RESOLUCION EXENTA N° 7915

PUNTA ARENAS, 09 AGO. 2018

VISTOS: Los antecedentes respectivos: 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; Resolución Exenta N°4322/26.04.2018 Estructura Orgánica del Servicio de Salud Magallanes; Resolución Exenta N°6440/25.06.2018 que modifica la Resolución Exenta N°4322/26.04.2018; Resolución Exenta N°2888/20.07.2011 de la DSSM, que encomienda como Subdirectora Médica del Servicio de Salud Magallanes a Dra. Maria Cristina Diaz Muñoz; Decreto Exento N°83/12.04.2018 Ministerio de Salud, pone término y establece orden de subrogancia al cargo de Director del Servicio de Salud Magallanes; Decreto Exento N°97/31.05.2018 que modifica Decreto N°83 que establece orden de subrogancia al Cargo de Director del Servicio de Salud Magallanes y en uso de las facultades dicto lo siguiente:

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

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,

Memorándum N°15/07.07.2018 de Gestor Regional TI de la Dirección del Servicio de Salud Magallanes, que solicita validar Políticas de Seguridad y Procedimientos,

R E S O L U C I O N

1.- APRUÉBASE a contar del 11 de Julio de 2018 y hasta nueva revisión la **POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN** del Departamento Control de Gestión y Tecnología de Información y Comunicaciones.

2.- Entiéndase como parte integrante de la presente resolución dicho documento, que a continuación se indica:

Política de Clasificación y Manejo de la Información.

Preparado por:	Andrés Martínez Chamorro.		
Revisado por	Equipo TIC del Servicio de Salud Magallanes		
Revisado por			
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	10-07-2018	Pablo Cona Romero	11-07-2018		

(*) 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.

ÍNDICE

INTRODUCCIÓN

La Dirección Servicio Salud Magallanes considera que la protección de sus activos debe ser uno de los compromisos más importantes, bajo esta consideración, reconoce a la información y a los sistemas que la sustentan y procesan, como uno de sus activos más importantes a proteger, y establece como objetivo la gestión efectiva y eficiente de los riesgos a los que se ven sujetos, garantizando un adecuado control interno de los mismos.

La DSSM adquiere la responsabilidad de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la confidencialidad de la información, dentro de un marco general de gestión de riesgos de seguridad.

OBJETIVO

El objetivo del presente documento es definir el modelo de clasificación de activos de información que debe ser utilizado dentro de la Dirección Servicio Salud Magallanes con carácter global.

Este modelo de clasificación de la información es aplicable con carácter obligatorio a todos los usuarios que hagan uso de la información en el desarrollo de sus actividades, en cualquier momento del ciclo de vida de la información.

Si por motivos técnicos u otros no es posible cumplir con las especificaciones de este documento, se debe reportar a los responsables de seguridad para solicitar modificaciones en los procedimientos o políticas.

1. GESTIÓN DE ACTIVOS

La información es un recurso que como el resto de los activos, es importante y es esencial para el funcionamiento de la Dirección Servicio Salud Magallanes y por consiguiente para que ésta alcance sus objetivos, debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión del servicio.

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la confidencialidad, la disponibilidad y la integridad de las misma, para lo cual el objetivo del control de los activos es garantizar que toda la información administrada por Dirección del Servicio de Salud Magallanes, reciban un apropiado nivel de protección.

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad; de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

Inventario de los Activos DSSM

Se encuentra Adjunto en el **Anexo n° 1 de esta política: "Inventario de los activos DSSM".**

En el cual se identifican los activos importantes asociados a cada sistema de información de la DSSM, sus respectivos propietarios y su ubicación.

Este inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de su Unidad Organizativa.

1.1 PROPIEDADES DE LOS ACTIVOS DSSM

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

En la Dirección del Servicio Salud Magallanes la responsabilidad administrativa de toda la información y los activos asociados con los medio de procesamiento de información se ha designado a cada Jefe de su respectivo departamento de esta Dirección.

a. **Propietario del activo de información:** Se entiende por tal, a toda persona o entidad que tiene las habilidades de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo, lo que no le confiere en ningún caso derecho de propiedad sobre el mismo.

El propietario de la información, es el encargado de:

1. Clasificar los activos de información de acuerdo su grado de sensibilidad y criticidad y asegurar que la información y los activos asociados sean clasificados en forma apropiada.
2. Documentar y mantener actualizada la clasificación efectuada y definir las funciones que deberán tener permisos de acceso a los activos de información.
3. Definir y revisar cada 3 meses o cuando sea requerido, restricciones y clasificación del acceso al activo teniendo en cuenta la presente política.

b. Pasos y responsabilidades para la gestión de la información:

Nombre del paso	Responsabilidad
1. Ingreso del activo de información en el Inventario de activos DSSM.	Encargado Seguridad de la Información, Departamento TIC
2. Clasificación de la información	Propietario del activo.
3. Etiquetado de la información	Propietario del activo.
4. Manejo de la información	Personas que poseen derechos de acceso de acuerdo con esta Política

Si la información clasificada proviene de afuera de la organización, el Propietario del activo es el responsable de su clasificación según las reglas establecidas en esta Política, y esta persona se convierte en el propietario de ese activo de información.

1.2 LINEAMIENTOS DE CLASIFICACIÓN DE LA INFORMACIÓN

Para que la información pueda protegerse adecuadamente contra la divulgación, la modificación, la supresión y/o el uso no autorizado por parte de cualquier entidad ajena a la DSSM, se debe establecer un criterio único de clasificación cuyo alcance englobe a todos los integrantes de la organización.

Cabe recalcar la importancia de este aspecto, ya que sin un compromiso global para colaborar en la definición de los tipos de información que manejará DSSM en materia de clasificación de la información, no se podrán obtener resultados óptimos.

a. **Ciclo de Vida de la Información** A continuación, están enumerados los distintos estadios del ciclo de vida de la información.

- **Creación**: Incluye todas las posibilidades de elaboración de información.
- **Transmisión**: Incluye todos los mecanismos y tecnologías de transmisión de la información.
- **Procesamiento**: Incluye todas las aplicaciones que tratan la información.
- **Almacenamiento**: Incluye todas las formas de almacenamiento de la información.
- **Destrucción**: Incluye todas las posibilidades de eliminación de información.

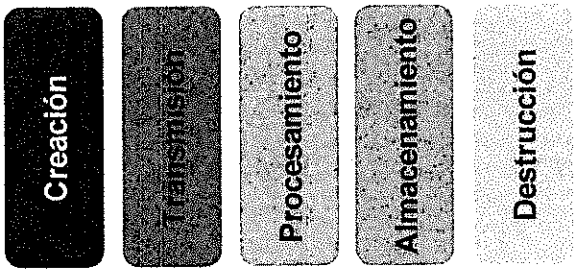


Gráfico 1: Estados del ciclo de vida de la información.

b. Características de Clasificación

Para establecer una adecuada protección de la información, éstos deben ser clasificados prioritariamente en función de:

- Valor de la información; significa que la información sólo será divulgada a quien tenga la necesidad legítima y demostrable de recibir la información, ya que según su clasificación se identificará el riesgo que representa una eventual divulgación, adulteración o indisponibilidad.

- Su nivel de sensibilidad, que es el atributo que indica los requerimientos de confidencialidad e integridad de la información gestionada por un sistema de información.

- Los requisitos legales por los que se encuentra afectada, de acuerdo a lo establecido por la Ley N° 20.285, sobre acceso a la información pública: "es pública la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la administración", en consecuencia la información tratada en la DSSM está contemplada dentro del alcance definido por este cuerpo legal y su propiedad corresponde al Estado de Chile, así como también los sistemas asociados a ella, los cuales deben ser protegidos de acuerdo a su valor y criticidad.

c. VALORACIÓN DE ACTIVOS: CONFIDENCILIDAD

A continuación se establece el criterio de clasificación dela información, de esta forma se logrará determinar el nivel de Confidencialidad de la información que se maneja en la Dirección Servicio Salud Magallanes.

Clasificación	Definición	Criterios de clasificación	Restricción de acceso
1 Pública	La información pública es aquella que ha sido divulgada o publicada previa autorización otorgada por el propietario de la información.	Este tipo de información no requiere de protección especial más allá de la revisión periódica de integridad bajo demanda, ya que su divulgación no supondrá ningún perjuicio	La información pública es accesible a todo aquel interesado en acceder a ella. En cuanto a los permisos de acceso, no existirá ningún tipo de restricción para el acceso

Clasificación	Definición	Criterios de clasificación	Restricción de acceso
			a este tipo de información.
	La información interna es aquella necesaria para el correcto desempeño de las funciones de la DSSM y por lo tanto accesible por el personal interno de la DSSM o ligado contractualmente a él, sin restricciones. No debe transmitirse ni comunicarse fuera del mismo sin autorización previa.	El acceso no autorizado a la información o bien una divulgación accidental o intencional de este tipo de información, podría ocasionar daños y/o inconvenientes menores, o perjuicio no significativo a la DSSM.	En cuanto a los permisos de acceso, esta información se encuentra disponible para todo el personal interno de la DSSM y terceros autorizados.
3 Confidencial / Restringida	La información confidencial es el tipo de información cuya divulgación, alteración o pérdida puede suponer un impacto significativo para la DSSM.	El acceso a la información debe ser restringido severamente, esta información deberá ser resguardada con especial recelo, limitando su acceso a aquellas personas, que previamente sean autorizadas por el propietario de la información y con un consentimiento formal. El acceso no autorizado a la información o una divulgación accidental o intencional de este tipo de información, podría	En cuanto a los permisos de acceso, estos deben ser restringidos severamente, se deben definir grupos específicos y limitados de acceso a este tipo de información (lista cerrada). La información está disponible solamente para un grupo específico de empleados y de terceros autorizados.

Clasificación	Definición	Criterios de clasificación	Restricción de acceso
		dañar considerablemente la imagen de la DSSM.	
4 Secreta	Información secreta es aquélla que debe ser conocida únicamente por el propietario de la misma.	El mal uso de información secreta puede tener un impacto significativo en la DSSM.	Los permisos de acceso a esta información deben ser únicos para el titular de la misma.

La regla básica es utilizar el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección para evitar gastos de protección innecesarios.

- **Lista de personas autorizadas**

La información clasificada como "Restringida" y "Confidencial" debe estar acompañada de una lista de personas autorizadas en la que el propietario de la información específica los nombres o los cargos de las personas que tienen derechos de acceso para esa información.

La misma regla aplica para el nivel de confidencialidad "Uso interno" si las personas externas a la organización tendrán acceso a esos documentos.

- **Reclasificación**

Los propietarios de activos deben revisar el nivel confidencialidad de sus activos de información y deben evaluar si se puede cambiar dicho nivel. Si es posible, deberían bajarlo.

d. VALORACIÓN DE ACTIVOS: INTEGRIDAD

Clasificación	Definición
1 Fácil Reparación	Información cuya modificación no autorizada puede repararse y no afecta el funcionamiento de la DSSM.
	Información cuy modificación no autorizada puede reparase aunque podría ocasionar pérdidas leves para la DSSM.
3 Difícil Reparación	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la DSSM.
4 Irreparable	Información cuya modificación no autorizada no podría reparase, ocasionando pérdidas graves para la DSSM.

e. VALORACIÓN DE ACTIVOS: DISPONIBILIDAD

Clasificación	Definición
1 Dispensable	Información cuya inaccesibilidad no afecta las gestiones y/u operaciones de la DSSM.
	Información cuya inaccesibilidad permanente durante 10 días podría ocasionar pérdidas significativas para la DSSM.
3 Muy indispensable	Información cuya inaccesibilidad permanente durante 5 días, podría ocasionar pérdidas significativas para la DSSM.
4 Absolutamente imprescindible	Información cuya inaccesibilidad permanente durante 1 día podría ocasionar pérdidas significativas para la DSSM

f. ESCALA DE PUNTUACIONES DE VALORES DE LOS ACTIVOS

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la disponibilidad, integridad, confidencialidad de cada uno de los activos. Al obtener cada uno de los puntajes asignados estos se promedian para poder obtener la valoración final de cada uno, dato que nos servirá para calcular el nivel de riesgo.

VALOR = PROM (DISPONIBILIDAD+INTEGRIDAD+CONFIABILIDAD)

PUNTUACIÓN	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
4	Absolutamente imprescindible	Irreparable	Secreta
3	Muy indispensable	Difícil reparación	Uso confidencial
2	Indispensable	Reparable	Uso interno
1	Dispensable	Fácil reparación	Acceso público

Tabla 1 Escala de puntuaciones de valores de los activos

1.3 USO ACEPTABLE DE LOS ACTIVOS

1. **Definiciones**

a. **Sistema de información**: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la organización, o que se encuentran bajo responsabilidad de la organización. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

b. **Activos de información:** en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

2. **Uso aceptable**

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades del servicio con el objetivo de ejecutar tareas vinculadas con la organización.

3. **Responsabilidad sobre los activos**

Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

4. **Actividades prohibidas**

Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad.

También está prohibido:

- Descargar archivos de imágenes o vídeos que no tienen objetivos de la DSSM, enviar cadenas de correos electrónicos, jugar juegos, etc.
- Instalar software en un ordenador local sin el permiso explícito del Jefe departamento de Informática
- Utilizar aplicaciones Java, controles Active X y otros códigos móviles, excepto cuando esté autorizado por el Departamento TIC.
- Utilizar herramientas criptográficas (encriptado) sobre ordenadores locales, excepto en los casos especificados en la Política de Clasificación de la Información.
- Descargar códigos de programa de soportes externos.
- Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del Jefe departamento de Informática.

5. Uso de activos fuera de las instalaciones

Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo del Jefe departamento de Informática y Jefe departamento de finanzas.

Mientras los activos en cuestión permanecen fuera de la organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

6. Procedimiento para copias de seguridad

El usuario debe realizar la copia de seguridad de toda la información sensible almacenada en su ordenador en una carpeta específica, compartida por el departamento TIC, como mínimo, una vez por día.

7. Protección antivirus

En cada ordenador debe estar instalado McAfee o Avira free con actualización automática activada.

8. Facultados para el uso de sistemas de información

Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.

Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

9. Responsabilidades sobre la cuenta de usuario

El usuario no debe, directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.

El propietario de la cuenta de usuario es su usuario, que es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

10. Responsabilidades sobre la clave

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo la jefatura y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el Comité de Seguridad de la Información.
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).
- Las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Se deben escoger claves seguras de la siguiente forma:
    - utilizando al menos ocho caracteres;
    - utilizando al menos un carácter numérico; un carácter alfabético en mayúscula (Obligatorio) y uno en minúscula;
    - utilizando al menos un carácter especial;
    - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;
    - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);

- no se deben usar nuevamente las últimas tres claves.
- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).

11. Política de pantalla y escritorio limpio

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a lo establecido en la Política de Clasificación de la Información, es considerada sensible para este punto.

12. Política de escritorio limpio

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo a lo establecido en la Política de Clasificación de la Información.

13. Política de pantalla limpia

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo.

14. Protección de instalaciones y equipos compartidos

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras y fotocopiadoras.

El uso no autorizado de impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado no está permitido, cada usuario debe manejar su clave. Por lo cual cada vez que utilice el equipo debe cerrar la sesión.

15. Uso de Internet

Sólo se puede acceder a Internet a través de la red local de la organización, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está prohibido.

El Departamento TIC puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la DSSM. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita al Encargado de Seguridad de la Información, solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.

El usuario debe considerar como no confiable la información recibida a través de sitios web no verificados.

El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

16. Correo electrónico y otros métodos de intercambio de mensajes

Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde Internet, la transferencia de datos por medio de teléfonos, el envío de mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

De acuerdo con esta política el Encargado de Seguridad de la Información determina el canal de comunicación que se puede utilizar para cada tipo de dato, como también las posibles restricciones sobre quién tiene permiso para utilizar los canales; es decir, define qué actividades están prohibidas.

Los usuarios solamente pueden enviar mensajes que contengan información veraz. Está prohibido enviar materiales perturbadores, desagradables, sexualmente explícitos, groseros, difamatorios o cualquier otro contenido inaceptable o ilegal. Los usuarios no deben enviar mensajes basura a personas con las cuales no se ha establecido o a personas que no solicitaron ese tipo de información.

Si un usuario recibe un correo electrónico basura, debe informarlo al Encargado de Seguridad de la Información.

Si se envía un mensaje con una etiqueta de confidencialidad, el usuario debe protegerlo de acuerdo con lo establecido en la Política de Clasificación de Información.

El usuario debe guardar todos los mensajes que contienen datos importantes para La DSSM utilizando el método especificado por el Comité de Seguridad de la Información.

Cada correo electrónico debe incluir una exención de responsabilidad, salvo los mensajes enviados a través de los sistemas de comunicación determinados por el Comité de Seguridad de la Información. Si un usuario envía un mensaje a través de un sistema de intercambio de mensajes (redes sociales, foros, etc.), debe declarar sin ambigüedades que no representa el punto de vista de la organización.

17. Derechos de autor

Los usuarios no deben realizar copias no autorizadas del software que pertenece a la DSSM, excepto en los casos permitidos por ley, por el propietario o por el Comité de Seguridad de la Información.

Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

18. Computación móvil

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, Tablet, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

Reglas básicas: Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos u otros medios de transporte, espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.

- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- La protección contra códigos maliciosos se instala y actualiza por el Departamento TIC.
- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad de datos a través de la nube de la DSSM.
- La protección de datos sensibles debe ser implementada de acuerdo con la Política de Clasificación de Información.
- En el caso que el equipamiento de computación móvil sea desatendido, se deben aplicar las reglas para equipamiento de usuario desatendido de acuerdo a la Política de pantalla y escritorio limpios.

El Encargado de Seguridad de la Información es el responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

19. Supervisión del uso de sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación, de la organización, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad de [nombre de la organización].

Los usuarios aceptan que personas autorizadas de la organización puedan acceder a todos los datos de ese tipo y que el acceso de dichas personas no será considerado una violación de privacidad del usuario.

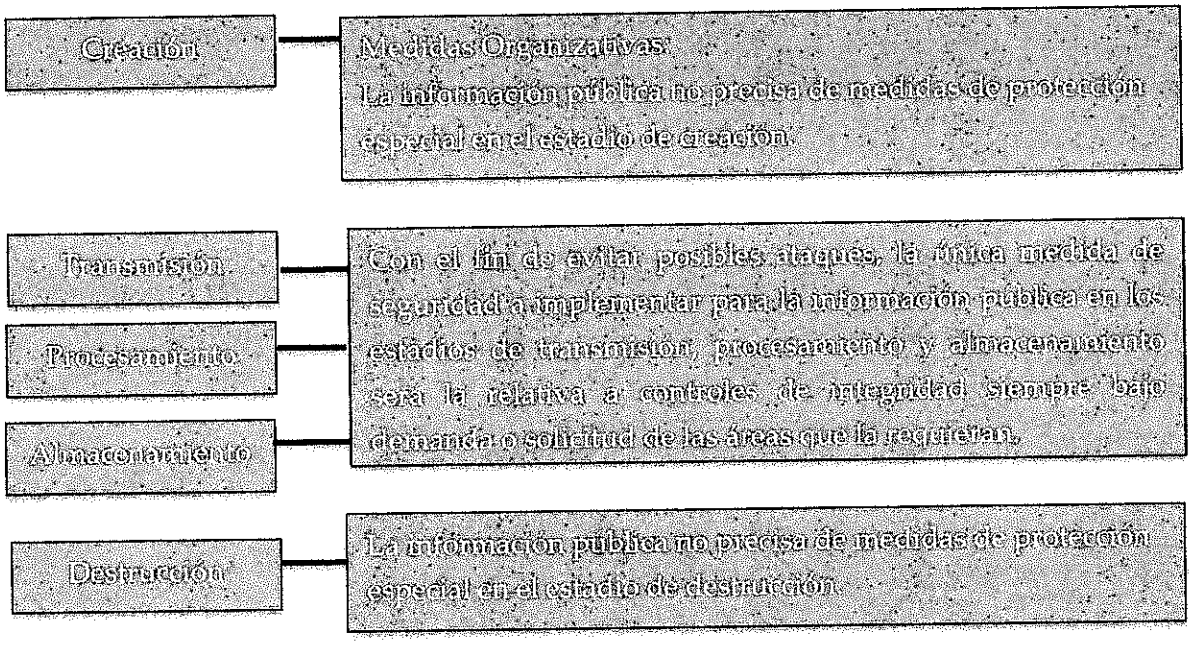
La organización puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

20. Incidentes

Cada empleado, proveedor o tercero que esté en contacto con datos y/o sistemas de la Dirección Servicio Salud Magallanes, debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente, de acuerdo a lo establecido en el Procedimiento para gestión de incidentes.

USO ACEPTABLE Y MEDIDAS DE SEGURIDAD EN CADA ESTADIO DEL CICLO DE LA INFORMACIÓN.

Información Pública digital o impresa:



Información Interna / Departamental: DIGITAL

Creación

Medidas Organizativas:

- La política de contraseñas configurada para el acceso a los PC y portátiles de los usuarios de la DSSM, se debe diseñar en conformidad con los estándares.
- Utilización de etiquetas que identifiquen su nivel.

Medidas Tecnológicas:

- Autenticación contra un servicio de directorio homologado por Seguridad de la Información. El mantenimiento y actualización de dicho directorio se debe realizar conforme a los procedimientos formales de aprovisionamiento.
- Antivirus y cortafuegos personales con actualización automática de firmas en los PC y portátiles de usuarios.
- Parches de seguridad correctamente actualizados en los PC y portátiles de usuarios conforme a las directrices establecidas por Seguridad de la Información.

Información Interna / Departamental: DIGITAL

Transmisión

Medidas Organizativas:

- Difusión acotada a grupos de interés y siempre limitada al entorno DSSM.
- Prohibición expresa de difusión en medios públicos.

Medidas Tecnológicas:

Los accesos a Internet a través de las redes de datos, desde un PC o portátil, deben disponer de las siguientes medidas de seguridad:

- Antivirus en la plataforma de correo.
- Antivirus en la plataforma de navegación.
- Cortafuegos personales instalados en los ordenadores portátiles.

Información Interna / Departamental: DIGITAL

Procesamiento

Medidas Organizativas:

- La política de contraseñas configurada para el acceso a los PCs y portátiles de los usuarios de la DSSM, debe diseñarse en conformidad con los estándares

Medidas Tecnológicas:

- Autenticación contra un servicio de directorio homologado por Seguridad de la Información. El mantenimiento y actualización de dicho directorio se debe realizar conforme a los procedimientos formales de aprovisionamiento.
- Antivirus y cortafuegos personales con actualización automática de firmas en los PCs y portátiles de usuarios la DSSM.
- Parches de seguridad correctamente actualizados en los PCs y portátiles de usuarios conforme a las directrices establecidas por Seguridad de la Información

Información Interna / Departamental: DIGITAL

Almacenamiento

Medidas Organizativas:

- Prohibición de almacenamiento en medios públicos sin control de acceso. Únicamente podrá ser almacenada en servicios digitales públicos (por ejemplo Google Docs) con la condición de que éstos dispongan de medidas de control de acceso. Por ejemplo: acceso mediante contraseña.

Medidas Tecnológicas:

- La realización de las copias de respaldo debe garantizar la recuperación de la información, con una pérdida máxima (RPO) de 24 horas.
- Medidas de seguridad estándar para protección de medios de almacenamiento y dispositivos móviles (teléfonos móviles, PDA, pen-drive, discos duros externos y dispositivos análogos).
- Todos los discos de red deben disponer de las siguientes medidas de protección estándar:
    - Los discos de red de la DSSM deben disponer, de la protección que proporciona su ubicación en zonas seguras y en redes protegidas.
- La ubicación física de los servidores de red de la DSSM debe realizarse en un lugar protegido con medidas de control de acceso, que garanticen que sólo el personal autorizado pueda tener acceso físico a los sistemas.
- Los servidores de red de la DSSM deben estar ubicados en un lugar protegido con medidas de control ambiental, que garanticen su protección contra fluctuaciones del fluido eléctrico, fluctuaciones de temperatura, inundaciones e incendios.
- La accesibilidad a los servidores de red de la DSSM debe estar restringida a través de redes protegidas, mediante sistemas de firewall e IDS/IPS.

Información Interna / Departamental: DIGITAL

Destrucción
La información digital interna no precisa de medidas de protección especial en el estadio de destrucción.

Información Interna / Departamental: IMPRESA

Creación
Las medidas para el estadio de creación de información interna en papel son: Medidas Organizativas: • Utilización de etiquetas que identifiquen su nivel: • Utilización de plantillas. • Paleta de colores corporativos • Logo DSSM

Información Interna / Departamental: IMPRESA

Transmisión
Las medidas definidas para el estadio de transmisión de información interna en papel son: Medidas Organizativas: • Difusión acotada a grupos de interés y siempre limitada a la DSSM. • Prohibición expresa de difusión en medios públicos

Información Interna / Departamental: IMPRESA

Procesamiento

La información interna en papel no precisa de medidas de protección especial en el estadio de procesamiento.

Información Interna / Departamental: IMPRESA

Almacenamiento

Las medidas definidas para el estadio de almacenamiento de información interna en papel son:

Medidas Organizativas:

- Cumplimiento de la política de escritorios limpios.

Información Interna / Departamental: IMPRESA

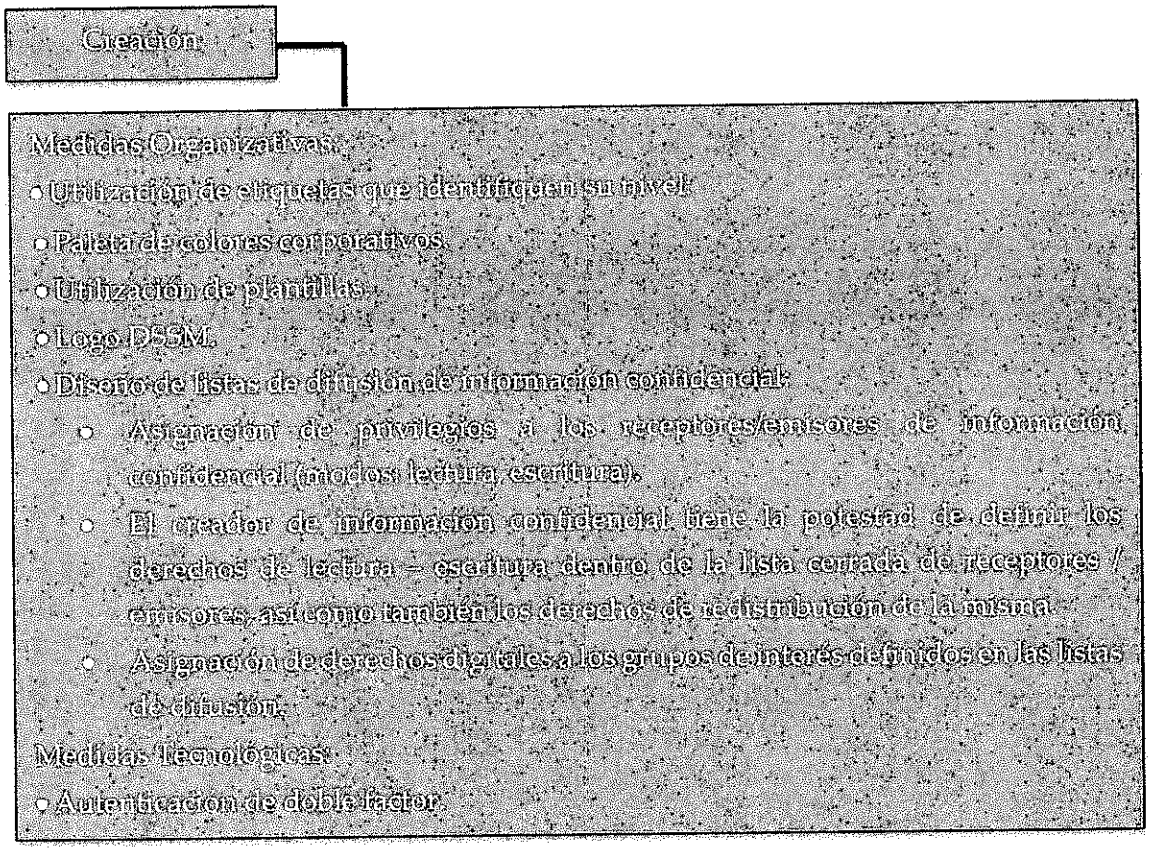
Destrucción

Las medidas definidas para el estadio de destrucción de información interna en papel son:

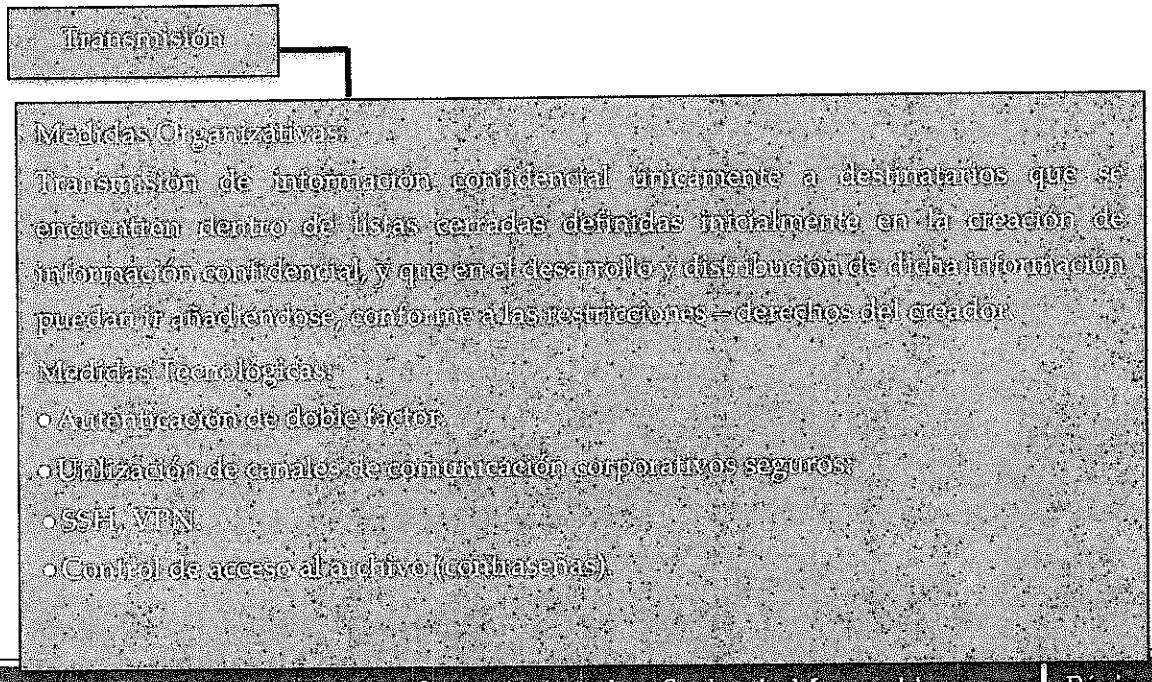
Medidas Organizativas:

- Uso obligatorio de papeleras para documentación interna.

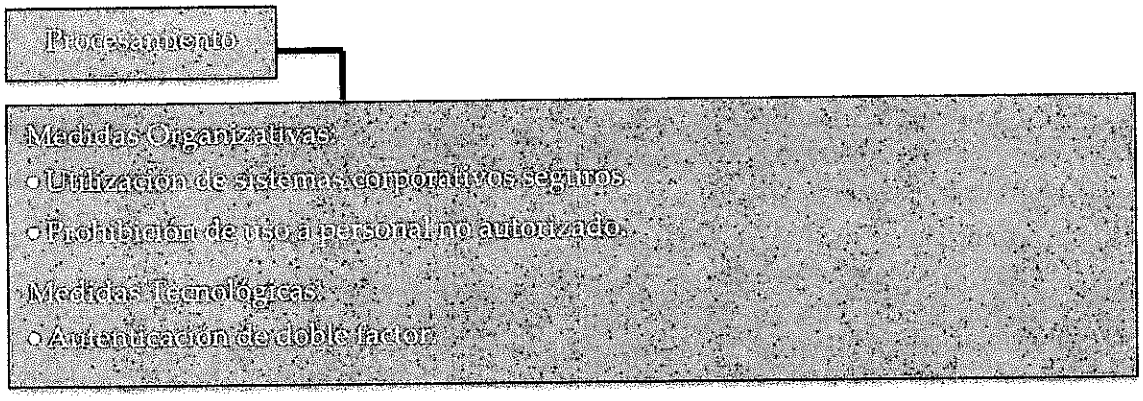
Información Confidencial / Restringida: DIGITAL



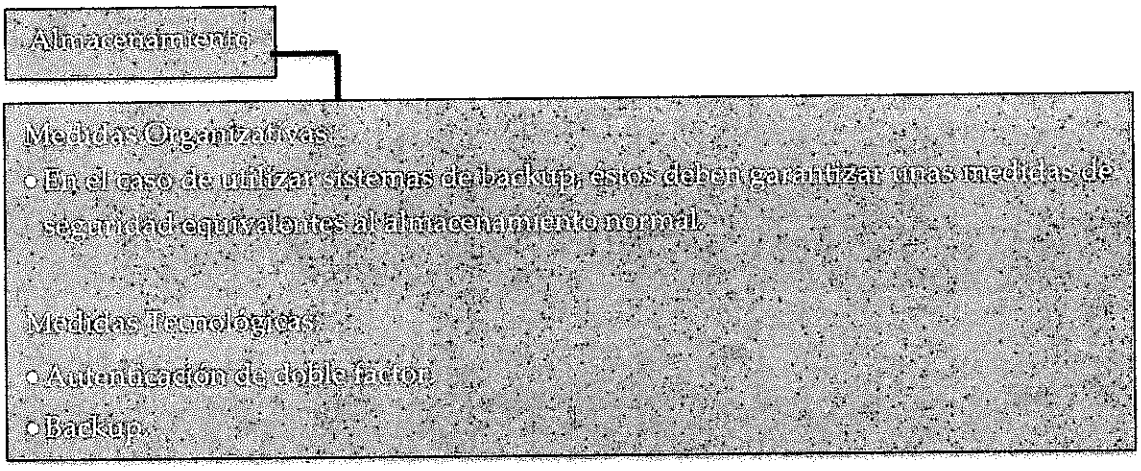
Información Confidencial / Restringida: DIGITAL



Información Confidencial / Restringida: DIGITAL

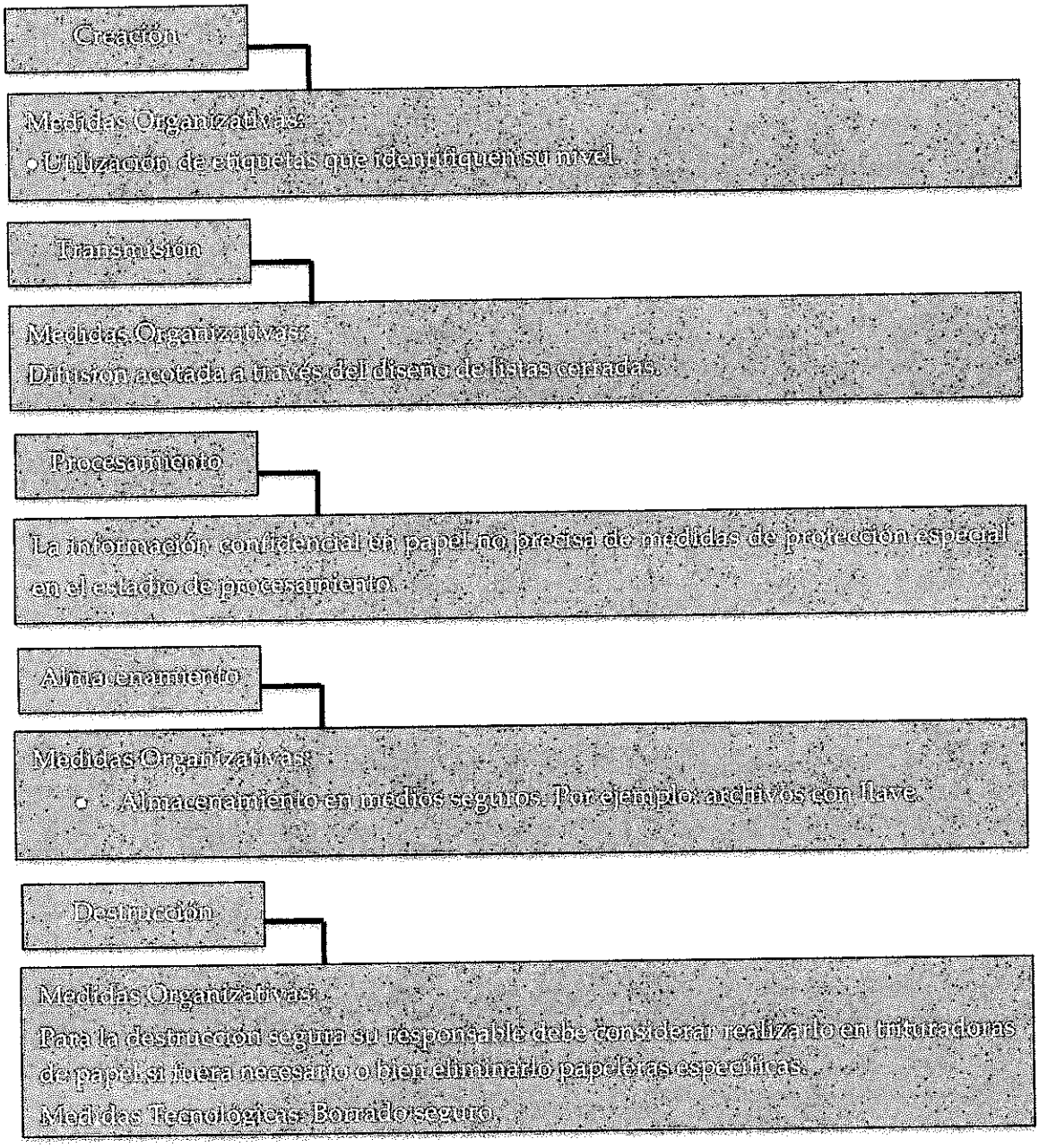


Información Confidencial / Restringida: DIGITAL



Información Confidencial / Restringida: DIGITAL

Información Confidencial / Restringida: IMPRESA



Copiado e impresión de información confidencial

1.4 ETIQUETADO Y MANEJO DE LA INFORMACIÓN

Toda información que disponga de la imagen corporativa de la DSSM o sus formatos será automáticamente clasificada como de uso interno.

- Soporte papel: cualquier documento en formato corporativo se entenderá asignado al nivel de clasificación USO INTERNO.
- Soporte electrónico: Para los soportes propios o generados en la entidad, no será necesario el etiquetado del mismo salvo en los siguientes casos:
Contengan datos de carácter personal de la entidad.

Nivel de confidencialidad	Etiquetado
Pública	(sin etiquetar)
Uso interno	USO INTERNO
Restringida/ Confidencial	RESTRINGIDA

Los niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel**: se indica el nivel de confidencialidad en la esquina supeior derecha de cada página del documento; también se indica en la portada o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.
- **Documentos electrónicos**: se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento.
- **Sistemas de información**: el nivel de confidencialidad en aplicaciones y bases de datos debe ser indicado en la pantalla de acceso al sistema, como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.

- **Correo electrónico**: se indica el nivel de confidencialidad en la primera línea del cuerpo del correo electrónico.
- **Soporte de almacenamiento electrónico** (discos, tarjetas de memoria, etc.): se debe indicar el nivel de confidencialidad sobre la superficie de cada soporte.
-
- **Información transmitida oralmente**: el nivel de confidencialidad de la información confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

Para la correcta identificación de los tipos de información, se ha definido la siguiente paleta de colores:

Información Pública: *Paleta RGB (146, 208, 80)*

Información Interna / Departamental: *Paleta RGB (255, 255, 102)*

Información Restringida/Confidencial: *RGB (255, 153, 0)*

Manejo de información clasificada

Todas las personas que tienen acceso a información clasificada deben seguir las reglas enumeradas en el siguiente cuadro. El Responsable de la Seguridad de la Información o La Jefatura Pertinente deben activar acciones disciplinarias cada vez que no se cumplan las reglas o si la información se transmite a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el Procedimiento para gestión de incidentes.

Los activos de información pueden ser llevados fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la Política de uso aceptable.

	Uso interno	*Uso Restringido/ Confidencial*
Documentos en papel	• Sólo las personas autorizadas pueden tener acceso. • Si es enviado fuera de la organización, el documento debe ser enviado por correo certificado. • Los documentos sólo pueden ser guardados en habitaciones sin acceso público. • Los documentos deben ser retirados frecuentemente de impresoras.	• El documento debe ser almacenado en un gabinete con llave. • Los documentos pueden ser transferidos dentro y fuera de la organización solamente en un sobre cerrado. • Si es enviado fuera de la organización, el documento debe ser enviado con acuse de recibo. • Los documentos deben ser retirados inmediatamente de impresoras. • Solamente el propietario del documento puede copiarlo. • Solamente el propietario del documento puede destruirlo.
Documentos electrónicos	• Sólo las personas autorizadas pueden tener acceso. • Cuando se intercambian archivos, mensajería instantánea, etc., deben estar protegidos con clave. • El acceso a los sistemas de información en los que están almacenados los documentos debe estar protegido por una clave segura. • La pantalla en la que se muestra el documento debe bloquearse automáticamente luego de 10 minutos de inactividad.	• Sólo las personas con autorización para este documento pueden acceder a la parte del sistema de información en el que está guardado el documento. • Cuando se intercambian, mensajería instantánea, etc., deben estar encriptados. • Solamente el propietario del documento puede borrarlo.

Sistemas de información	• Sólo las personas autorizadas pueden tener acceso. • El acceso al sistema de información debe estar protegido por una clave segura. • La pantalla debe bloquearse automáticamente luego de 10 minutos de inactividad. • El sistema de información puede estar ubicado solamente en habitaciones con acceso físico controlado.	• Los usuarios deben finalizar la sesión en el sistema de información si abandonan temporal o permanentemente su lugar de trabajo. • Los datos deben ser borrados solamente con un algoritmo que garantice un borrado seguro.
Correo electrónico	• Sólo las personas autorizadas pueden tener acceso. • El remitente debe verificar cuidadosamente el destinatario.	• El correo electrónico debe estar encriptado si se envía fuera de la organización.
Soportes de almacenamiento electrónico	• Sólo las personas autorizadas pueden tener acceso. • Los soportes o archivos deben estar protegidos con clave. • Si es enviado fuera de la organización, el soporte debe ser enviado por correo certificado. • El soporte solamente puede ser guardado en habitaciones con acceso físico controlado.	• Los soportes y archivos deben estar encriptados. • El soporte debe ser almacenado en un gabinete con llave. • Si es enviado fuera de la organización, el soporte debe ser enviado con acuse de recibo. • Sólo el propietario del soporte puede borrar sus datos o destruirlo.
Información transmitida oralmente	• Sólo las personas autorizadas pueden tener acceso a la información. • Las personas no autorizadas no deben estar presentes en la habitación cuando se comunica la información.	• La habitación debe tener aislamiento acústico dentro de lo posible. • La conversación no debe ser grabada.

*Los controles se implementan acumulativamente; es decir, los controles para cualquier nivel de confidencialidad conllevan los controles definidos para los niveles inferiores: si se

GLOSARIO

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **DSSM:** Dirección Servicio Salud Magallanes.
- **TIC:** Tecnologías de la información y la comunicación.
- **Activo de Información:** Se entenderá por tal, todo elemento en que se registre, en que se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, procedimientos operacionales o de soporte, información de auditorías, información archivada, activos de software, activos físicos y servicios.
- **Confidencialidad:** Garantía de acceso a la información sólo por aquellas personas autorizadas a hacerlo.
- **Integridad**: Mantenimiento de la exactitud y totalidad de la información y de los métodos de procesamiento.
- **Disponibilidad:** Garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES * DIRECTOR *

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
N° 3423
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA