los activos
    - Devolución de activos
    - Clasificación de Información
    - Manejo de activos
    - Gestión Medios removibles
    - Eliminación de medios de almacenamiento
    - Transferencia de medios.
    - integración a la metodología de riesgos

8.2.3 DEFINIR Y MANTENER UN INVENTARIO ACTUALIZADO DE ACTIVOS.

Se requiere identificar y generar un inventario completo de los activos de información más relevantes, el que debe mantenerse actualizado y vigente durante todo el ciclo de vida de dichos activos.

Dicho inventario de activos debe ser preciso, actualizado, coherente y consistente con otros inventarios que pueda manejar el Servicio de Salud Magallanes de para otros fines.

La institución debe definir para su inventario de activos de información:

- Un diccionario de nombres y tipos de activos, para facilitar el trabajo colaborativo.
- Los campos o características que va a mantener. para cada tipo de activo. Por ejemplo:
    - Cantidades existentes
    - Propietario
    - Clasificación de sensibilidad o criticidad
    - Relación de dependencia con los procesos de negocio
    - Proveedor
    - Vida útil
- Frecuencia de revisión y actualización del inventario.
- Ubicación y controles de acceso para su revisión y modificación.

8.2.4 ESTABLECER LA PROPIEDAD DE LOS ACTIVOS.

A los activos que se mantienen en el inventario, para efectos del Sistema de Gestión de Seguridad de la Información, se les debe asignar un dueño o propietario, responsable de su clasificación, control de acceso y de determinar restantes controles de seguridad para el nivel de protección adecuado a la sensibilidad del activo y su aporte a la continuidad operacional.

El servicio debe asignar dicho propietario al momento de la creación, recepción o adquisición y de manera sistematizada. Hasta que se cambie al propietario del activo, este debería hacerse responsable de la correcta administración de sus activos durante todo su ciclo de vida, hasta su eliminación o destrucción.

La revisión permanente de Roles y Responsabilidades debe velar por la correcta asignación de propietarios de los activos más relevantes.

Asimismo, la institución debe correlacionar los movimientos de colaboradores y terceros contra los sistemas de control de acceso, particularmente al término del contrato o de la relación funcional.

El propietario o quien este designe, debe periódicamente revisar las restricciones de acceso y clasificaciones para los activos importantes.

8.2.5 DETERMINAR USO ACEPTABLE DE ACTIVOS.

Se deben identificar, documentar e implementar las reglas para el uso aceptable de los activos de información relevantes de la institución, con especial interés en la información crítica y las instalaciones y recursos tecnológicos necesarios. A mayor criticidad del activo, mayor especificación de condiciones de uso aceptable.

Se deberían considerar las normas para almacenamiento, manipulación y destrucción de activos según Ley N°20.285.

8.2.6 DIRECTRICES PARA LA DEVOLUCIÓN DE LOS ACTIVOS.

El Servicio de Salud Magallanes debe formalizar los mecanismos que permitan que todos empleados y usuarios de terceras partes hagan oportuna devolución de los activos pertenecientes a la institución que estén en su poder como consecuencia de la finalización o cambio de su relación laboral, contrato y/o acuerdo.

Se deben tomar, al menos, los siguientes resguardos:

- Transferir la información institucional en caso que haya estado usando algún equipamiento personal y que sea eliminada de aquel.
- Documentar toda información operacional importante que posea el empleado o usuario externo.
- Tener una clara definición de accesos de altos privilegios o únicos que pudiese tener el usuario, para respaldarlos.
- Restringir el acceso y uso de los recursos asignados al usuario.
- Garantizar una custodia con atribuciones reguladas para los activos devueltos por el usuario.
- Respaldar la información del activo (pc, notebook, celular, Tablet, etc.) institucional con el cual el usuario cumplía sus funciones laborales.
- El Servicio de Salud deberá garantizar las condiciones para la preservación y seguridad de los respaldos de la información de aquellos funcionaros que finalicen su relación laboral y/o contractual, por al menos un año.
- La realización del proceso de respaldo de toda información de los activos será responsabilidad del departamento TIC de esta dirección de servicio.

8.2.7 ESTABLECER NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN.

Se espera que cada establecimiento perteneciente al Servicio de Salud Magallanes pueda asegurar que la información reciba el nivel de protección adecuado de acuerdo con su importancia, por lo que se requiere poder diferenciar la más relevante o sensible. Por tanto, los activos deben ser clasificados en términos de requisitos legales, valor, criticidad y sensibilidad para evitar cualquier divulgación o modificación sin autorización.

La institución debe plantear un esquema consistente y se debe evaluar mediante el análisis y valoración de la confidencialidad, integridad y disponibilidad. Para un activo dado, la clasificación puede variar durante su ciclo de vida.

Las clasificaciones y los controles de protección asociados de la información deberían considerar las necesidades que tiene la organización de compartir o restringir información, así como también los requisitos legales, en particular aquellos establecidos en la Ley N°20.285 de transparencia y la Ley N°19.628, sobre la protección de la vida privada.

Para estos efectos, se recomienda que las políticas de gestión de activos que apruebe cada establecimiento dependiente del Servicio de Salud Magallanes contengan, como mínimo, las materias tratadas en la presente política.

ANOTESE, COMUNIQUESE Y ARCHIVASE.

SERVICIO DE SALUD MAGALLANES
DIRECTORA
XII REGIÓN

KARIN ERIKA URIBE SOTO
DIRECTORA (S) SERVICIO SALUD MAGALLANES

KEUS/MRBU/KGCG/kcg
Nº 4680 /

DISTRIBUCIÓN:

- Dirección SSM
- Depto. Subdirección Recursos Físicos y Financieros
- Depto. Subdirección Gestión Asistencial
- Depto. Subdirección Recursos Humanos
- Depto. Control de Gestión y Tecnología de Información y Comunicación
- Oficina de Partes