Política de Dispositivos Móviles

1 INDICE

2 OBJETIVO

Establecer los requisitos y controles para uso y conexión de equipos portátiles y dispositivos móviles para todo funcionario del Gobierno regional Metropolitano, no importando su calidad contractual y que se le haya asignado un dispositivo móvil, para así dar un buen uso del acceso a internet y al plan de minutos asignados para contribuir al ahorro de recursos del Servicio

3 ALCANCE

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Gobierno Regional Metropolitano y que disponga de un equipo móvil facilitado por el Gobierno Regional Metropolitano.

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de hacer la entrega y velar por el buen uso de los dispositivos móviles.

Cada usuario al cual se le haga entrega de un dispositivo móvil será responsable de velar por la seguridad del equipo según indiquen las Políticas, Normas u otros documentos aprobados por el Servicio en materia de Seguridad de la Información, tal como se describen en el siguiente punto.

Todo usuario que se sorprenda haciendo mal uso de los dispositivos móviles se le solicitará la devolución del mismo y se informará al Encargado de Seguridad para su evaluación.

Todo funcionario que haga uso del Dron Institucional, será responsable de tener con su credencial de piloto a distancia al día, que le permita operar y desempeñarse como piloto a distancia de Drones o similares autorizados y registrado en su credencial.

5 CONTROL NORMATIVO SSI

La siguiente política tiene por finalidad dar cumplimiento a los siguientes controles de la norma NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.06.02.01	Política de dispositivos móviles	Se debe adoptar una política y medida de apoyo a la seguridad para gestionar los riesgos introducidos al usar dispositivos móviles.
A.11.02.05	Retiro de activos	El equipamiento, no se debe retirar del local de la organización sin autorización previa.
A.11.02.06	Seguridad del equipamiento y los activos fuera de las instalaciones	Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

6 DEFINICIONES

6.1 Hurto

En relación con la conducta, ésta debe consistir en una apropiación, que debe ser ejecutada sin voluntad del dueño de la cosa apropiada y con ánimo de lucro. En relación con el objeto material de la acción, debe tratarse de una cosa corporal, mueble, ajena, susceptible de apropiación y de apreciación pecuniaria y se realiza sin que se use la fuerza o violencia.

6.2 Robo

Es un delito contra el patrimonio, consistente en el apoderamiento de bienes ajenos de otras personas, empleando para ello fuerza en las cosas o bien violencia o intimidación en las personas

6.3 Notebook

Es un dispositivo informático que se puede mover o transportar con relativa facilidad. Los Computadores portátiles (notebook) son capaces de realizar la mayor parte de las tareas que realizan los computadores de escritorio, también llamados "de torre", o simplemente pc, con similares capacidades y con la ventaja de su peso y tamaño reducidos. Además, también tienen la capacidad de operar por un período determinado por medio de baterías recargables, sin estar conectadas a una red eléctrica.

6.4 Tablet

Una tableta, en muchos lugares también llamada por el anglicismo tablet,12 es una computadora portátil de mayor tamaño que un teléfono inteligente o un PDA (en inglés Personal Data Assistant), integrada en una pantalla táctil (sencilla o multitáctil) con la que se interactúa primariamente con los dedos o un estilete (pasivo o activo), sin necesidad de teclado físico ni ratón.

6.5 Teléfono Inteligente

El teléfono inteligente (smartphone en inglés) es un tipo de computador de bolsillo que combina los elementos de una tablet con los de un teléfono móvil sobre una plataforma informática móvil, con mayor capacidad de almacenar datos y realizar actividades, semejante a la de una computadora, y con una mayor conectividad1 que un teléfono convencional.

6.6 Sim o Tarjeta Sim

Una tarjeta SIM (acrónimo en inglés de Subscriber Identity Module, en español módulo de identificación de suscriptor) es una tarjeta inteligente desmontable usada en teléfonos móviles que se conectan al dispositivo por medio de una ranura lectora o lector SIM. Las tarjetas SIM almacenan de forma segura la clave de servicio del suscriptor usada para identificarse ante la red telefónica, de forma que sea posible cambiar la suscripción del cliente de un terminal a otro simplemente cambiando la tarjeta

6.7 Red WIFI

Es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Los dispositivos habilitados con wifi (marca de la alianza WI-Fi (tales como computadoras personales, teléfonos, televisores,) pueden conectarse entre sí o a internet a través de un punto de acceso de red inalámbrica.

6.8 Red Abierta

Es una red wifi gratuita que carece de claves o contraseña para conectarse. Se presume como una red poco segura.

6.9 Bluetooth

es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) creado por Bluetooth Special Interest Group, Inc. que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2.4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles.
- Eliminar los cables y conectores entre estos.

6.10 Freeware

El término software gratis (en inglés freeware, abreviatura de free software, a veces confundido con el "software libre" por la ambigüedad del término en el idioma inglés) define un tipo de software que se

distribuye sin costo, disponible para su uso,1 pero que mantiene el copyright, por lo que no se puede modificar o utilizar libremente como ocurre con el software libre.

6.11 Hacker

Comúnmente el término es asociado a todo aquel experto informático que utiliza sus conocimientos técnicos para superar un problema, normalmente asociado a la seguridad. Se recomienda diferenciar claramente entre hacker y cracker,9 ya que, si bien ambos son expertos en colarse en sistemas, el segundo lo hace con propósitos ilícitos

El Gobierno Regional de la Región Metropolitana proveerá las condiciones para el manejo de los dispositivos móviles (Notebooks, teléfonos inteligentes y tabletas, entre otros) institucionales y personales, que hagan uso de servicios de la institución. Así mismo, a través de su Departamento de Informática, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por el GORE, llevando un registro de los equipos móviles entregados, señalando las restricciones de su uso y pautas de manejo respecto de la información que por ellos se transfiere, en especial con las claves asignadas en lo que se refiere a su no divulgación.

Para todo esto el usuario se compromete a través de un documento de entrega del móvil a cuidarlo y responder en caso de pérdida o robo estampando su firma como signo de aprobación de estas políticas.

6.12 Dron

Dispositivo aéreo no tripulado, que en el caso de este Gobierno Regional servirá para registras imágenes y videos de las actividades autorizadas por el Servicio. Está diseñado para operar sin un piloto a bordo, capaz de sustentarse en vuelo de acuerdo a sus formas aerodinámicas, pilotada a distancia por medios de control a través de sistemas electrónicos. También podrá ser llamado RPA (Aeronave pilotada a distancia y que no lleva piloto a bordo).

6.13 GDAC.

Dirección General de Aeronáutica Civil, es un organismo civil dependiente de la Fuerza Área de Chile y que está encargada de la seguridad aeronáutica del país y la infraestructura aeroportuaria nacional.

6.14 Normas DAN

Las normas DAN, son las disposiciones que la DGAC emite en el ejercicio de las atribuciones que le otorga la Ley para regular aquellas materias de orden técnico u operacional, tendientes a resguardar la seguridad área.

6.15 Altitud

Distancia vertical entre un nivel, punto u objeto considerado como punto, y el nivel medio del mar (MSL).

6.16 ÁREAS POBLADAS

Zonas en las que existan centros urbanos, asentamientos de personas con fines habitacionales o laborales, o en las que se desarrollen actividades que convoquen la aglomeración de personas al aire libre.

6.17 ENLACE DE MANDO Y CONTROL

Enlace de datos entre la aeronave pilotada a distancia y la estación de pilotaje a distancia para fines de dirigir el vuelo

6.18 PILOTO A DISTANCIA

Persona designada por el explotador para operar los controles de vuelo de una aeronave pilotada a distancia durante el tiempo de vuelo. A falta de persona designada, se presumirá que el piloto es quien dirige la operación de vuelo.

6.19 NOTAM

Aviso distribuido por medio de telecomunicaciones que contiene información relativa al establecimiento, condición o modificación de cualquier instalación aeronáutica, servicio, procedimiento o peligro, cuyo conocimiento oportuno es esencial para el personal encargado de las operaciones de vuelo. Esta información está disponible en página Web institucional www.dgac.gob.cl /servicios online/ IFIS y/o en las oficinas ARO de los aeródromos

6.20 SOFTWARE NO AUTORIZADO

No se permitirá instalar, descargar o usar software que no se encuentre autorizado por el Gobierno Regional Metropolitano de Santiago. El software no autorizado puede introducir serias vulnerabilidades de seguridad dentro del Servicio, afectando el trabajo de todo el personal de la Institución. Está estrictamente prohibida la instalación y utilización de aplicaciones de hackeo, crackeo, gestores de descargas u otros que no sean afines a las labores habituales del personal.

El Departamento de Informática tiene bajo su responsabilidad suministrar el soporte técnico en lo que se refiere a configuración de las aplicaciones y servicios autorizados por Gobierno Regional de la Región Metropolitana, todo otro soporte es responsabilidad exclusiva del funcionario. Si el funcionario desea utilizar un equipo distinto a los asignados por el Gobierno Regional de la Región Metropolitana, este será revisado por el Departamento de Informática y deberá apegarse a las disciplinas en el uso del servicio. Igualmente, debe ser utilizado por el funcionario para realizar las funciones establecidas para su cargo y su uso debe estar orientado a agilizar las funciones inherentes al mismo.

6.21 SOFTWARE NO LICENCIADO

Se realizará un control minucioso y detallado de las licencias de software instalado en los equipos computacionales del Servicio. La mayoría del software que sea específicamente identificado como" freeware" o "de dominio público", puede ser instalado y/o usado si la licencia ha sido previamente autorizada explícitamente por la Unidad de Desarrollo y no contravenga el punto anterior. Las aplicaciones shareware o de prueba deben ser eliminadas o licenciadas una vez terminado el período de prueba

6.22 PROTECCIÓN CONTRA VIRUS EN LOS COMPUTADORES PORTÁTILES

Los virus son la mayor amenaza para los equipos portátiles y para la información en ellos almacenada, si no se tienen las precauciones necesarias. La aplicación del antivirus debe ser actualizada a lo menos una vez al mes. La forma más fácil de hacer este procedimiento, es, conectando al equipo a la red del Gobierno Regional Metropolitano de Santiago, el cuál actualizará automáticamente el equipo portátil. Si existe algún problema, contacte al Departamento de Informática y notifique el problema.

Los archivos adjuntos en los correos son una fuente de virus de computadores. Evite abrir cualquier archivo adjunto en caso de que este se encuentre en un correo electrónico de una dirección que no conozca.

Cada vez que descargue algún archivo a su equipo portátil, utilice siempre la aplicación de antivirus para revisar su contenido. Normalmente el antivirus automáticamente revisa cualquier tipo de archivo. Si desea realizar un escaneo de archivos manual o tiene dudas, podrá preguntar al Departamento de Informática.

Para reportar cualquier incidente de seguridad (ya sea virus, spam y otros) deberá comunicarse con el Departamento de Informática para minimizar los daños. No reenvíe archivos desde su computador si sospecha que éste pueda estar infectado.

Si el equipo presenta problemas de virus, se deberá notificar inmediatamente al Departamento de Informática con la finalidad de que pueda tomar las medidas correspondientes para solucionar el incidente

6.23 CONTROLES PARA ACCESO NO AUTORIZADO A LOS EQUIPOS

Deberá utilizar la aplicación de encriptación de datos que posee el equipo portátil entregado por el Gobierno Regional Metropolitano de Santiago, asegurándose de elegir una contraseña de largo razonable y que no sea común. Contáctese con el Departamento de Informática para obtener información relacionada con la encriptación en el equipo portátil. Si el equipo portátil es robado o extraviado, la encriptación provee de una protección extremadamente segura contra accesos no autorizados a la información.

Su identificación con la que ingresa dentro de la red del Servicio debe mantenerla a resguardo debido ya que pone en peligro la información de la Red. Deberá abstenerse de compartir dicha contraseña.

Los equipos portátiles asignados por el Gobierno Regional Metropolitano de Santiago son de uso exclusivos del personal, debiendo evitar el uso por familiares y/o amigos.

Evite dejar el equipo portátil con la sesión abierta. Siempre apague, bloquee (teclas Windows + L) o active el protector de pantalla con contraseña después de utilizar activamente el equipo.

6.24 ESTÁNDARES DE USO DE LA POLÍTICA DE DISPOSITIVOS MÓVILES

El Gobierno Regional de la Región Metropolitana cuenta con un plan corporativo de servicios de telefonía móvil suministrado por un operador determinado.

El Departamento de Informática es responsable de la contratación del servicio de telefonía celular con el prestador de servicios que garantice las mejores condiciones para el Servicio, en términos de prestaciones, costos, planes y cobertura.

Utilización de Internet móvil: El Gobierno Regional de la Región Metropolitana asigna servicio de Internet móvil a los funcionarios que salen frecuentemente a terreno.

Es responsabilidad de los funcionarios hacer un uso adecuado de éste servicio. Así mismo, deben acogerse las Normas de uso Navegación por internet, las cuales prohíben, entre otros, la consulta de páginas violentas, pornográficas o que atenten contra los principios, ética y moral de los funcionarios.

La asignación de los equipos móviles y planes de telefonía celular para los funcionarios se realiza de acuerdo con las responsabilidades y funciones de cada cargo.

La entrega de los equipos celulares se realiza únicamente con los accesorios originales propios de cada teléfono y de acuerdo con los modelos correspondientes al plan o servicio contratado.

El usuario al momento de recibir el equipamiento deberá firmar un acta de asignación con el detalle de los equipos recibidos, cantidad de minutos asignados y plan de internet asociado.

El Departamento de Informática tiene bajo su responsabilidad suministrar el soporte técnico en lo que se refiere a configuración de las aplicaciones y servicios autorizados por Gobierno Regional de la Región Metropolitana, todo otro soporte es responsabilidad exclusiva del funcionario. Si el funcionario desea utilizar un equipo distinto a los asignados por el Gobierno Regional de la Región Metropolitana, este será revisado por el Departamento de Informática y deberá apegarse a las disciplinas en el uso del servicio. Igualmente, debe ser utilizado por el funcionario para realizar las funciones establecidas para su cargo y su uso debe estar orientado a agilizar las funciones inherentes al mismo.

Planes de datos: Los funcionarios con plan de datos asignado, deben dar un uso racional y estrictamente laboral a este. No deben realizarse labores que generen costos adicionales ni descargar software no autorizado en los dispositivos que cuenten con plan de datos pagado por el Gobierno Regional de la Región Metropolitana. Esta estrictamente prohibido compartir el Plan de Datos con otros dispositivos móviles sin la autorización del Departamento de Informática, de realizarlo podría causar un cobro extra el cual será descontado de su remuneración.

6.25 En caso de pérdida

En el caso de pérdida, hurto, daño o deterioro del equipo o dispositivo móvil, su reposición, reparación o mantenimiento es responsabilidad del funcionario. Así mismo, el funcionario deberá llenar el formulario "notificación pérdida dispositivo móvil" que se encuentra en la Intranet Institucional en un plazo no superior a 72 horas, además deberá:

- Dejar la constancia en Carabineros de Chile, indicando si fue extravío, hurto o robo.
- Comunicarse con el Departamento de Informática señalando la pérdida.
- El Departamento de Informática se encargará de comunicar a la Unidad de Inventarios y Departamento Jurídico para que sigan los procesos correspondientes.
- Será la Jefatura directa el funcionario quien solicite formalmente otro equipamiento justificando su necesidad

6.26 CESIÓN DE LÍNEAS TELEFÓNICAS

El usuario que se cese funciones con Gobierno Regional de la Región Metropolitana, si desea continuar con la misma línea telefónica, deberá completar el formulario "solicitud de cesión de línea", existente en la Intranet Institucional. El Departamento de Informática procederá con el trámite de cesión de la línea a

modo prepago y a inscripción al nombre del funcionario, así mismo los planes serán sujetos a las tarifas comerciales del Operador móvil.

6.27 DIRECTRICES ANTES DE LA ENTREGA

El Departamento de Informática debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el Gobierno Regional Metropolitano.

El Departamento de Informática debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el Gobierno Regional de la Región Metropolitana.

El Departamento de Informática debe instalar un software de antivirus tanto en los dispositivos móviles institucionales como en los personales que hagan uso de los servicios provistos por el Gobierno Regional de la Región Metropolitana

El Departamento de Informática debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

El Departamento de Informática debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

El Departamento de Informática debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

El Departamento de Informática debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

El Departamento de Informática, siempre debe revisar los consumos de voz y datos de cada usuario al que se le ha asignado la línea, si aquellos valores sobrepasan los límites autorizados se informará a la Jefatura de la División de Administración y Finanzas para proceder al descuento de las remuneraciones si no hay una justificación al respecto.

6.28 SEGURIDAD FUERA DE LA OFICINA

Los funcionarios del Gobierno Regional Metropolitano que usen equipamiento tecnológico de propiedad del GORE, deberán tener el equipo siempre a resguardo, no conectarse a redes abiertas, como tampoco podrán instalar software que no hayan sido autorizados por el Departamento de Informática.

Para el uso de equipos computacionales y la utilización del software instalado en ellos, el Servicio reconoce, y en todas sus funciones se rige por la normativa legal vigente en lo relacionado con propiedad intelectual, derechos de autor y seguridad de la información, siendo ésta parte integral de la Política General de Seguridad de la Información del Servicio.

Será tarea de los usuarios llevar el equipo portátil al menos cada tres meses al Departamento de Informática para que la unidad de soporte pueda hacer mantención del equipo física y lógicamente, hacer las actualizaciones que corresponda y revisar el software que ha sido instalado bajo las condiciones que establece el Gobierno Regional Metropolitano.

Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

El usuario deberá proteger los dispositivos móviles contra la exposición a campos electromagnéticos fuertes, según indicaciones de los fabricantes.

7 Respecto del DRON como dispositivo móvil

El Dron es un dispositivo móvil aéreo no tripulado, que en el caso de este Gobierno Regional servirá para registras imágenes y videos de las actividades autorizadas por el Servicio. Está diseñado para operar sin un piloto a bordo, capaz de sustentarse en vuelo de acuerdo a sus formas aerodinámicas, pilotada a distancia por medios de control a través de sistemas electrónicos.

Quien opere este Dron, deberá contar con una credencial de vuelo autorizada que indique además los tipos de dispositivos que le está autorizado a volar.

Este dispositivo móvil o Dron, deberá ser operado de acuerdo a las normas emanadas por la DGCA, en especial por la DAN 91 y 151 entre otras.

Deberá estar inscrito en la DGCA en el registro especial para RPA antes de iniciar las operaciones.

Se deberá dejar detalle de las salidas y operaciones del Dron indicando, por ejemplo:

Objetivo del vuelo, piloto tiempo aproximado de duración del vuelo

Ubicación, fecha y hora

Revisiones del equipamiento

Si es actividad pública o privada, etc

y alguna observación según lo muestra el anexo 8

7.1 CONDICIONES DE OPERACIÓN

Toda persona que se encuentre operando un RPA de acuerdo a esta norma, deberá portar:

1) La tarjeta de registro del RPA.
2) La credencial de piloto a distancia de RPA.
3) La autorización de operación de RPA otorgada por la DGAC.

4)

(a) Los documentos anteriormente indicados son intransferibles.

(b) El piloto a distancia es el encargado de la dirección del RPA y responsable de la conducción segura de acuerdo a lo establecido en la presente norma.

(c) Toda operación de RPA, debe efectuarse en condiciones meteorológicas de vuelo visual (VMC).

(d) El piloto a distancia deberá, previo a iniciar un vuelo, determinar si el RPA se encuentren en condiciones seguras para operar.
(e) El RPA debe ser controlado manualmente en todas las etapas del vuelo.
(f) El piloto a distancia debe mantener permanentemente contacto visual directo con el RPA (VLOS).
(g) Un piloto a distancia durante la operación de un RPA **no podrá**:

(1) Poner en riesgo la vida de las personas.
(2) Poner en riesgo la propiedad pública o privada.
(3) Violar los derechos de otras personas en su privacidad y su intimidad.
(4) Operar en forma descuidada o temeraria que ponga en riesgo a otras aeronaves en tierra o en el aire.
(5) Operar a una distancia menor de dos (2) kilómetros de la prolongación del eje de la pista, medidos desde el umbral y a una distancia menor de un (1) kilómetro paralelo al eje de la pista de un aeródromo. (6) Operar en zonas prohibidas y zonas peligrosas publicadas por la DGAC. B.2 ED.2/SEPTIEMBRE 2015 (7) Operar en zonas restringidas, a menos que cuente con autorización de la DGAC.
(8) Operar sin tomar conocimiento de los NOTAMS vigentes publicados por la DGAC.
(9) Operar más de un RPA en forma simultánea.
(10) Operar en la noche, sin una autorización especial de la DGAC.
(11) Efectuar operaciones a una distancia mayor de 500 metros en una pendiente visual y a una altura superior a 400 pies (130 m) sobre la superficie en que se opere.
(12) Ocupar un RPA para el lanzamiento o descarga de objetos desde el aire, sin una autorización especial de la DGAC.
(13) Operar bajo la influencia de las drogas o el alcohol.
(14) El tiempo total de vuelo en una operación de un RPA, no podrá exceder el 80% de la máxima autonomía que le permita la carga eléctrica del RPA, no pudiendo durar el vuelo más de 60 minutos.

5) La operación del Dron o RPA se divide en tres etapas: Etapa 1: Pre Vuelo; Etapa 2 Vuelo; Etapa 3 Post Vuelo.

Etapa 1: Pre vuelo

a) Preparación y chequeo del vuelo
b)

- Verificar que los dos juegos de baterías se encuentren cargados
- Revisar que la radio del Dron se encuentre cargada completamente
- Verificar que el Ipad se encuentre totalmente cargado
- Revisar que el control remoto del paracaídas se encuentre totalmente cargado

- Revisar en el maletín los accesorios que estén al menos el cable cargador del Ipad, strap o correas, adaptador de enchufe y otros
- Revisar que este la carpeta de documentación y que contenga al menos: Tarjeta de registro del Dron emitida por la DGAC, la Póliza de Seguro y la autorización de vuelo emitida por la DGAC
- Efectuar inspección visual de cada hélice con su respectivo motor, soportes, para caída, antenas de GPS y cables en general.
- Revisar que la tarjeta Micro SD se encuentre instalada en la cámara de video del Dron y además que tenga espacio suficiente para efectuar las grabaciones y toma de imágenes
- Preparar y revisar el plan de vuelo que se realizará

c) Espacio de operación y condiciones del clima
- Para la operación de vuelo, deberá encontrarse en un espacio abierto y libre de obstáculos
- Debe preparar un área de restricción de al menos 9 m2.
- El área de despegue y aterrizaje, deberá encontrarse nivelada y no podrá ser tierra, agua, arena, o encontrarse con exceso de polvo ya que podría ocasionar daños en las partes mecánicas del equipo.
- No podrá volar si a nivel de piso el viento excede los 30 km/h
- No podrá operar el Dron ante las siguientes condiciones climáticas: si existe niebla, llovizna, lluvia o escasa visibilidad

Etapa 2: Vuelo

a) Despegue
Al realizar el despegue, el piloto deberá:
- Abrir y revisar todas las hélices del RPA y ajustarlas correctamente}
- Verificar que las antenas del GPS se encuentren bien extendidas, aseguradas y sin daños.
- Verificar que las luces de la batería se enciendan
- Se podrá hacer uso del despegue automático o hacerlo manualmente
- Informar inicio y término de las operaciones

b) Vuelo
- La operación del Dron deberá ser manual, debiendo en todo momento mantenerse a la vista del operador
- En l operación del Dron, no podrá excederse la altura y distancia según la autorización de vuelo de la DGAC

- Tendrá que verificarse constantemente la carga de batería a través de la aplicación de vuelo del Ipad, si la carga se encuentra en un 30% o menos, se deberá volver de inmediato al punto de despegue.
- Si existe riesgo en el vuelo, se deberá regresar de inmediato al punto de despegue o bajar el Dron procurando aterrizar en un área segura, lejana de peatones, árboles, calzadas, casas o zonas de riesgo
- Si existe un riesgo inminente de caídas por fallas mecánicas u otras causas, se deberá accionar de inmediato el sistema de paracaídas
- Se deberá informar el motivo de la emergencia.

Etapa 3: Post vuelo

Esta etapa podrá ser por cambio de baterías o por finalización del plan de vuelo

- EL piloto deberá apagar inmediatamente los motores antes de manipular el Dron
- El piloto deberá efectuar un cheque visual completo del Dron, con el objetivo de detectar posibles fallas, roturas o daños en general del Dron durante el vuelo
- Si corresponde cambio de baterías deberá dejarse una nota en el cuaderno de anotaciones para que esta sea cargada inmediatamente al llegar de vuelta a la oficina
- Si la operación termino, se deberán guardar todos los elementos en el maletín, verificando antes el estado de cada uno de ellos.
- La cámara deberá ser fijada mediante los elementos de sujeción de manera de evitar daños durante su traslado

Grabación e imágenes

Las grabaciones y/o imágenes que se realicen durante el plan de vuelo, solo podrán efectuarse en los lugares públicos definidos por la autoridad y con los fines de difusión institucionales correspondientes y en cumplimiento según lo dispuesto en la ley 18.628 respecto de la protección de la vida privada de las personas.

Los archivos digitales que contenga la memoria deberán ser bajados y guardados por un funcionario que haya sido señalado para tal efecto por el jefe de la DIPLADE.
La memoria Micro SD deberá ser limpiada y dejada lista para ser usada durante el próximo plan de vuelo.

Todo ciudadano tendrá derecho a solicitar copia de las imágenes, debiendo solicitarlo por escrito al jefe de la DIPLADE, indicando el día al que hace referencia, razón de la solicitud. Según anexo 9

8 ANEXOS

8.1 Asignación BAM.

ACTA DE ASIGNACIÓN DE DISPOSITIVO DE NAVEGACIÓN

DATOS FUNCIONARIO

Nombre de Funcionario: RUN:
Departamento: Fecha de Entrega:

Se asigna equipo Banda Ancha Móvil (BAM):

Marca_____, modelo _____, IMEI n°_____, n° de serie _____
Linea n°_____, chip n°_____ PIN_____ PUK_____

Plan de Datos

☐ 6 GB ☐ 1 GB

☐ 3 GB ☐ 600 MB

_____
FIRMA JEFE DAF

_____
FIRMA USUARIO
RECIBE CONFORME

_____
FIRMA RESPONSABLE
ADMINISTRACIÓN CELULARES

En caso de pérdida del equipo, está sujeto a una indemnización correspondiente a 2.5 UF más el costo del equipo a reponer y adicionalmente a estos la reposición de una Simcard cuyo valor es de $4.000. Deberá informar inmediatamente al Jefe del Departamento de Informática Sr. José Ignacio Gutiérrez al Teléfono 2250 9264 Celular 09-9978656, para proceder a bloquear el equipo y efectuar la reposición del mismo.

8.2 Asignación celular

DATOS FUNCIONARIO

Nombre de Funcionario: RUN:
Departamento: Fecha de Entrega:

Se asigna equipo celular:
Marca: x Modelo: x IMEI N° x, N° de serie: x, Linea N° x, chip N°: x PIN; x, PUK: x

Plan de telefonía (voz)

- ☐ Minutos ilimitados
- ☐ 1000 Minutos
- ☐ 500 Minutos
- ☐ 350 Minutos
- ☐ 250 Minutos
- ☐ 150 Minutos
- ☐ 100 Minutos
- ☐ 50 Minutos

Accesorios

☐ Cargador ☐ Manos Libres ☐ Cable USB ☐ Adaptador Micro USB

Plan de Datos

☐ 10 GB ☐ 6 GB ☐ 3 GB

FIRMA JEFE DAF
MAYURI REYES TORRES

FIRMA USUARIO
RECIBE CONFORME

FIRMA RESPONSABLE
ADMINISTRACIÓN CELULARES (S)
HECTOR SALINAS MURUA

En caso de pérdida del equipo, está sujeto a una indemnización correspondiente a 2.5 UF más el costo del equipo a reponer y adicionalmente a esto la reposición de una Simcard cuyo valor es de $4.000. Deberá informar inmediatamente al Jefe del Departamento de Informática Sr. José Ignacio Gutiérrez al Teléfono 2250 9 264 Celular 09-9978656, para proceder a bloquear el equipo y efectuar la reposición del mismo.
Los equipos móviles no deben quedar sin supervisión en lugares públicos.
Los equipos móviles asignados por el Gobierno Regional Metropolitano de Santiago son de uso exclusivos del personal, debiendo evitar el uso por familiares y/o amigos. No se permitirá instalar, descargar o usar software que no se encuentre autorizado por el Gobierno Regional Metropolitano de Santiago.

8.3 Devolución BAM

ACTA DE DEVOLUCIÓN DE DISPOSITIVO DE NAVEGACIÓN

DATOS FUNCIONARIO

Nombre de Funcionario:
Departamento:

RUN:
Fecha de Entrega:

Se recibe equipo Banda Ancha Movil (BAM):

Marca_____, modelo _____, IMEI n°_____, n° de serie _____
Linea n°_____, chip n°_____ PIN_____ PUK_____

Plan de Datos

☐ 6 GB ☐ 1 GB

☐ 3 GB ☐ 600 MB

Observaciones:_____
_____
_____
_____

_____
FIRMA JEFE DAF

_____
FIRMA USUARIO
ENTREGA CONFORME

_____
FIRMA RESPONSABLE
ADMINISTRACIÓN CELULARES

En caso de pérdida del equipo, está sujeto a una indemnización correspondiente a 2.5 UF más el costo del equipo a reponer y adicionalmente a estos la reposición de una Simcard cuyo valor es de $4.000. Deberá informar inmediatamente al Jefe del Departamento de Informática Sr. José Ignacio Gutiérrez al Teléfono 2250 9 264 Celular 09-9978656, para proceder a bloquear el equipo y efectuar la reposición del mismo.

8.4 Devolución celular

ACTA DE DEVOLUCIÓN DE EQUIPO TELEFONO CELULAR
CON PLAN DE MINUTOS Y NAVEGACIÓN

DATOS FUNCIONARIO

Nombre de Funcionario: RUN:
Departamento Fecha de Entrega:
Se recibe equipo celular:

Marca_____, modelo _____, IMEI n°_____, n° de serie _____
Línea n°_____, chip n°_____ PIN_____PUK_____

Plan de telefonía (voz)

☐ 1000 Minutos ☐ 150 Minutos
☐ 500 Minutos ☐ 100 Minutos
☐ 350 Minutos ☐ 50 Minutos
☐ 250 Minutos ☐ Otro (indicar)

Accesorios

☐ Cargador ☐ Manos Libres ☐ Cable USB

Plan de Datos

☐ 6 GB ☐ 1 GB
☐ 3 GB ☐ 600 MB

Observaciones:_____
_____
_____

_____
FIRMA JEFE DAF

_____
FIRMA USUARIO
ENTREGA CONFORME

_____
FIRMA RESPONSABLE
ADMINISTRACIÓN CELULARES

En caso de pérdida del equipo, está sujeto a una indemnización correspondiente a 2.5 UF más el costo del equipo a reponer y adicionalmente a estos la reposición de una Simcard cuyo valor es de $4.000. Deberá informar inmediatamente al Jefe del Departamento de Informática Sr. José Ignacio Gutiérrez al Teléfono 2250 9 264 Celular 09-9978656, para proceder a bloquear el equipo y efectuar la reposición del mismo.

8.5 Solicitud de cesión.

SOLICITUD CESIÓN DE LÍNEA TELEFÓNICA

DATOS SOLICITANTE

Nombre de Funcionario: RUN:
Departamento: Fecha de Solicitud:

Mediante el presente la persona anteriormente individualizada, solicita gestionar la cesión de línea telefónica en modo prepago para sí. De acuerdo a lo establecido en Política de dispositivos móviles de este Gobierno Regional.

Línea n°_____, chip n°_____PIN_____PUK_____

Fecha cese de funciones:_____

_____
FIRMA JEFE DAF

_____
FIRMA SOLICITANTE

_____
FIRMA RESPONSABLE
ADMINISTRACIÓN CELULARES

8.6 Acta de préstamos de equipo computacional

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

ACTA DE PRESTAMO EQUIPO COMPUTACIONAL
DEPARTAMENTO DE INFORMÁTICA

Nombre de Funcionario
Dependencia:
Fecha de entrega:
Fecha devolución:

EQUIPO	MARCA	PLACA N°

Uso Interno ☐ **Uso Externo** ☐

Los equipos portátiles asignados por el Gobierno Regional Metropolitano de Santiago son de uso exclusivos del personal, debiendo evitar el uso por familiares y/o amigos.
Los equipos no deben quedar sin supervisión en lugares públicos.
En caso de que el equipo necesite ser sacado fuera de las dependencias del Gobierno Regional Metropolitano, quien recibe se hace responsable por cualquier daño, hurto o mal funcionamiento del equipo, lo que deberá ser informado a la brevedad al departamento de informática.
Evite dejar el equipo portátil con la sesión abierta. Siempre apague, bloquee o active el protector de pantalla con contraseña después de utilizar activamente el equipo.
No se permitirá instalar, descargar o usar software que no se encuentre autorizado por el Gobierno Regional Metropolitano de Santiago.

En virtud del cumplimiento de los controles normativos de seguridad de la información.

_____ ENTREGA CONFORME

_____ RECIBE CONFORME

8.7 Acta de Devolución de equipos

ACTA DE DEVOLUCION EQUIPO COMPUTACIONAL

DEPARTAMENTO DE INFORMATICA

Nombre de Funcionario

Dependencia:

Fecha de Devolución:

Se realiza devolución del siguiente equipo informático (marque con una X)

NOTEBOOK		CELULAR	
Marca	Modelo	Serie/IMEI	Placa Inventario

PRUEBA DE FUNCIONALIDAD

Descripción	Calificación		Descripción	Calificación	
Pruebas On/Off	Ok	falla	Prueba de Sonido	Ok	Falla
Función S.O.	Ok	falla	Función Monitor	Ok	Falla
Función Aplicaciones	Ok	falla	Función Teclado	Ok	Falla
Unidad Optica	Ok	falla	Función Mouse	Ok	Falla
Cargador	OK	Falta	Candado	OK	Falta
bolso	OK	Falta	USB	OK	Falta
Otras Observaciones					

Entregado por	Recibido por
Nombre y Cargo	Nombre y Cargo

8.8 Plan de Vuelos

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**GOBIERNO REGIONAL METROPOLITANO – SSI** **Anexo Plan de vuelo** **DRON Institucional**	Anexo 8

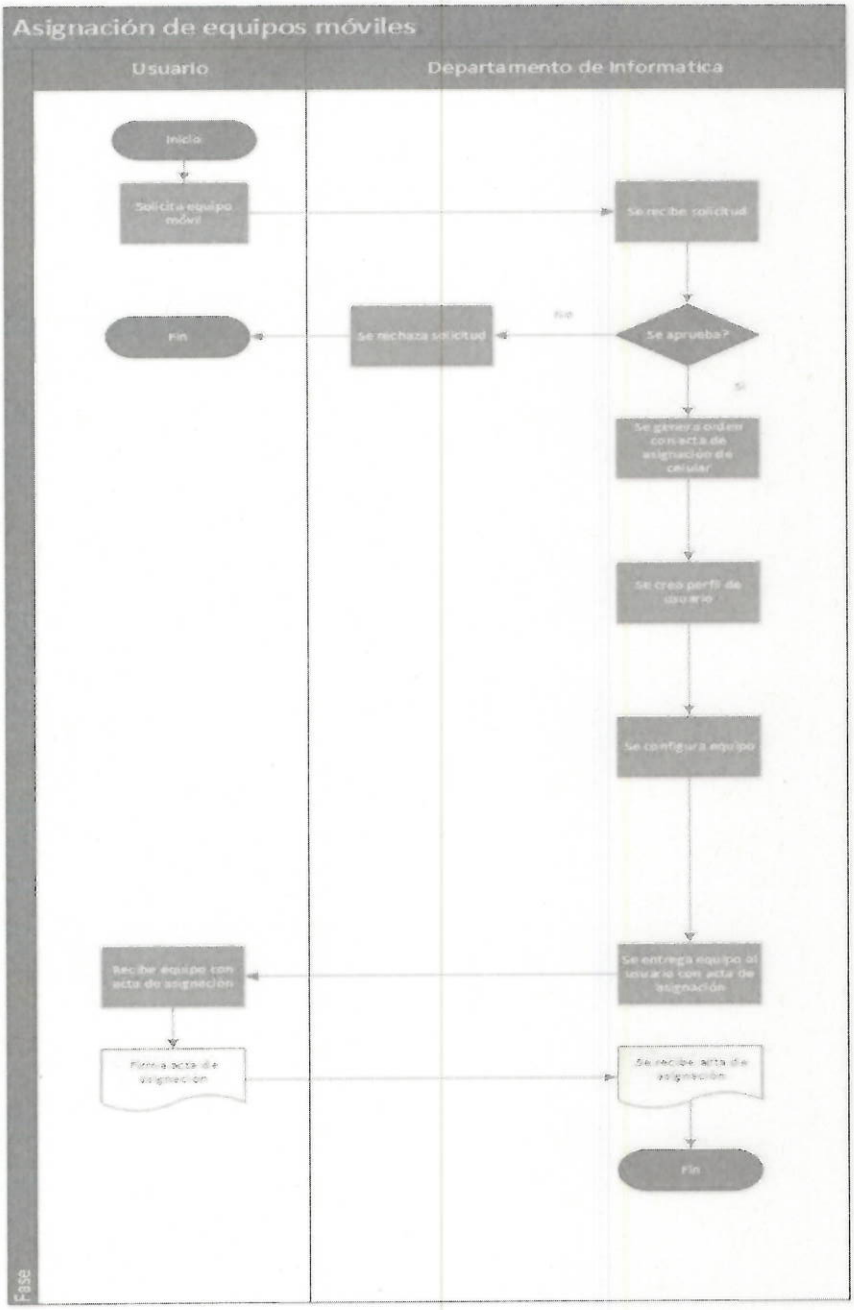
Objetivo del Vuelo:	
Ubicación:	
Fecha:	
Hora	
Piloto:	
Tiempo aproximado de duración del vuelo:	
Actividad Publica: Si____ No____	
Clima:	
Revisión de Equipamiento:	
Baterías	
Hélices y Antenas	
Cámara y Memoria Mico SD	
Cables	
Ipad	
Cargadores	
Observaciones	

Nombre del Solicitante:	
Rut:	
Domicilio	
Comuna	
Fecha del vuelo	
Tiempo aproximado de duración del vuelo:	
Actividad Publica: Si_____	No_____
Razon de la solicitud	
Autoriza solicitud	
Copia realizada por	
Medio de almacenamiento	
Observaciones	

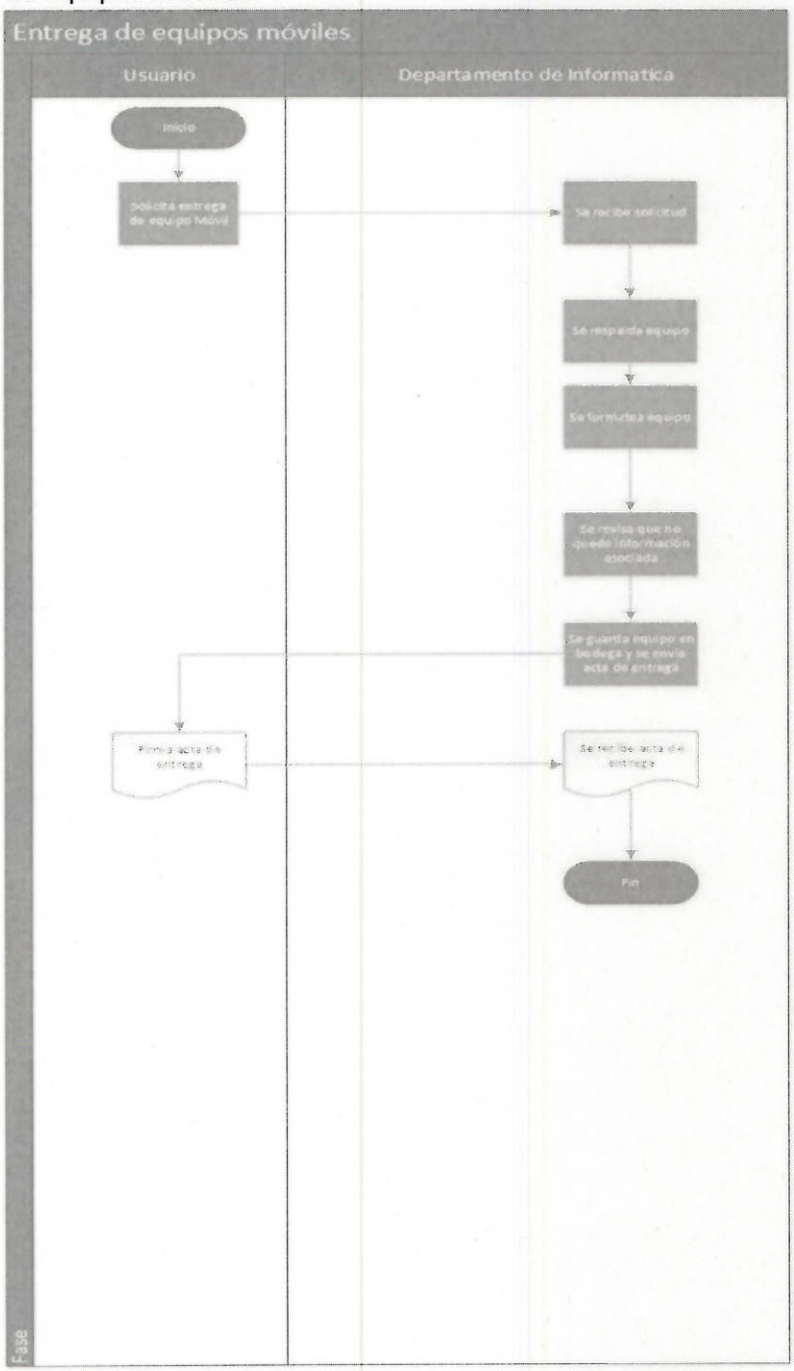
AUTORIZADO POR

RETIRADO POR

9 Flujo de asignación de equipos móviles



Flujo entrega de equipos móviles



10 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

11 PERIODICIDAD DE EVALUACION Y REVISIÓN

La siguiente Política será revisada, evaluada y/o actualizada según corresponda y aprobada su vigencia una vez al año por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

12 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política de dispositivos móviles.

13 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	11-08-16	Creación Documento
02	Carlos Hernández	todas	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control
03	Mauricio Marín	14 ,15	07-11-17	Incorpora flujos de asignación y entrega de equipos
04	Mauricio Marín	todas	19-02-18	Se agrega control A11.02.05 y se funde con Norma de Uso para los equipos tecnológicos portátiles Res. Ex N° 3044 del 22/12/18
05	Mauricio Marín V.	todas	2/08/2018	Se cambia título 7 por Registro de Operaciones Se cambia título 9 por Periodicidad de Evaluación y Revisión Se agregan Definiciones Se cambia título de Registro de Control por Registro de Operaciones Se cambia título de Revisiones por periodicidad de evaluación y revisiones
06	Mauricio Marín V.	todas	20/11/2018	Comité de Seguridad hace revisión de documento para el año 2018
07	Mauricio Marin V.	todas	14/02/2019	Se agregan definiciones y operaciones del Dron Institucional
08	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Política de dispositivos móviles año 2019.

09	Carlos Hernández	29	17-11-2021	Se agrega capítulo 12 formalización externa
10	Carlos Hernández	todas	23-11-2021	Comité SSI revisa y aprueba año 2021

14 FORMALIZACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A Analista Departamento de Informática	**José Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza R.** Encargado Unidad de Soporte **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Mayuri Reyes T.** Presidente Comité de Seguridad

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE REUNION COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 3 Fecha 23/11/ 2021

ACTA DE REUNION: Comité de Seguridad de la Información	
Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	Sala de Reunión 2° Piso

PUNTOS DE LA REUNION

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
    a. Caída de Switch piso 5 - 13 de septiembre 2021
    b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
    a. Switch
    b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

Aprobación los siguientes documentos

1. **Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio**
2. **Manual de gestión de archivos**
3. **Norma de acceso a la Red**
4. **Norma de Eliminación de Activos**
5. **Norma de la Seguridad de la información para la Gestión de Proyectos**
6. **Norma de Outsourcing**
7. **Norma de Trabajo Remoto**
8. **Norma de uso identificación y autentificación**
9. **Norma de uso de instalación legal de software**
10. **Norma de reutilización y devolución de activos**
11. **Plan de Continuidad**
12. **Plan de emergencia Institucional**
13. **Política clasificación de activos**
14. **Política de acceso físico**
15. **Política de correo electrónico e Internet**
16. **Política de Derechos de propiedad Intelectual**
17. **Política de desarrollos de sistemas**

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

DESARROLLO DE LA PRESENTACION

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.

Comité solicita que los mensajes de los protectores de pantalla sean un poco más "Rudos" refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas

Silvana Torres entrega información

- **Acerca del expurgo de documentos**
- **2022 se enviará soporte en papel a archivo nacional**
- **Se está digitalizando documentación antigua**
- **Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808**

José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando

Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI

Se aprueban políticas y documentación SSI

Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE ASISTENTES COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 1 Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			