RESOLUCION EXENTA Nº 7919

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 CONTROL ACCESO** 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 Control Acceso

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	11-07-2018	Pablo Cona Romero	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.

INTRODUCIÓN

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Está permitido el acceso a todos los sectores físicos de la organización, excepto a aquellos para las cuales el privilegio debe ser concedido por una persona autorizada (punto "Gestión de privilegios").

Esta Política determina reglas de acceso a sistemas, servicios e instalaciones, mientras que la Política de clasificación de información define reglas de acceso para documentos y registros individuales.

OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios vinculados con esta política serán todos los funcionarios (planta, contrata, reemplazos y suplencia) personal a honorarios y terceros (proveedores, compra de servicio, etc.) que tengan acceso a los recursos de información del Servicio de Salud Magallanes y Redes Asistenciales.

DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
- NCh-ISO 27002.Of2009 - Tecnología de la Información y Código de prácticas para la gestión de seguridad de la información - INN Chile.
- Decreto N° 83, de 2004, de la citada Secretaría de Estado: Aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad del documento electrónico.
- Decreto N° 93, de 2006, de la citada Secretaría de Estado: Aprueba norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados, en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
- Decreto N° 271, de 2009, del Ministerio de Economía, Fomento y Reconstrucción: Reglamento de la inscripción de esquemas documentales en el Repositorio del Administrador de Esquemas y Metadatos para los órganos de la Administración del Estado.
- Ley 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
- Ley 19.628 de Protección de vida privada y datos.
- Ley 19.223 de Delitos informáticos.
- Ley 19.927 de Delitos de Pornografía Infantil.
- Política de Seguridad de la Información
- Declaración de aplicabilidad
- Política de Clasificación de la Información.
- Lista de requisitos legales, normativos, contractuales y de otra índole.

DEFINICIONES

Activos de información: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, Notebook, Router, Switch, impresoras, Equipos de Comunicaciones, PBX, cintas, discos, UPS, muebles etc.

ROLES/RESPONSABILIDADES

- Funcionarios: deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las directivas que se impartan a tal efecto.
- Jefe Departamento: será el encargo de autorizar los permisos de acceso y solicitar los espacios necesarios.
- Departamento TIC: se encarga de realizar el control de cumplimiento sobre las cláusulas de seguridad.
- Encargado de Seguridad de la Información: revisar, a lo menos una vez al año, que los requerimientos de confidencialidad y no divulgación definidos en este procedimiento reflejen las necesidades de la DSSM para proteger la información.
- Comité de Seguridad de la Información: tiene la facultad de suspender o eliminar los accesos a cualquier persona que represente riesgo en la confidencialidad, integridad o disponibilidad de la información.

CONTROL DE ACCESO

Reglas para el control de acceso

Las reglas para el control de acceso, estará documentado a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos.

Gestión de identidades

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. Se usará para la asignación de las credenciales de accesos a los diferentes sistemas, un formulario con el nombre del sistema, nombre usuario, contraseña temporal y la asignación de derechos al sistema y/o los servicios.

Responsabilidad de los usuarios

Todos los funcionarios o terceros que tengan un usuario en la plataforma tecnológica de la División Informática, deberán conocer y cumplir con su uso de esta Política específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios, así como políticas de protección de usuario desatendido, escritorio y pantalla limpia.

Control de Acceso a la Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.
Las reglas de acceso a la red a través de los puertos, estarán basadas en la premisa —todo está restringido, a menos que este expresamente permitido".

Política de utilización de los servicios de red

Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Controlar el acceso a los servicios de red tanto internos como externos.
- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización de acceso entre redes.
- Establecer controles y procedimientos de administración para proteger el acceso y servicios de red.

Autenticación de usuarios para conexiones externas

El departamento TIC contempla como servicios de conexiones externas SSL, VPN y primarios para funcionarios que requieran conexión remota a la red de datos institucional.

La autenticación a los servicios VPN para usuarios con conexiones externas., está documentado mediante el procedimiento — Anexo 1 Solicitud Para la Utilización del Acceso Remoto VPN".

Identificación de equipos en la Red

El departamento TIC controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y filtrado de IP y MAC.

Protección de los puertos de configuración y diagnostico remoto

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estará restringido a los administradores de red o servidores.

Los usuarios finales deberán permitir tomar el control remoto de sus equipos para el Área de Soporte, teniendo en cuenta, no tener archivos con información sensible a la vista, no desatender el equipo mientras que se tenga el control del equipo por un tercero.

Separación de redes

La División Informática utilizará dispositivos de seguridad —firewalls", para controlar el acceso de una red a otra.

La segmentación se realizará en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLANs en los equipos de comunicaciones layer 3.

Las redes inalámbricas no podrán conectarse a la red alámbricas, por restricciones de políticas a nivel de los equipos de comunicaciones layer 3.

Control de conexión de las redes

- La seguridad para las conexiones WiFi será WPA2 o superior. Dentro de la red de datos institucional se restringirá el acceso a:
- Mensajería instantánea.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

Control de enrutamiento de red

El acceso a redes desde y hacia afuera de la cumplirá con los lineamientos del numeral

Control de acceso a la red y adicionalmente se utilizaran métodos de autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.

Control de enrutamiento de red

La División Informática, proveerá a través de sus ISPs (Proveedor de Servicio de Internet) el servicio de internet institucional, el cual será administrado por el proceso de direccionamiento tecnológico y será el único servicio de internet autorizado.

Control de Acceso al Sistema Operativo

Registro de inicio seguro

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas.
- No transmitir la contraseña en texto claro.

Perfil de Usuario Estándar

El perfil de usuario estándar tiene los siguientes derechos de acceso:

Nombre del sistema / red / servicio	*Derechos de usuario estándar*
Sistemas Operativos	Permite usar la mayoría de los programas instalados en el equipo, pero no se puede instalar o desinstalar software ni hardware, eliminar archivos que son necesarios para que el equipo funcione, o cambiar opciones de configuración en el equipo que afecten a otros usuarios.
Carpetas Compartidas	Permite al funcionario tener acceso a la información solo en modo Lectura, esto nos permite mantener la disponibilidad, integridad y confiabilidad de la información.
Internet	Limita el ancho de banda consumido por Navegar de internet, por lo cual tendrá bloqueado el uso de streaming ejemplo: youtube.com, etc.

Todos los funcionarios tienen derechos de acceso de acuerdo al Perfil de usuario estándar

Perfil de usuario Administrador

El perfil de usuario Administrador tiene los siguientes derechos de acceso:

Nombre del sistema / red / servicio	*Derechos de usuario*
Sistema Operativos	Permite instalar y desinstalar programas o modificar la configuración del equipo. Este tipo de usuario es algo **sensible en materia de seguridad**
Carpetas Compartidas	Permite realizar lectura, escritura, modificar y eliminar información.
Internet	Permite la Navegación en páginas tales como youtube.com, etc.., pero también se le aplica un filtro que no permite descarga ni actualización de sistema operativo, etc..

Los siguientes cargos o áreas tienen derechos de acceso de acuerdo al Perfil de usuario Administrador:

- Departamento TIC

Bloqueo de Sesión

Después de cinco (10) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red.

Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagados al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

Control de acceso a la información

El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

Gestión de privilegios

Los privilegios respecto de los perfiles de usuario mencionados anteriormente (concesión o eliminación de derechos de acceso) son asignados de la siguiente forma:

La administración de perfiles de usuarios radica en los funcionarios administradores de cada aplicación o información y las jefaturas de división correspondientes. La responsabilidad de asignar un determinado perfil a un usuario corresponderá a la Jefatura de división solicitante o quien delegue a través del formulario de solicitud para creación / eliminación de accesos (Anexo 2). El cual puede ser enviado vía correo electrónico a tic.ssmagallanes@redsalud.gov.cl o a través de la Oficina de Partes al Departamento TIC.

Al asignar privilegios, la persona responsable debe tener en cuenta los requerimientos del Servicio de Salud Magallanes y de seguridad para el acceso (definidos en la evaluación de riesgos), como también la clasificación de la información a la que se accede con esos derechos de acceso, de acuerdo con la Política de clasificación de información.

Solo se deben conceder accesos a terceros previa solicitud del dueño del medio de procesamiento de información y el dueño de la información, y nunca antes de firmado un acuerdo de confidencialidad. Las cuentas de acceso a terceros deben tener especificados un tiempo de expiración el que debe ser controlado por el Departamento TIC.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas e información será considerado un incidente grave, por lo que debe reportarse de inmediato según lo descrito en el procedimiento.

Ante cualquier daño a un activo de información se procederá de acuerdo a lo descrito en la Política General de Seguridad de la Información (Sanciones) y Gestión de Privilegios Especiales.

El otorgamiento de accesos con mayores privilegios (por ejemplo acceso a: bases de datos, código fuente, etc.) a funcionarios que no pertenecen a las unidades del departamento TIC, debe ser solicitado por la Jefatura de la División responsable o quien delegue, al Encargado de Seguridad de la Información justificando la solicitud.

Revisiones periódicas de los derechos de acceso

Los propietarios de cada sistema de información y de las instalaciones para los cuales se requieren derechos de acceso especiales deben, según los siguientes intervalos, revisar si los derechos de acceso concedidos se mantienen de acuerdo a los requerimientos de seguridad:

Nombre del sistema / red / servicio / sector físico	***Intervalos para revisiones periódicas***
Limpieza de Active Directory: Eliminar cuentas de usuario inactivas, registrar el proceso en planilla de eliminación de cuentas.	Cada 6 meses.
Cuentas de Correo Electrónico: Eliminar cuentas de usuario inactivas, registrar el proceso en planilla de eliminación de cuentas.	Cada 6 meses.
Cambiar contraseñas de active directory y Correo Electrónico de funcionarios desvinculados laboralmente.	24 horas antes del cese de sus funciones recursos humanos debe dar aviso al departamento TIC. (formulario de creación y modificación de cuentas de usuario)
Carpetas compartidas: Verificar las restricciones de acceso a dichas carpetas.	Cada 3 meses.

Controlar el acceso a red de contingencia WIFI: Cambio de Contraseña.	Cada 3 meses
VPN: Eliminar cuentas de usuario inactivas, registrar el proceso en planilla de eliminación de cuentas	Cada 3 meses

Cambio de estado o finalización de un contrato

Cuando se produce un cambio o finalización de empleo de algún funcionario, el área de Recursos Humanos debe informar 24 horas antes al departamento TIC para bloquear los privilegios y/o accesos del funcionario en cuestión.

Cuando se modifican las relaciones contractuales con proveedores que tienen acceso a sistemas, servicios e instalaciones, o cuando finaliza el contrato, el propietario del contrato debe informar inmediatamente a las personas que autorizaron los privilegios de las entidades externas en cuestión.

Los derechos de acceso para todas las personas que han modificado su condición de empleo o relación contractual deben ser eliminados o modificada inmediatamente por las personas responsables de acuerdo a lo que se define en la siguiente sección.

Implementación técnica

La implementación técnica de la asignación o eliminación de derechos de acceso la realizan las siguientes personas:

Nombre del sistema / red / servicio / sector físico	*Persona responsable de la implementación*
Cuentas Active Directory	Departamento TIC
Cuenta Correo Electronico	Departamento TIC
Creación de carpetas compartidas y asignación de privilegios.	Departamento TIC
Subir equipos al dominio	Departamento TIC

Autoconsulta SIRH	Ximena Avendaño
SIRH	Ximena Avendaño
Reloj Control	Departamento TIC
VPN	Departamento TIC
Sala de Servidores	Departamento TIC

Las personas detalladas en este cuadro no pueden asignar ni eliminar libremente los derechos de acceso, sino solamente en base a los perfiles de usuario definidos en la presente Política y a solicitudes de personas autorizadas para asignar privilegios.

Gestión de la clave del usuario

Cuando se asignan y utilizan claves de usuarios, se deben cumplir las siguientes reglas:

- Al firmar la Declaración de aceptación de los documentos del SGSI, los usuarios también aceptan la obligación de mantener sus claves en forma confidencial, como se establece en este documento.
- Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos corresponda.
- Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo informado anteriormente.
- Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.
- El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez.
- El sistema de gestión de claves debe requerir que el usuario escoja contraseñas seguras.
- El sistema de gestión de claves debe requerir que los usuarios cambien sus claves cada tres meses.
- El usuario debe confirmar la recepción de la clave mediante correo electrónico institucional.
- La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
- Si un usuario ingresa una clave incorrecta tres veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión.
- Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.
- Los archivos que contienen claves deben ser guardados en forma separada de los datos de sistema de la aplicación.

Control de Acceso al Código Fuente.

El departamento de Tecnología de la Información y las Comunicaciones debe mantener los códigos fuentes de los programas y artículos asociados en un almacenamiento seguro, centralizado y controlado.

El control de acceso y cambios al código fuente del programa debe ser gestionado con herramientas con funcionalidades de historial de cambios, que permitan una vuelta a estados anteriores del código fuente, es responsabilidad de la unidad de Tecnología de la Información y Telecomunicaciones definir la(s) herramienta(s) que se utilizara para tal efecto

La modificación del código fuente del programa solo debe realizarse bajo supervisión y aprobación de los respetivos Jefes de Proyectos y la unidad de la Tecnología de información y Telecomunicaciones, deben mantener un adecuado registro de las modificaciones al código fuente.

Control de acceso a la información

El departamento de informática, identificará según los niveles de clasificación de información cuales sistemas considera sensibles y que deberían gestionarse desde ambientes tecnológicos aislados e independientes.

Al aislar estos sistemas se debe prever el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

Computación Móvil y Trabajo Remoto

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación se establecen directrices que permitirán regular el uso de la computación móvil y trabajo remoto:

Computación y comunicaciones móviles

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones.
El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

ANEXO N° 1 FORMULARIO PARA CREACIÓN DE VPN

Formulario Requerimiento	
ESTABLECIMIENTO	
TIPO	Seguridad
SUB-REQUERIMIENTO	VPN
ACCIÓN	HABILITAR VPN
DATOS SOLICITANTE:	
NOMBRE COMPLETO*	
RUT	
ESTABLECIMIENTO*	
TELEFONO*	
CARGO*	
FECHA	
EMAIL*	
DATOS BENEFICIARIOS:	
NOMBRE COMPLETO*	
RUT	
ESTABLECIMIENTO*	
TELEFONO*	
CARGO*	
FECHA	
EMAIL*	
DATOS TECNICOS:	
ES PROVEEDOR?	
NOMBRE DE GRUPO VPN	
FECHA DE EXPIRACIÓN	
LISTADO DE IP A ACCEDER*	
PUERTOS*	
TIME OUT VPN	
NOTA: Los campos marcados con * son de carácter obligatorio, en caso de que estos no se indiquen no se generará ticket y por lo tanto no se cursará el requerimiento. Importante: Al solicitar una cuenta VPN, esta de acuerdo con la politica de uso de VPN	
OBSERVACIÓN:	

ANEXO N° 2
FORMULARIO DE SOLICITUD PARA CREACIÓN / ELIMINACIÓN ACCESOS DSSM

Servicio de Salud Magallanes
Región de Magallanes
Ministerio de Salud

JEFATURA O ENCARGADO RESPONSABLE QUE SOLICITA AUTORIZACION DE ACCESO (Campo Obligatorio)					
Departamento o Unidad:					
Nombre:					
Cargo:				**Fecha:**	
TIPOS DE PRIVILEGIOS (Marque la opción requerida)					
Lectura		**Modificar**		**Eliminar**	

IDENTIFICACION DEL USUARIO (Campo Obligatorio)

Nombre	**Apellido Paterno**	**Apellido Materno**
Rut	**Unidad o Departamento**	**Jefe Directo**
Ciudad	**Teléfono o anexo**	

EJEMPLO DE RUTAS DE ACCESOS:

Ruta Depto. o Unidad: "\\dssmfiles\nombre departamento\nombre unidad\nombre carpeta"

RUTAS DE ACCESOS (Campo Obligatorio)

Ante cualquier duda o consulta, comuníquese con el Departamento TIC al 611159- 611160- 611161

Definiciones de privilegios:

Lectura: Listar carpetas y archivos. **Modificar:** Crear, copiar, borrar y modificar carpetas y archivos. **Eliminar**: Borrar el permiso (usuario) y los privilegios otorgados.

Firma Jefe Departamento

Uso exclusivo del Departamento de Tecnología de la Información y Telecomunicaciones

Fecha de Ejecución	**Fecha BºVº**
Ejecutado por	**Responsable BºVº**

Uso de usuario y contraseña para acceso al mismo.

- Cifrado de la información.
- Uso de software antivirus provisto por la División Informática.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por la División Informática.
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo
- No dejar desatendidos los equipos
- No llamar la atención, acerca de portar equipos móviles
- No identificar el dispositivo con distintivos de la División Informática
- No colocar datos de contacto técnico en el dispositivo
- Mantener cifrada la información clasificada
- No conectarse a redes WiFi publicas
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES * DIRECTOR * XII

MARIA CRISTINA DIAZ MUÑOZ
DIRECTORA (S) SERVICIO SALUD MAGALLANES

MCDM/OPVV/ncr
N° 3420
DISTRIBUCION:
DEPTO. SUBD. RECURSOS HUMANOS
DEPTO. CONTROL DE GESTIÓN Y TECNOLOGIA DE INFORMACION Y COMUNICACIONES
OFICINA DE PARTES

COPIA