Ministerio de Defensa Nacional
Dirección General Marítima
Autoridad Marítima Colombiana

POLITICA

POLITICA DE SEGURIDAD INFORMATICA DE DIMAR

Proceso/Subproceso: GOBIERNO Y GESTIÓN DE TIC´S

Código: A3-00-POL-001

Versión: 1

DEFINICIONES

Auditoria: Proceso por el que se lleva a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

Bases de Datos: Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

Confiabilidad: Está determinada por el posible daño, como resultado de una operación del sistema de información realizada en forma incorrecta, incompleta, impropia o inoportuna.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria, es una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

Contraseña o Clave: Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso. Las claves suelen tener limitaciones en sus caracteres (no aceptan algunos) y su longitud.

Desarrolladores de Sistemas: Funcionarios quienes “en representación del usuario” seleccionan, desarrollan y dan mantenimiento a los sistemas automatizados.

Dueño (Propietario) del Sistema: Funcionario responsable por la definición y aceptación de los requerimientos para el desarrollo y mantenimiento de los sistemas automatizados y con autoridad sobre su uso.

Estándar: Patrón uniforme o muy generalizado de un procedimiento establecido.

Funcionarios: Personal contratado por DIMAR, indistintamente de estar nombrado en propiedad, subcontratado o en entrenamiento.

Gerente del Proyecto: Funcionario responsable de coordinar las actividades administrativas relacionadas con el proyecto y su ciclo de vida (análisis, pruebas, capacitación, implementación, paralelos y otros).

Líder técnico: Analista de alto nivel contratado con amplia trayectoria en análisis, responsable de brindar apoyo técnico al director del proyecto y de coordinar las diferentes instancias ante la DIMAR en el desarrollo de un proyecto.

Mejor Práctica (Buena Practica): Corresponde a un modelo completamente definido, cuyos buenos resultados operacionales están comprobados y que está disponible para ser utilizada.

Política: Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. También puede definirse como una manera de ejercer el poder con la intención de resolver o minimizar el choque entre los intereses encontrados que se producen dentro de una sociedad.

Política de Seguridad Informática (PSI): Una política de seguridad informática es una forma de comunicarse con los usuarios. Las políticas de seguridad informática (PSI) establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que deseamos proteger y el porqué de ello. Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

Procedimiento: Sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación.

Red LAN: Red de Área Local (Local Área Network).

Red WAN: Red de Área Ancha (Wide Área Network).

Sistemas críticos: Sistemas fundamentales para la operación de DIMAR y la presentación de los servicios básicos a los usuarios.

Software de aplicación: Es aquel destinado a satisfacer las necesidades funcionales de los usuarios, este puede ser desarrollado tanto interna como externamente.

Usuario: Es aquel funcionario que tiene relación directa con la entidad, Ya sea funcionario, contratista o Tercero

ANTECEDENTES

Las Tecnologías de Información y comunicaciones se encargan del servicio directo al usuario, en materia de informática, desde el equipamiento, instalación, alteración, cambio de lugar, programación, en todo el territorio nacional de jurisdicción; por lo que ha sido necesario emitir políticas particulares para la red de DIMAR, que es el nombre oficial de un conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a cada proceso y/o subproceso que se lleva en la entidad. Así pues este documento contiene una clasificación de estas políticas.

Es responsabilidad de la DIMAR, por medio de los dueños de los procesos y propietarios de la información, asegurar una adecuada segregación roles, responsabilidades y funciones dentro de su estructura organizacional para el uso de las herramientas tecnológicas e informáticas, las cuales deben estar adecuadamente asignadas al personal calificado. Es responsabilidad de la DIMAR asegurar que los derechos de acceso de sus funcionarios a los sistemas de información y recursos informáticos, estén de acuerdo, y permanezcan actualizados con el nivel de autorización asociado a sus funcionarios y le permitan desarrollar adecuadamente su trabajo.

CONSIDERACIONES GENERALES

- Los encargados de las áreas de Informática en el ámbito nacional deberán de emitir en coordinación con GRUINCO los planes de contingencia que correspondan a las actividades críticas que realicen en caso de que el Sistema, Aplicativos y servicios en general tenga algún fallo.
- Debido a los niveles de calificación de la información, el personal de GRUINCO -DIMAR deberá comportarse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos, por GRUDHU y SUBAFIN, así como tener la ficha de autorización con el perfil de manejo de información.
- El oficial de Seguridad de la Información, así como la oficina de Seguridad Física de DIMAR deberán ser informados de los eventos asociados de Seguridad y Física, para que se impartan las medidas de control.
- Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.
- Se prohíbe totalmente la publicación de datos sensibles de personal de DIMAR, así como fotografías que atenten contra la reputación, imagen y buen nombre de las personas.
- El uso inadecuado de los recursos tecnológicos o incumplimiento a alguna de las presentes políticas dará lugar en primera instancia a llamado de atención por parte de la coordinación de GRUINCO (según informe del grupo de plataforma Redes y Seguridad Informática); de persistir y de reincidir se suspenderán los servicios a los usuario implicado, y se informará a las segundas instancias GRUCOG y GRUDHU, por el incumplimiento de las políticas de la entidad. En caso de considerarse el incumplimiento de mayor gravedad, se llevaran los debidos procedimientos descritos en el régimen de control interno.

POLITICA DE SEGURIDAD INFORMATICA

La Dirección General Marítima -DIMAR- a través del Proceso A3 - Gobierno y Gestión de TICs bajo responsabilidad del Grupo de Informática y Comunicaciones -GRUINCO- se compromete a proteger la información institucional que se genera, circula, procesa y almacena por medios digitales.

El Grupo de Informática y Comunicaciones -GRUINCO- liderará la revisión, cumplimiento y mejoramiento continuo de la seguridad informática, y generara la documentación necesaria como procedimientos, manuales, instructivos y demás elementos que sean necesarios para tal fin.

Las políticas relacionadas a la Seguridad de la Información como son el presente documento, la Política de Seguridad Física y la Política de tratamiento de datos personales deberán ser difundidas a todo el personal involucrado en su definición.

REGLAMENTO DE SEGURIDAD INFORMATICA

RESPONSABILIDADES

- Equipo de Seguridad de la Información: Velar por el cumplimiento de la presente política, garantizando los niveles de seguridad adecuados para el uso de los dispositivos móviles institucionales.
- Coordinador Grupo Informática y Comunicaciones: Designar el personal idóneo para que establezca y configure los dispositivos, redes de datos, elementos de seguridad, estaciones de trabajo y demás elementos que hagan parte de la red de datos y servicios digitales de la Dirección General Marítima, acogiendo los lineamientos de seguridad definidos en la presente política.
- Personal: Hacer uso responsable de los dispositivos móviles acogiendo los lineamientos establecidos por la DIMAR.

GENERALIDADES

- Los usuarios de los servicios se regirán por los lineamientos técnicos establecidos por GRUINCO.
- Todo funcionario es responsable de reportar inmediatamente las anormalidades e incidentes de seguridad que observe en los sistemas, tanto a su superior jerárquico como al Grupo de Informática y Comunicaciones GRUINCO.
- Las modificaciones a los datos e información de los sistemas en producción deben estar estrictamente restringidas a las transacciones y procesos expresamente diseñados para tal fin.
- DIMAR, en coordinación con GRUINCO debe definir un responsable para la administración de cada red LAN en las sedes a nivel nacional, cuyas funciones y tareas estén claramente definidas y delimitadas, en apoyo de la empresa encargada del mantenimiento preventivo y correctivo de los equipos de cómputo en cada sede, Capitanía o centro.
- Todo el equipo Informático (computadoras, estaciones de trabajo, estaciones gráficas, servidores y equipo accesorio, dispositivos móviles, tabletas, Smartphone), que esté o sea conectado a la Red de DIMAR, o aquel que en forma autónoma se tenga y que sea propiedad de la institución, o que use la red de datos de la entidad debe sujetarse a las normas y parámetros de instalación y configuración que emita la Dirección Marítima.
- GRUINCO, o quien hagas sus veces o cumpla tales funciones en las regionales, deberá tener un registro en donde se asocie el usuario con la estación de trabajo, la dirección IP y el perfil de navegación asignado.

- El Encargado de Control de Activos deberá tener un registro de todos los equipos propiedad de DIMAR y debidamente ingresados en el sistema de inventarios SAP - SILOG, este deberá contener el nombre del funcionario que tiene a cargo el equipo o recurso tecnológico en el inventario fiscal debidamente actualizado.
- El personal (personal de planta, contratista o tercero) que tenga como finalidad de su contrato la prestación de servicios y/o administración de plataforma tecnológica, redes de comunicaciones o responsabilidades relacionadas con el funcionamiento y administración de la red de datos de la entidad, estará bajo órdenes y mando del Coordinador del Grupo de Informática y Comunicaciones.

CONTROL DE ACCESO

1. Cada usuario debe tener una identificación única e intransferible dentro del sistema de control de accesos. La combinación de usuario y “clave” deben ser únicos.
2. Los nombres de usuario y “claves” son personales e intransferibles, y solamente deben ser utilizados por el funcionario al que le fueron asignados. Está totalmente prohibido que un funcionario autorice el uso de clave a terceros o que preste sus credenciales de acceso.
3. Todo funcionario será responsable de las actividades y transacciones que sean realizadas con su “usuario y clave” de carácter confidencial.
4. Los derechos de acceso de los usuarios a las transacciones específicas de cada uno de los sistemas de información deben estar formalmente autorizados por la DIMAR a través del Grupo de Informática y Comunicaciones bajo cuya responsabilidad trabaja el usuario.
5. Los derechos de acceso deben ser asignados de tal forma que no interfieran con las actividades o datos privados de otros usuarios.
6. Al asignarse por primera vez la “clave” a un funcionario debe realizarse su cambio en forma inmediata.
    a. Para la “clave” y nombre de usuario, deberá tener en cuenta lo siguiente:
    b. Las “claves” de usuario deben ser alfanumérica, contener caracteres especiales y una longitud no menor a 8 (ocho) sin utilizar espacios en blanco.
    c. Deben contener tanto caracteres alfabéticos como numéricos. Deben contener al menos 4 (cuatro) caracteres distintos entre sí.
    d. No deben estar basados en palabras de un diccionario, para no ser fácilmente descifrados. NO deben revelarse bajo ninguna circunstancia.
    e. No se deben utilizar “claves” previamente utilizadas.
    f. El nombre de usuario y la “clave” deben ser diferentes entre sí.
7. No se deben utilizar claves con información fácilmente identificable como, fecha de cumpleaños, nombres de familiares y apellidos, números de identificación, y/o demás información personal evidente.

8. Se debe mantener en un sobre sellado y bajo la responsabilidad de la Coordinación de GRUINCO un código de usuario de contingencia y respectiva “clave” que posea todos los privilegios del Administrador de la Red, Administrador de Base Datos, Administrador de Sistemas de Información u otros, para ser utilizado solamente en caso de emergencia. En caso de requerir su uso debe quedar debidamente registrado. La “clave” debe ser cambiada periódicamente mínimo dos veces al año.
9. Debe mantenerse activo el cambio automático de “clave”, según las políticas establecidas en el directorio activo; Es responsabilidad de todos los funcionarios cambiar su “clave”.
10. El Grupo de Informática y Comunicaciones deberá revisar al menos 02 (Dos) veces al año los derechos de accesos conferidos a los usuarios administradores de los sistemas bajo su responsabilidad grupos de privilegios (incluye personal de la propia oficina, personal técnico, auditor y cualquier otro que lo requiera), verificando que los derechos asignados se ajustan a las funciones y tareas de cada funcionario, previa verificación con el Jefe o Coordinador de área, para esto deberá registrarse en el sistema asignado para tal fin.
11. GRUINCO es responsable de dejar deshabilitados los derechos de acceso de aquellos funcionarios que presenten novedades de personal (incapacidad, permisos, traslados y otros), basándose en la información o novedades reportadas por el Grupo de Desarrollo Humano -GRUHDU- o La Maestría de Armas. En caso de requerir el acceso a la cuenta del usuario, el Jefe Directo o Supervisor del Contrato autorizará si así lo requiere los nuevos accesos del personal de remplazo de los privilegios que fueron suspendidos temporalmente hasta el regreso del titular.
12. El tiempo de acceso a los sistemas debe permitirse dentro de un horario particular de acuerdo con las necesidades de la oficina, en caso de requerirse las jefaturas deberán estar informadas de los horarios extendidos.
13. Las cuentas de usuario que permanezcan inactivos por más de 30 (treinta) días deben quedar deshabilitados. Podrán ser activados nuevamente mediante solicitud formal del funcionario facultado para tal efecto; siendo que está totalmente prohibido el uso de la cuenta por otro funcionario, salvo autorización expresa de las Subdirecciones, Coordinaciones o Jefes de área, mediante formato establecido “Solicitud de Servicios Informáticos”.
14. Los privilegios especiales del sistema operativo o software utilitario, que permitan examinar el contenido de los archivos de otros usuarios, deben restringirse únicamente a aquellos usuarios responsables de la administración de la red y su seguridad Informática de la entidad, siempre que hayan recibido el entrenamiento adecuado y en caso estrictamente necesario por labores de monitoreo y control.
15. El control de acceso a cada sistema de información de DIMAR será determinado por el Proceso, Dependencia y/o Grupo responsable de generar y procesar los datos

involucrados, y su autorización se realizara a través de los formatos establecidos de solicitud de servicios informáticos.

16. Tendrá acceso a los sistemas administrativos solo el personal de DIMAR que tenga la autorización de la Subdirección Administrativa y el Área respectiva.
17. No se deben dejar nombres de usuario y “claves” escritos en lugares donde puedan ser vistos o tomados por terceros (por ejemplo en la carpeta del escritorio, pantalla del equipo, bajo el teclado… etc.).
18. Los usuarios no deben dejar desatendidas las estaciones de trabajo. Todo funcionario es responsable de desactivar las aplicaciones (cerrarlas) de ser necesario, cada vez que se ausente de su puesto de trabajo, y dejarla bloqueada con contraseña.
19. Todo equipó Portátil, Tablet, cámara Fotográfica, USB propiedad de terceros contratistas y/o visitantes, deberá ser registrado en la guardia (recepción) de cada unidad, así mismo deberá ser inspeccionado su contenido, si el mismo va hacer conectado a la red de DIMAR, esta inspección deberá ser realizada por personal de GRUINCO en sede central, en las unidades personal de sistemas o el personal Oficial o Suboficial de guardia.

INTERNET

1. El acceso a Internet e Intranet, es una herramienta de trabajo que provee la Institución a sus funcionarios, por lo tanto, es responsabilidad de cada usuario, utilizar prudente y apropiadamente este servicio.

2. Todo evento que se dé a través del uso de este servicio, será administrado, monitoreado y regulado por el área de Plataforma, Redes y Seguridad Informática el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información de DIMAR, así mismo, reportará a la Coordinación GRUINCO cualquier uso indebido del servicios, y se creará el Incidente de seguridad informática de requerirse a través de los formatos establecidos.

3. Se prohíbe el acceso a sitios de Internet que no tengan relación alguna con los objetivos institucionales, tales como los relacionados con: sexo, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas y sanitizacion de la red.

4. Desde GRUINCO se crearan y monitorearan perfiles de navegación con la finalidad de brindar a los usuarios medios de acceso y consulta a Internet. Dichos perfiles son:

    a. Bajo: Navegación únicamente a dominios:

        - Gubernamentales (GOV + BOB)
        - Militares (MIL)
        - Educativos (EDU)

    b. Medio: Navegación con bloqueo categorías:

        - Media & Streaming
        - Redes Sociales
        - Correos electrónicos personales
        - News & Media
        - Compartición de Archivos
        - Shopping and auction
        - TV y Radio

- Lencería
- ChatWeb

Aplicativos Bloqueo:

- Evasion y proxies
- Skype
- Acceso Remoto
- P2P
- File sharing (Dropbox, OneDrive, Google Drive)

c. Alto: Navegación con bloqueo categorías

- Media & Streaming
- Redes Sociales
- News & Media

Aplicativos Bloqueo:

- Evasion y proxies
- Acceso Remoto
- PSP

d. Vip: Sin restricciones de navegación, solamente

5. La asignación de perfiles de navegación será previo análisis de necesidad y autorización del Jefe de Dependencia o Unidad.

6. No se autoriza a los funcionarios acceder a sitios para el establecimiento de charlas, salvo que tengan relación alguna con las funciones que desempeña. En caso de que el funcionario requiera charlas o intercambio de mensajes de texto, deberá hacer uso de los recursos brindados por la entidad.

7. Sólo personal previamente autorizado podrá “descargar” información desde Internet (incluye software gratuito y de uso temporal), con fines investigativos, prueba, o de apoyo en el desarrollo de actividades, test que se realizaran controladamente y bajo la supervisión y monitoreo del área encargada.

8. Toda información descargada de Internet debe estar relacionada con los objetivos misionales, gerenciales y/o de apoyo de DIMAR y las funciones que lleva a cabo el usuario.

9. Todos los archivos obtenidos de la red Internet deben ser revisados (filtrados) para detección de virus previo a ser descargados en cualquier computador, para ello debe estar instalado en todas los PC de DIMAR el antivirus Corporativo.

10. El tiempo de acceso a Internet no debe interferir ni distraer a los usuarios de sus funciones normales.

11. La actualización de versiones de software por medio de Internet no está permitido; solo las actualizaciones Windows update que realiza Microsoft por su sistema operativo, u otras que la Dirección General Marítima a través de GRUINCO expresamente haya autorizado a la empresa encargada del mantenimiento preventivo y correctivo del equipo de cómputo.

12. Periódicamente se deben generar reportes que muestren entre otros: información acerca del nombre de sitios visitados, duración, estaciones desde las cuales se accedió al servicio y cualquier otra que se estime conveniente, cualquier anomalía deberá ser reportada a la Coordinación GRUINCO.

13. El establecimiento de conexiones directas entre sistemas internos, equipos de DIMAR y computadoras de organizaciones externas, vía Internet, VPN, Accesos remotos o cualquier otra red pública está prohibido. Salvo en los casos ya estipulados y las concesiones realizadas entre el MDN, ARC y demás Organismos, en caso de ser necesario, esta conexión deberá ser analizada y aprobada por GRUINCO previo análisis de la herramienta a utilizar quienes valoraran la necesidad y conveniencia, así como los mecanismos de seguridad pertinentes.

CORREO ELECTRONICO

1. El Correo Electrónico, es una herramienta de trabajo que provee la Institución a sus funcionarios, por lo tanto, es responsabilidad de cada usuario, utilizar prudente y apropiadamente este servicio.

2. Todo evento que se dé a través del uso del Correo Electrónico, será administrado, monitoreado y regulado por el área de Plataforma, Redes y Seguridad Informática el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información de DIMAR, así mismo, reportará a la Coordinación GRUINCO cualquier uso indebido del servicio, y se creará el Incidente de seguridad informática de requerirse a través de los formatos establecido.

3. El contenido de los mensajes creados, enviados, recibidos y almacenados debe limitarse a los propósitos Misionales y/o Operativos de DIMAR, su contenido debe ser respetuoso y no debe atentar contra la imagen ni integridad moral de sus funcionarios y usuarios.

4. Queda totalmente prohibido enviar mensajes de correo electrónico masivos por parte de personal no autorizado. Tales permisos quedan reservados para los coordinadores de grupo, capitanes de puerto o áreas de comunicaciones internas de la entidad.

5. Las cuentas de correo electrónico institucional deberán ser usadas solamente para fines laborales; No para suscripción de servicios y/o listas de correo relacionadas con temas personales.

6. El tamaño de los archivos que circulan por correo electrónico o a través de los canales de comunicación, así como el espacio del buzón asignado a cada usuario para el almacenamiento de estos archivos, se hará con base en las necesidades de los usuarios, mediante la definición de perfiles, así mismo cada usuario está obligado a tener en su equipo un archivo de almacenamiento de correos .PST, con la ayuda de personal GRUINCO con el fin de optimizar espacio en los servidores de correo y cumplir con las normas de sanitizacion del espacio, así como las estaciones de trabajo, cuya capacidad no afecte la operación normal de su buzón.

7. La información que se haya definido como sensible por DIMAR se puede transferir por medio de correo electrónico solamente si existe la necesidad real de transferir la información.

8. Debe existir un permiso de parte del dueño de la información que se va a transferir, siempre bajo el monitoreo y supervisión de GRUINCO.
9. Los mensajes creados, enviados, recibidos o almacenados no deben ser impresos, especialmente los configurados como de carácter reservado o confidencial, salvo que sea estrictamente requerido o necesario.
10. Los usuarios NO deben acceder a cuentas de correo personal desde la red de datos de la entidad; En caso de requerir una cuenta de contingencia o enviar un mensaje de cuenta diferente a la inicialmente establecida por DIMAR, deberá solicitar la cuenta en el dominio @dimarnet.mil.co.
11. DIMAR cuenta con herramientas de protección del servicio de correo electrónico, sin embargo, los usuario NO deben abrir mensajes de los cuales desconoce su origen o propósito; En caso de recibir un mensaje de dudosa procedencia, deberá solicitar al Plataforma, Redes y Seguridad Informática su análisis antes de darle tratamiento.
12. La información alojada en la cuenta de correo de cada uno de los usuarios es responsabilidad de los usuarios, quienes en caso de llegar a la capacidad de almacenamiento de la misma o tener archivos históricos, deberá pedir asesoría a GRUINCO para las copias de seguridad y preservación de la información.

USO DE DISPOSITIVOS MÓVILES

Los dispositivos tipo PC Portátil, laptop, notebook o similar se regirán bajo la política de seguridad informática y el reglamento de seguridad Informática; Las presentes directrices solamente aplican a teléfonos inteligentes, tabletas y asistentes personales y/o dispositivos con Sistema Operativo IOS y/o Android.

En cualquier momento el equipo de Seguridad de la Información de la Dirección General Marítima podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.

Las Auditorías internas o de tercera parte pueden realizar la verificación de las configuraciones de los equipos móviles y su cumplimiento con los lineamientos de esta política.

Para el uso de dispositivos, GRUINCO debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de

respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad dela información.

La Dirección General Marítima pone a disposición de algunos miembros del personal dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos.

Con el fin de dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir las directrices consignadas en el Reglamento de uso de Dispositivos móviles.

GRUINCO deberá contar con un listado actualizado en donde se relacione:

- Identificación del Dispositivo Móvil (Marca, Modelo, Serial, IMEI)
- Numero celular asignado
- Nombre de responsable del Dispositivo
- Listado de Software Instalado
- Ubicación Física (Unidad)
- Detalle de configuración de las cuentas de correo configuradas en el dispositivo (Conexión con Exchange Institucional) y administración y gestión remota para borrado en caso de emergencia.

USUARIO DISPOSITIVO MOVIL

El personal que haga uso del dispositivo móvil asignado por la Dirección General Marítima, deberá:

1. Antes de empezar a usar el equipo, el usuario deberá leer y aceptar la política de seguridad Informática y el reglamento de Seguridad Informática, como evidencia de lo anterior, deberá firmar dichos documentos y hacerlos llegar a GRUINCO por medio de correo electrónico.
2. Mantener la configuración del dispositivo, los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.
3. NO almacenar información personal en los dispositivos móviles asignados por la Dirección General Marítima.
4. Está prohibido realizar instalación de aplicaciones no autorizadas por GRUINCO.
5. Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.

6. Se autoriza el uso de WhatsApp, sin embargo, no se permite por esta aplicación el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

QUIEN CONFIGURA DISPOSITIVO MOVIL

1. Se deberá validar que el dispositivos tenga instalado y configurado un software de antivirus.
2. Se debe establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
3. Se debe configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
4. Se debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
5. Es necesario realizar el cifrado del dispositivo móvil.
6. Configurar sólo las cuentas organizacionales en los dispositivos de la Dirección General Marítima que tendrán acceso a la información de la Entidad.
7. En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la Dirección General Marítima, se debe reportar la perdida a la Oficina de las TIC lo más pronto posible.

SISTEMAS DE INFORMACION

1. La instalación, diseño, creación y uso de los sistemas de información se rigen por el las solicitudes realizadas a través de los formatos establecidos para tal fin, y bajo los parámetros de seguridad que se establezcan en los documentos de solicitud existentes.
2. Todos los sistemas de información, herramientas de datos (programas, bases de datos, sistemas de información, interfaces y demás) desarrollados con o a través de los recursos de DIMAR se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo, incluyendo sus diseños, fuentes, documentación y demás aspectos de desarrollo.
3. Todos los Sistemas de Información deberán ser desarrollados y documentados de acuerdo con la metodología estándar definida por la DIMAR – GRUINCO, basados en el área de proyectos fichas de concepto técnico GRUINCO, así mismo coexistir con protocolo IPv6 a nivel de capa de Red y Transporte.
4. Para todos los sistemas de información, la seguridad debe ser considerada como obligatoria desde el inicio del ciclo de vida. Así mismo deben ser realizados las pruebas

de vulnerabilidades y seguridad que la Coordinación de GRUINCO a través del área encargada considere pertinentes y no se pondrán en producción hasta tanto no se hayan corregido las vulnerabilidades existentes.

5. Durante cada fase del proceso de desarrollo de sistemas, mantenimiento y ajustes, los aspectos de seguridad deben ser definidos explícitamente, documentados por el equipo de desarrollo y establecidos como un requerimiento de seguridad específico.
6. En la fase inicial de definición del proyecto, de un nuevo sistema, deberá asignarse el "titular" del sistema, en cumplimiento de las responsabilidades básicas en seguridad informática, así mismo estipular los formatos de seguimiento y control de cambios para este tema GRUINCO, a través del área de Sistemas de Información, deberá trabajar en PRO de la Calidad del Software, validaciones a través del ciclo de vida de una aplicación.
7. Al inicio de la fase de diseño del proyecto deberá realizarse un análisis de riesgos del nuevo sistema por parte o en representación del "Gerente de Proyecto", a fin de clasificarlo de acuerdo con su continuidad, confiabilidad y confidencialidad. Para esta evaluación se utilizará como guía el documento denominado "Sistema de Valoración del Riesgo" elaborado por el grupo de Sistemas de Información con el apoyo del Grupo de Planeación y Control Interno.
8. DIMAR, con apoyo y orientación de GRUINCO, con base en el análisis y clasificación del riesgo del sistema y durante la fase de diseño del proyecto, deberá definir formalmente los requerimientos de seguridad por parte del "usuario" del sistema o un representante del mismo. Las medidas de seguridad deben ser definidas a partir de los requerimientos de seguridad establecidos.
9. Los requerimientos de seguridad de los sistemas que no puedan ser adecuadamente satisfechos deben ser explícitamente reportados al "usuario" del sistema y a la Coordinación GRUINCO y a quienes afecte directamente el proceso a fin de identificar, tratar el riesgo, y mitigar su impacto.
10. En la fase de pruebas e implementación, las medidas de seguridad deben ser probadas adecuadamente por el Comité Gerencial del proyecto con apoyo y orientación de GRUINCO .Las pruebas deben ser documentadas en un reporte, remitidas al "usuario" del sistema y a la Coordinación GRUINCO.
11. Las regulaciones de seguridad y demás normativas que aseguran la calidad y confiabilidad de los sistemas, deberán mantenerse para aquellos proveedores externos de sistemas, así como en la compra de paquetes, Suite y demás Sistemas de Información, así mismo se les deberá exigir un test de vulnerabilidades o Ethical Hacking realizado por quien ellos consideren pero que garantice el estudio y análisis de Vulnerabilidades que avale que dicho sistema es óptimo en su seguridad.
12. Cuando se realicen pruebas deberán de realizarse en un ambiente de prueba antes de poner la aplicación en producción y deberá considerarse el uso en paralelo del nuevo sistema y del antiguo sistema, a fin de detectar errores.

13. La responsabilidad última por aceptación formal de las aplicaciones corresponde al Gerente del Proyecto y la Área y/o Proceso misional responsable del proyecto del desarrollo en los aspectos relativos a la funcionalidad de la aplicación. GRUINCO acompaña y asesora al proceso en los requerimientos NO funcionales; Sin embargo la funcionalidad es la que determinarán que la herramienta informática funcione a satisfacción y que este ajustada a los requerimientos.
14. El Comité Gerencial, deberá velar por que la aplicación desarrollada cumpla con la funcionalidad para la cual el desarrollo/Sistema de información fue contratado; GRUINCO –por medio del área de Sistemas de Información- velara por que se cumplan los lineamientos, normativa técnica y metodológica de desarrollo vigente en DIMAR, además de que todos los componentes (programas, fuentes, programas objeto, macros, documentación, diagramas y otros) asociados a la aplicación estén debidamente actualizados y sean compatibles con dispositivos móviles.
15. A los responsables de “producción”, a efecto de asegurar que los aspectos operacionales que conlleva la aplicación sean adecuados y no afecten adversamente el medio ambiente de operación general (software, ambiental, comunicaciones, y otros), otras aplicaciones o la operación satisfactoria de la misma aplicación.
16. El proceso de puesta en producción de las aplicaciones, de los sistemas o de sus actualizaciones, debe realizarse de tal forma que no deteriore los servicios a los usuarios o la operación normal, por tanto, debe coordinarse adecuadamente y realizarse con cronogramas y horarios preestablecidos.
17. DIMAR debe procurar porque todo sistema cuente con un esquema de contingencia el cual debe contemplar aspectos de software, hardware y recurso humano necesario para la continuidad del servicio; Esto debe ser revisado por el responsable de cada proceso en conjunto con GRUINCO.
18. Todo sistema de información debe tener asignado un administrador del sistema responsable de actividades de operación, manejo, cumplimiento de la seguridad establecida y enlace con GRUINCO.
19. GRUINCO será responsable de mantener la operatividad del servidor y atenderá las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware, storage.
20. GRUINCO garantizará a los usuarios del servicio los recursos de almacenamiento y los respaldos de la información allí contenida.
21. GRUINCO será responsable de administrar las cuentas de los usuarios autorizados para publicar contenido en el servidor FTP, a través del directorio activo de la entidad, sin embargo, Sera el propietario o responsable de la información quien solicite a GRUINCO que usuarios y con qué nivel de acceso pueden acceder a los recursos.

22. GRUINCO será responsable de monitorear la utilización de los recursos de hardware en el servidor. Esto con el fin de proceder a la actualización del mismo en el caso de ser requerido para garantizar la continuidad de los servicios.
23. GRUINCO notificará a los usuarios las ventanas de mantenimiento o la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad del mismo.
24. Todo código fuente, script o archivo relevante para el desarrollo de los sistemas de información deberá ser copiado y respaldado en el computador del programador que lo está elaborando y deberá alojar una versión en el repositorio de código fuente (SVN)
25. Todo cambio deberá ser documentado, y de igual forma, deberá contar con una ventana de mantenimiento para su puesta en producción. Dichas ventanas de mantenimiento deben estar debidamente documentadas indicando fecha, responsable, servidor y aplicativo afectado, además de la razón de los cambios efectuados.

SEPARACION DE AMBIENTES

a. La entidad deberá contar con ambientes separados para Desarrollo, Pruebas y Puesta en Producción de los Sistemas de Información. Bajo ningún motivo se podrá desarrollar aplicaciones en el ambiente productivo.
b. Las funciones de desarrollo de aplicaciones, prueba, aceptación y producción de aplicaciones, y la custodia del software e información ligada, deben estar separadas y ser realizadas por funcionarios distintos entre sí, a efecto de asegurar una adecuada segregación de funciones.
c. Cuando se realizan las pruebas del nuevo Sistema de Información deberá realizarse previamente en un ambiente de pruebas del sistema preferiblemente virtualizado, con el fin de no comprometer la información ni las bases de datos de DIMAR o de los usuarios.
d. Las herramientas y privilegios propios del ambiente de desarrollo, que favorecen un ambiente y facilidades para las pruebas, no deben ser traspasados al ambiente de producción debido a que comprometen la seguridad de la operación normal; Las pruebas deberán de realizarse en un ambiente de prueba o en paralelo.

TRANSFERENCIA DE ARCHIVOS / INFORMACION

1. La documentación software, o cualquier tipo de información de uso, no debe ser transferida a terceros sin que medie autorización superior o un compromiso de confidencialidad entre DIMAR y terceros.

2. Toda información que se genere, procese, almacene y/o transite por la red de DIMAR se considera propiedad de la Dirección General Marítima.

3. La información transmitida, procesada producto de las funciones del personal y que concierne a DIMAR o a sus usuarios, no podrá ser interceptada o divulgada bajo ninguna circunstancia, por ningún usuario interno de la red DIMAR, salvo en aquellos casos que los organismos de seguridad establezcan bajo órdenes judiciales.

4. Queda totalmente prohibido cargar información de la entidad a nubes públicas como los son Dropbox, OneDrive, Google Drive o Servicios similares. En caso de requerirse la transferencia de información entre Sedes o hacia un externo, se deberá usar el servicio de nube privado (cloud.dimar.mil.co), en donde se podrá:

    a. Dar permisos de acceso, consulta y/o modificación por correo electrónico.

    b. Asignar tiempo de publicación de la información

5. En caso de requerirse transferir información a un tercero, el dueño de la información deberá solicitar asesoraría a GRUINCO sobre cifrado de la información y uso de llaves criptográficas; Se deberá procurar transferir información siempre cifrada.

Servicio FTP:

El Servicio FTP (File Transfer Protocol) proporcionará a los usuarios de DIMAR a nivel nacional, la publicación temporal de documentos, archivos, carpetas, en cualquier extensión, o ejecutables autorizados por GRUINCO.

1. El servicio será exclusivamente para los usuarios cuya Facultad o Dependencia requieran trasferir información., de modo temporal, el mismo no será sitio para alojar definitivamente ningún tipo de archivos, imágenes, videos, o cualquier otro tipo de dato.

2. Este servicio se brindará de acuerdo a la disponibilidad de los recursos de hardware en los servidores de DIMAR – GRUINCO.

3. El contenido de los servidores o almacenamientos será filtrado o eliminado con una periodicidad mensual, o cuando la falta de espacio en los discos lo requiera, este procedimiento no requiere notificar a ningún usuario en vista de que el protocolo FTP, es solo de trasferencia de archivos y no de repositorio por ende GRUINCO no es

responsabilidad de GRUINCO velar por la información allí alojada; así mismo la confidencialidad de los documentos allí alojados no deberán ser de carácter secreto, ultra secreto o datos sensibles.

4. El personal de DIMAR autorizado para cargar los contenidos en el servidor FTP deberá realizarlo por medio de las credenciales del Directorio Activo ó por medio de usuario y un password, que se autenticara de manera inmediata.
5. La aplicación autorizada por DIMAR para la publicación del contenido en el servidor será el WS_FTP, o trasferencia directa sobre el enlace mencionado.
6. Las dependencias deberán comprobar que la publicación se haya realizado correctamente, antes de suministrar la ruta al usuario solicitante.
7. Cada dependencia informará al solicitante por correo electrónico, la ruta o dirección de ubicación del contenido.
8. GRUINCO - Plataforma Redes y Seguridad Informática eliminará el contenido vencido según la vigencia especifica.

Requisitos para optar al Servicio:

a. El contenido objeto de la solicitud de publicación en el servidor FTP deberá ser de carácter institucional y de acceso público, en la red DIMAR.

b. La solicitud de publicación en el servidor FTP deberá venir acompañada del contenido a ser publicado y la fecha hasta la cual estará publicada o vigente.

c. El solicitante del servicio deberá ser funcionario y/o contratista de la entidad.

d. En caso de que el contenido sea de software, el mismo deberá ser freeware, opensource o que no requiera licenciamiento. No se permitirá la colocación de software privativo o ilegal (No licenciado), y el mismo deberá ser autorizado publicar por parte de GRUINCO, solicitud expresa por escrito.

GESTION DE RECURSOS HUMANOS

1. Antes de empezar a ejecutar las funciones por las cuales se adquiere vínculo con DIMAR, el personal deberá ser capacitado en las políticas con las cuales adquiere responsabilidad y los sistemas de información con los cuales tendrá contacto; Se deberá dejar evidencia de dichas capacitaciones en los formatos destinados para tal fin.
2. Se deberá realizar reinducción permanente (mínimo una vez al año) en las temáticas de políticas de seguridad de la Información y Seguridad Informática.
3. Al cambiar la relación laboral de cualquier funcionario (despido, renuncia, traslado, etc.), será responsabilidad del Grupo de Desarrollo Humano y de Maestría de armas informar a GRUINCO las novedades de personal, quien a su vez deberá revocar y/o cambiar los derechos del usuario, esto soportado por reporte de, quien bajo procedimiento informara el retiro, renuncia o traslado de personal para tales fines. GRUINCO debe preservar los archivos alojados por el usuario en el servidor destinado para tal fin; El perfil local del usuario (PC de trabajo) será almacenado por un tiempo pertinente para su posterior acceso en caso de ser necesario.
4. En caso de finalizar el vínculo entre la persona y DIMAR, se deberá hacer entrega de la información a la cual tuvo acceso; esto deberá ser informado al supervisor del contrato y reposar en actas; NO se podrá realizar liquidación del contrato hasta que no se dé visto bueno del supervisor del contrato de contar con la totalidad de la información a la que haya tenido acceso y uso el contratista.

REDES INALAMBRICAS

Esta política establece las reglas para el uso de tecnología inalámbrica, servicios WIFI en DIMAR. La administración de los recursos de tecnologías de la información y las comunicaciones es importante para el cumplimiento y desarrollo de labores en la Dirección General Marítima (DIMAR). Las redes inalámbricas requieren de un alto grado de responsabilidad por parte de los usuarios de la red para aprovechar y maximizar los beneficios de la tecnología, brindando cobertura de red inalámbrica y un sistema de comunicaciones seguro en las edificaciones de la entidad.

Toda persona autorizada para utilizar los servicios de red inalámbrica que ofrece la Dirección General Marítima deberá cumplir con el reglamento vigente sobre su uso, así como el Reglamento para el uso de la Red LAN de la Dirección General Marítima. El no conocimiento de los mismos no exonera de responsabilidades asignadas con la utilización de los servicios ya mencionados.

1. Los equipos y antenas inalámbricas única y exclusivamente deberán ser instalados por personal GRUINCO – Plataforma, redes y Seguridad Informática, o por quien se autorice para su instalación y destino de utilización. GRUINCO por medio del Área de Plataforma, Redes y Seguridad Informática deberá supervisar y monitorear su uso.

2. Los usuarios deberán evitar el mal uso de la red inalámbrica de la Dirección General Marítima, como el acceso a sistemas o aplicaciones no autorizadas (Redes Sociales, reproducción de videos, juegos en línea, descarga de aplicativos) que afectan el desempeño de la red inalámbrica diseñada y destinada con fines netamente laborales, para aplicativos misionales y de apoyo y paginas corporativas de aplicaciones de la entidad.

3. Se monitoreará las páginas visitadas, y las mismas serán restringidas a través de los perfiles de navegación definidos en esta política. (VIP, Alto, Medio y Bajo), según se requiera previa justificación de la necesidad. En caso de hacer mal uso de los recursos o violar alguno de los lineamientos de la entidad o atentar contra la Disponibilidad, Integridad o Confidencialidad de la información de la entidad, GRUINCO estará en la potestad de eliminar los permisos asignados e informar al superior de quien infrinja lo establecido.

4. Se restringe la propagación de SSID de dispositivos de anclaje, como modem 3G, 4G, y zonas de anclaje de celulares Smartphone.

5. Se Generaran informes de monitoreo de los equipos conectados a la Wifi de la entidad, así como los reportes necesarios de saturación de canal páginas visitadas, top 10 de consumo en ancho de banda y páginas visitadas y demás que se requieran.

6. Se prohíbe que las estaciones de trabajo que están conectadas mediante la tecnología Dial-Up módems, módems celulares y/o WiFi simultáneamente estén conectadas a las redes de área local o cualquier otra red de comunicación interna.

COPIAS DE SEGURIDAD

Respaldo y recuperación Información de Usuario

El área de plataforma redes y seguridad Informática, ha asignado a cada perfil de usuario de dominio una unidad de red en la cual almacenaran información de carácter estrictamente laboral, no se podrá almacenar fotos, música, videos e información personal, este deberá ser solicitado a través de los formatos establecidos o por solicitud expresa a GRUINCO al correo destinado para este fin seguridadinformatica@dimar.mil.co.

La unidad de red se encuentra identificada con una letra, de preferencia se mapeara con la (W:), con una capacidad de almacenamiento 1GB y con niveles de seguridad de la información que garantizan el acceso a la información única y exclusivamente al titular de la cuenta de dominio.

En caso que el usuario no tenga asignada la unidad de red a la sesión del usuario, acceso o permisos de lectura y escritura sobre la unidad de red, es responsabilidad del usuario notificar al área de plataforma, redes y seguridad informática la novedad para dar solución al mismo, hecho que no justifica la no ejecución de Backups de información y archivo pst de correo electrónico por parte del usuario.

1. Será responsabilidad de cada usuario a nivel nacional realizar el respaldo de su información, así como de cada Jefatura de los archivos que sean de uso común para el desarrollo de sus actividades misionales.

2. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse, y es responsabilidad del usuario su información, dicha copia deberá ser periódica e incremental; Dicho usuario deberá comunicarse con GRUINCO con el fin de establecer los medios adecuados para tales copias de seguridad.
3. Corresponderá a GRUINCO promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos, mismos que según evaluación se mantendrán en un lugar fuera de las instalaciones del Data Center, debidamente acondicionado para dicho fin.

BackUp Sistemas de Información e Infraestructura tecnológica

La Dirección General Marítima ha presentado un desarrollo en la infraestructura tecnológica con el fin de optimizar los procesos misionales y de apoyo que ofrece la entidad, el grupo de informática y comunicaciones (GRUINCO) ha establecido procesos internos para generar respaldo y contingencia, en pro de la continuidad del negocio y disponibilidad de la información. GRUINCO maneja información a nivel de plataforma tecnológica (Máquinas Virtuales y físicas), bases de datos (Aplicativos misionales), portales WEB (DIMAR, CIOH y CCCP), aplicaciones administradas por terceros y la información de usuario final, donde se han dispuesto diferentes métodos de respaldo de acuerdo al requerimiento y necesidades del proceso.

1. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados, por esquemas de control y salvaguarda.
2. GRUINCO y las Unidades en conjunto con las empresas responsable del mantenimiento preventivo y correctivo de los equipos de cómputo, definirán el personal que tendrá la responsabilidad de realizar los distintos tipos de respaldos. El personal no sólo debe ser capaz de generar el respaldo, sino estar capacitado para la recuperación de la información en caso de ser necesario.

BackUp Plataforma Tecnológica

Se ha establecido un plan de trabajo para la ejecución de copias de seguridad de la plataforma tecnológica de la Dirección General Marítima, en el cual se realiza una programación mensual para el respaldo de cada una de las máquinas virtuales que se encuentran creadas en el Clúster. Con el fin de garantizar la correcta ejecución de la copia de

seguridad de las máquinas virtuales se requiere crear una ventana de mantenimiento programada para detener los servicios y apagar el servidor para prevenir errores a la hora de generar la copia del disco de la máquina, y poder realizar un Backup completo y seguro de cada máquina virtual y/o física.

La programación para ejecución de copias de seguridad se realiza en conjunto con los grupos de la entidad (GRUCOG, GLEMAR, ACOES, GRUCOI, GPLAD, SUBDEMAR, SUBAFIN, SUBMERC, GRUDHU, GRASI, GRUINCO, capitanías de puerto, centros de investigaciones, intendencias y señalizaciones marítimas) según la criticidad del servicio para no generar impacto en los servicios prestados por la Dirección General Marítima.

BackUp Bases de Datos

El respaldo a las bases de datos es una actividad desarrollada por el área de Sistemas de Información en conjunto con el área de plataforma, redes y seguridad informática, la programación, ejecución y validación de la copia de respaldo está bajo supervisión de Sistemas de Información GRUINCO.

El Área de Plataforma, Redes y Seguridad Informática deberá entregar una unidad de Almacenamiento donde se alojaran los Backups de las bases de datos por parte de sistemas de Información, con el fin que el robot de Backup genere respaldo a la información que se encuentra en la unidad destinada para tal fin.

Backup Portal Dirección General Marítima Sede Central

El Backup al portal de DIMAR se encuentra configurado para su ejecución a nivel de archivos y base de datos, el cual se encuentra programado para su ejecución en forma automática, una vez al día, una vez por semana y una vez al mes, sobre archivos y base de datos, se debe tener en cuenta que la programación de Backup tiene un histórico de 4 Backup por periodo, el quinto Backup sobre escribirá el histórico con el fin de optimizar el almacenamiento de la entidad.

Backup De Portales Web Centros De Investigación

Los portales WEB de los centros de Investigación (CIOH Caribe y Pacifico) son administrados directamente por el administrador de cada Centro de Investigación, por ende es responsabilidad del administrador de sistemas de cada uno de los Centros la programación, ejecución y pruebas de restauración del mismo; El personal de GRUINCO en Sede central deberá programar y ejecutar copias de Seguridad en caso de que los servidores sean virtuales.

Backup De Sistemas y/o Aplicaciones Soportadas Por Terceros

La generación de copias de respaldo de las aplicaciones administradas por terceros, son programados, ejecutados y restaurados en un entorno de pruebas por parte del tercero, garantizando restauración de todos los componentes de máquinas físicas, virtuales y aplicativos administrados.

En el respaldo de los datos se debe considerar tanto los datos de la aplicación (archivos, bases de datos, datos estructurados y no estructurados) como los demás elementos necesarios para asegurar la prestación de servicios, tales como el software de la aplicación (programas) y parámetros de operación, documentación complementaria a los procesos, sistemas operativos, software de ambiente y otros utilitarios.

a. Debe crearse una programación sistemática de los procesos de respaldo (diarios, semanales, mensuales y anuales), además se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.

b. Todos los procesos de respaldo y recuperación de información deben proveer los elementos que evidencien (log de eventos) la ejecución del proceso, detalle del contenido de los mismos, así como deficiencias en caso de existir.

c. Los medios de respaldo deben ser protegidos de borrados accidentales a través del uso de medios físicos y lógicos de carácter preventivo (“lock” en los medios de Backup, otros).

d. Los medios de respaldo deben disponer de etiquetas externas e internas, así como una identificación permanente, que permita determinar fácil y confiablemente su contenido. Las etiquetas deben tener información de su contenido, nombre, fecha del respaldo y funcionario que lo realizó.

e. Los respaldos de datos y demás elementos complementarios, deben estar resguardados en sitios que dispongan de condiciones de acceso restringido y de medio ambiente apropiado a los medios utilizados, así como para hacer frente con éxito a eventos contingentes como incendios, inundaciones u otros (Sistemas de contingencia recuperación de Desastres PNC).

f. Antes de proceder a la restauración de datos sensibles o críticos a partir de un respaldo se debe realizar una copia de los mismos para minimizar efectos de corrupción o daños de los datos originalmente respaldados.

g. Se debe generar una copia de todos los respaldos, los cuales se custodiarán en un sitio alterno, que cumpla con las características y protección ambiental similares al sitio principal. La proximidad entre el sitio principal y el alterno se debe contemplar dentro de los parámetros que se establezcan en el convenio de salvaguarda y custodia con el proveedor y deben estar dentro de los parámetros de PCN “Plan de continuidad del Negocio” debe disponer al menos de dos vías de acceso distintas.

h. Se deben tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo al sitio alterno, a fin de garantizar no solo que llegarán a su

destino sino la integridad de los medios, las unidades deberán gestionar este procedimiento a través de los administradores regionales de informática.

i. Por lo menos dos veces al año se debe verificar la validez de los respaldos custodiados en el sitio principal y en sitio alterno. Se debe verificar la condición de los medios de almacenamiento y si los datos pueden ser restaurados oportuna y confiablemente. Periódicamente debe realizarse inventario de los medios de respaldo (mínimo cuatro veces al año). Se debe utilizar formulario diseñado para este fin.

j. Los equipos y medios de respaldo de las distintas plataformas tecnológicas deben obedecer a un estándar para facilitar el intercambio de datos, su control y una mayor economía de operación. Dicho estándar será el definido por la DIMAR con la empresa encargada de la custodia y salvaguarda de la información.

k. Los equipos y los medios usados para el respaldo deben ser sometidos a un mantenimiento preventivo por parte del proveedor (al menos 03 veces al año) que asegure las condiciones adecuadas del funcionamiento.

l. Una vez al mes se detendrán todos los servicios de plataforma virtualizada, con el fin de realizar un backup completo de las maquinas del Clúster de alta disponibilidad.

m. Registrar en las bitácoras propuestas a continuación la información más detallada sobre los resultados de las tareas de backup.

GENERACIÓN DE ENTORNO DE PRUEBAS PARA RESTAURACIÓN DE BACKUP

El área de plataforma, redes y seguridad informática, ha generado un escenario básico y similar al de producción, permitiendo validar las restauraciones de los backup realizados, con el fin de garantizar la integridad de la información extraída mediante el robot de backup. Estas pruebas se realizarán trimestralmente.

CUSTODIA BACKUP.

De forma trimestral se genera un Backup mediante el Robot de Backup en cinta o disco, sobre la información de la Dirección General Marítima, el responsable de la custodia del Backup es el tercero respaldado por el ISP, y será una custodia externa con todos los protocolos de seguridad que se contemplan en estos casos.

CRONOGRAMA EJECUCIÓN DE BACKUP SEDE CENTRAL

El área de plataforma, redes y seguridad informática ha establecido un modelo para la ejecución de Backup de Infraestructura e información de la dirección General Marítima, para garantizar la disponibilidad, confidencialidad e integridad de la información y servicios que soportan la operación operativa y misional de DIMAR.

REGISTRO DE ACTIVIDADES/TRANSACCIONES – LOGGING

1. Cada sistema debe contener la información necesaria para identificar cada nombre de usuario con el funcionario responsable de su uso.
2. El acceso a las bitácoras del sistema debe estar restringido al personal autorizado.
3. Los registros de eventos sensibles contenidos en la bitácora que pueden comprometer la confidencialidad y confiabilidad de los datos y los procesos deben estar restringidos a personal autorizado (Jefaturas, Auditor) y deben ser revisados periódica y oportunamente por la Coordinación de GRUINCO o por quién éste designe.
4. Los servidores de bases de datos misionales, de apoyo y administrativos son de acceso controlado y confidencial por ello son de acceso restringido, por tal motivo deberá quedar registro autorizado por parte de la coordinación de GRUINCO para la realización de copias de las Bases de Datos.
5. La entidad deberá contar con las herramientas necesarias que permitan registrar las actividades realizadas por los usuarios a nivel de acciones realizas en Sistemas de Información, Directorio activo, Servidores de archivos, navegación y transferencia de archivos
6. El responsable de Seguridad de la Información deberá realizar revisión periódica (mínimo cada tres meses) de las actividades realizadas por los administradores de Sistema, Plataformas, Redes y Seguridad Informática

SOFTWARE Y LICENCIAMIENTO

1. En los equipos de DIMAR únicamente se debe tener instalado aquel software debidamente autorizado por GRUINCO y para el que se disponga de las licencias de uso respectivo.

2. Es responsabilidad del Grupo de Informática y Comunicaciones tener un listado del Software autorizado que debe estar instalado en los equipos de trabajo (Computadores, Portátiles, Smart Phones, Tabletas … etc.), y velar por que NO se instale o utilice software adicional a este.

3. Es responsabilidad del Grupo de Informática y Comunicaciones tener actualizado el listado de licencias tanto de Sistema Operativo como de Aplicaciones y Software que se instala en los equipos de trabajo de la Dirección General Marítima.

4. GRUINCO o quien represente al grupo o haga sus veces en las diferentes regionales, administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática y de licenciamiento. Está prohibido la instalación de Software y/o dispositivos de salida que no hayan sido aprobados previamente por GRUINCO – Redes y Seguridad Informática, así mismo el código de desarrollo y/o software no autorizado.

5. En el caso de software gratuito o de uso restringido, solo podrá “descargarse” para la realización de pruebas y su uso debe estar justificado ante la jefatura de la dependencia o Unidad así como a GRUINCO para su respectiva autorización y registro.

6. Se realizaran periódicamente monitoreo y escaneos del Software utilizado en la entidad; el Software no autorizado que se encuentre en dicho monitoreo y escaneos de Red y a través de las herramientas destinadas para este fin, serán reportadas a los coordinadores, jefes de grupo y/o capitanes de puerto de las dependencias, así como al funcionario involucrado para tomar las medidas y acciones correctivas.

7. El software ambiental, Geográfico e Hidrográfico, Tráfico Marítimo y demás aplicaciones Misionales deben ser actualizados de acuerdo con la programación que establece cada una de las áreas responsables de los procesos en coordinación con GRUINCO.

8. Las estaciones de trabajo, redes y otros medios que pueden ser afectados por virus informáticos, deben contar con software antivirus, el cual debe ser actualizado

periódicamente y bajo una política única de actualización global del Servidor de Antivirus.

9. Está prohibido el uso del software y recursos informáticos propiedad de DIMAR para fines ajenos a las actividades propias de la institución.

ESCRITORIO LIMPIO

1. Es responsabilidad de GRUINCO realizar los ajustes técnicos para que los usuarios NO puedan almacenar en el escritorio de su Estacion de trabajo (PC) información.

2. Los usuarios NO debe almacenar información ni documentos más allá de iconos de acceso a aplicaciones en el escritorio de trabajo (en el PC).

3. No se debe dejar sobre el escritorio físico documentación calificada como “Publica Privada” o “Publica Reservada”; en caso de que sea estrictamente obligatorio hacerlo, se debe cubrir con un folio de color especial y con el sello de “CONFIDENCIAL” al finalizar la jornada laboral

USO ADECUADO Y CONSERVACION DE RECURSOS

1. GRUINCO coordinará con la empresa encargada del mantenimiento preventivo y correctivo del equipo de cómputo, la realización de estas tareas, así como la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir los procesos internos respectivos y relacionar dichas tareas en el sistema de información destinado para ello.
2. Deben ser protegidos con medios físicos (tales como candado, fajas, etiquetas u otros) aquellos equipos o sus componentes que por su valor o exposición pueden estar sujetos a pérdidas o sustracción.
3. La adquisición de los bienes (hardware y software) se realizará de conformidad con las directrices y normativas técnicas que establezca la Subdirección Administrativa y Financiera con base a las políticas sectoriales.
4. Todos los equipos tecnológicos deben ser objeto de mantenimiento preventivo, de conformidad con un cronograma preestablecido por el grupo interno de trabajo de GRUINCO (se recomienda que sea cada tres o cuatro meses). Se debe utilizar el formulario diseñado para este fin.
5. La empresa encargada del mantenimiento preventivo y correctivo del equipo de cómputo será la responsable del soporte y buen funcionamiento de los equipos de cómputo de la red DIMAR bajo la supervisión del responsable del área encargada GRUINCO, según los términos establecidos en la contratación del servicio y deben asegurar que las condiciones de medio ambiente en que operan éstos se ajustan a las establecidas por la DIMAR.
6. Se debe contar con documentación actualizada sobre los componentes y organización de las redes de DIMAR y de los recursos asociados a éstas, entre otros: enlaces y diapositivas de conexión físicas, protocolos de comunicaciones y direcciones IP, segmentaciones de la LAN extendida y canales de comunicación a nivel Nacional.
7. Los requerimientos para la instalación y actualización de redes deben ser formalizados y controlados adecuadamente, asegurando que su ejecución no interfiera con la operación normal de los servicios.
8. Los proveedores de servicios de redes y comunicaciones no deben hacer arreglos o actualizaciones completas de medios de transporte de datos, voz, corriente u otro sin el previo análisis de impacto para las unidades o dependencias y siempre bajo la supervisión de GRUINCO.

SEGURIDAD FISICA, ACCESO A CENTROS DE DATOS Y CABLEADO

1. Debe restringirse el acceso físico a las oficinas y áreas de DIMAR en las que se ubique equipo de cómputo en general y acceden y manipulen información relevante (tales como el área del servidor, equipo de comunicaciones, áreas del servicio al cliente donde se ubique equipo de cómputo y otros). Debe determinarse un método de control de acceso apropiado y acorde con la estructura de cada oficina o área, que garantice que solo personas previamente autorizadas y debidamente identificadas puedan ingresar.
2. Las rutas de acceso deben ser limitadas. Se debe considerar espacios libres y salidas de emergencia (las puertas deben abrir hacia fuera).
3. Las nuevas edificaciones o remodelaciones donde se ubique equipos de cómputo y de comunicaciones deben considerar dentro de su diseño, los requerimientos de seguridad que dicte la Dirección General Marítima.
4. Las medidas de seguridad física aplican a los funcionarios de DIMAR y a terceras personas que por razones calificadas deben acceder a áreas restringidas (funcionarios de otras dependencias, asesores, Contratistas y/o Visitantes.)
5. Todos los funcionarios que laboren o visiten áreas de acceso restringido, deberán portar el carnet de identificación suministrado por DIMAR en un lugar claramente visible.
6. Las personas ajenas a la Institución que visiten áreas restringidas deben portar una identificación y una autorización para transitar por dicho lugar, así mismo realizar el registro en los libros de minuta o planillas de registro destinadas para tal fin.
7. Las personas ajenas a las áreas restringidas deben ser dirigidas por el personal de la misma área cuando, en forma autorizada, transiten en ella. Esto incluye a empleados de otras dependencias, consultores, familiares, proveedores y otros.
8. El ingreso y permanencia de personal externo por efectos de tareas de mantenimiento, aseo y reparación de equipos deberá contar con la supervisión permanente de un funcionario autorizado del área.
9. Cuando un funcionario extravíe o le haya sido robada su identificación de acceso físico a cualquier área restringida, deberá reportarlo a la DIMAR oficina de seguridad y al superior jerárquico en forma inmediata.

10. Los funcionarios no deben permitir el ingreso de personas no autorizadas a áreas restringidas; en caso de ser testigo o evidenciar un desconocido en las instalaciones o áreas restringidas, DEBERA notificar al área de Seguridad Física.

11. La información que por alguna razón se considera valiosa, crítica o sensible, no debe estar en manos de un único funcionario, por lo tanto, no debe permitirse que un funcionario trabaje solo en áreas que contienen esta clase de información. Este tipo de información será valorada por la DIMAR.

12. El acceso a áreas restringidas que manejan información sensible, crítica o valiosa debe permitirse sólo dentro del horario normal o con la debida autorización en horario extraordinario previa autorización a través de los formatos establecidos.

13. Todo equipo de cómputo o de comunicaciones que deba ser trasladado de una unidad hacia otra, debe tener la respectiva autorización, misma que será verificada por personal de vigilancia, Suboficial y/o Oficial de Guardia de la dependencia. Se debe utilizar formato diseñado para este fin y/o libro de minuta.

14. El personal de vigilancia o la empresa contratada para tal fin, deben revisar el contenido de toda cartera, maleta, bolsa y otros para prevenir la sustracción de componentes de equipo de cómputo o de información en medios magnéticos o físicos.

15. Cada dependencia que utilice el sistema de acceso electrónico a sus instalaciones, deberá solicitar periódicamente a la de seguridad u responsable, según sea el caso, una lista de funcionarios con derechos de acceso físico a fin de garantizar que corresponden a los actualmente autorizados y para que validen los derechos de acceso o bien realicen los ajustes pertinentes.

16. Cuando un funcionario termine su relación laboral o sea trasladado, deberá ser reportado por su Superior Jerárquico a fin de que sea desactivado todo código de acceso por él conocido y utilizado. Dichos códigos no podrán ser utilizados por ningún otro funcionario.

17. Es responsabilidad de GRUINCO inhabilitar o gestionar la inhabilitación temporal de los derechos de acceso físico previo reporte y/o acuerdo con GRUDHU y/o Maestría de Armas para aquellos funcionarios que se ausenten de sus puestos por un período mayor a 30 (treinta) días hábiles (incapacidades, permisos, suspensiones, etc.).

18. Para un mejor control, es necesario mantener respaldada y archivada información de los últimos tres meses sobre las personas que ingresaron en las áreas restringidas y registros de las que comúnmente ingresan. Además, es

necesario mantener control de las personas que diariamente ingresan y salen, para facilitar acciones en caso de tener que evacuar áreas de acceso restringido.

19. La distribución física de las oficinas de DIMAR debe asegurar la protección de las computadoras, sistemas de comunicación y equipo en general de acceso no autorizado, para prevenir robos, accidentes, uso no autorizado de equipos, información u otros.

20. En las áreas de acceso restringido se debe mantener las puertas con llave y limitar el acceso solo al personal autorizado.

21. Las áreas de acceso restringido no deben utilizarse para custodiar suministros de cómputo (cintas, papel, CD – DVD o medios extraíbles) o salvaguardar objetos personales o de valor distinto a los requeridos en el área misma, que puedan comprometer la seguridad.

22. Para efectos de seguridad, no se debe colocar rótulos que identifiquen los sitios donde se ubican los servidores, el equipo de comunicaciones y otros equipos de cómputo en sitios donde el área no sea de acceso restringido.

23. Las puertas de acceso a las áreas restringidas deben permanecer siempre cerradas. No podrán mantenerse abiertas mediante el uso de sillas, tacos de papel en las cerraduras, llaves puestas en el la chapa u otros objetos que obstruyan su cierre y faciliten el acceso a personas no autorizadas.

24. Todas las dependencias y/o Unidades de DIMAR deberán mantener un inventario actualizado de equipo de cómputo y de comunicaciones (microcomputadoras, PC portátiles, impresoras, módems, etc.), asignados bajo su responsabilidad.

25. Los equipos de cómputo y de comunicaciones deben estar asignados a un funcionamiento responsable, quien velará por el buen estado de los mismos y de la infraestructura, asegurando que se les preste el oportuno y cuidadoso mantenimiento, así como se realicen las pruebas de funcionalidad que correspondan.

26. Se prohíbe las actividades de fumar, beber o ingerir comidas en áreas de cómputo o en áreas que así hayan sido delimitadas con tal prohibición.

27. Los suministros de cómputo deben estar bajo la responsabilidad de un funcionario a fin de garantizar su uso racional.

28. Está prohibido introducir a las áreas de trabajo elementos potencialmente peligrosos para la seguridad de las personas, de los equipos de cómputo y de comunicaciones de DIMAR, tales como armas, explosivos, imanes u otros.

29. Es responsabilidad de los funcionarios de DIMAR, cumplir con las directrices establecidas por la Subdirección Administrativa y Financiera para el seguimiento y/o reclamación de las pólizas de seguros de infraestructura tecnológica.

30. La Dirección General Marítima es responsable de mantener en forma actualizada un "Esquema de Contingencias", situación que coordinará con la empresa proveedora de servicios de aseguramiento del equipo de cómputo. Este debe incluir el detalle del inventario de recursos informáticos asignados bajo su responsabilidad, el detalle de los respaldos periódicos en existencia, un inventario de sistemas críticos, nombres y números de teléfono u otro medio de localización de personal asignado para atender situaciones de emergencia (Administradores Guardias Informáticas, personal de soporte técnico, otros) y números de teléfonos de emergencia.

INCUMPLIMIENTO Y SANCIONES

El incumplimiento de estas políticas de seguridad, privacidad y reglamento de Seguridad Informática traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

a. Cualquier violación a la política y reglamento de Seguridad informática y Física de DIMAR deberá ser sancionada de acuerdo al Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley Colombiana así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones van desde una llamada de atención o informar al usuario, hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

c. Corresponderá al Grupo de Informática y Comunicaciones elaborar un informe preliminar a la Coordinación con copia a quien corresponda con las infracciones a la seguridad correspondiente a fin de que se tomen las acciones normativas que correspondan a quienes violen las disposiciones en materia de informática de la institución.

d. Todas las acciones en las que se comprometa la seguridad de la Red de la Dirección General Marítima y que no estén previstas en esta política, deberán ser revisadas por GRUINCO y los Miembros del Área de Redes y Seguridad Informática, para dictar una directiva sujetándose al estado de derecho.