Universidad de Costa Rica

Sistema de Estudios de Postgrado

"Evaluación del inventario de las armas propiedad del Ministerio de Seguridad Pública"

Trabajo Final de Graduación aceptado por la Comisión del Programa de Postgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster en Administración y Dirección de Empresas con énfasis en Auditoría de Tecnologías y Sistemas de Información.

Jeffrey Eubanks Jara

Carné: A46775

Ciudad Universitaria "Rodrigo Facio", Costa Rica

2007

DEDICATORIA

A mi novia y prometida María del Mar Chacón Salazar, a mi suegra doña Nuria Chacón Salazar.

A mi familia Eubanks Jara.

A mis tutores, Lic. Sergio Espinoza Guido, Lic. Virgilio Siles Elizondo y el Lic. Douglas Elliott Martínez.

AGRADECIMIENTOS

A Dios por darme la vida por medio de mi madre, también por que me dio sabiduría durante todo el tiempo que curse la maestría.

A mi novia y prometida María del Mar por creer en mí y brindarme su apoyo en todo momento que lo necesite.

A doña Nuria mi suegra por su apoyo incondicional durante todo el tiempo que cursé la maestría.

A mis tutores por su ayuda y aportes en la realización de este trabajo.

A la Auditoría General del Ministerio de Seguridad Pública por su confianza depositada en mi persona, para desarrollar este trabajo.

HOJA DE APROBACIÓN

Este Trabajo Final de Graduación fue aceptado por la Comisión del Programa de Postgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster con énfasis en Auditoría de Tecnologías y Sistemas de Información.

_____	_____
Msc. Aníbal Barquero Chacón	Master. Sergio Espinosa Guido
Director Programa de Maestría	Profesor Coordinador
_____	_____
Lic. Virgilio Siles Elizondo / P.E.M	Lic. Douglas Ellioth Martínez
Profesor Guía	Supervisor Laboral

_____

Ing. Jeffrey Eubanks Jara

Estudiante

CONTENIDO

"Evaluación del inventario de las armas propiedad del Ministerio de Seguridad Pública"

ÍNDICE DE ANEXOS COMPLEMENTARIOS

ÍNDICE DE SIGLAS Y ABREVIATURAS

Ministerio de Seguridad Pública	MSP
Dirección General de Armamento	DGA
Arsenal Nacional	AN
Control Armas y Municiones	CARMU

RESUMEN

Eubanks Jara, Jeffrey

"Evaluación del inventario de las armas propiedad del Ministerio de Seguridad Pública".

Programa de Postgrado en Administración y Dirección de Empresas. –San José, CR.: J. Eubanks J., 2007.

El objetivo general del trabajo es comprobar la existencia y cumplimiento de procedimientos, políticas, normas y directrices organizacionales de seguridad, mediante la verificación y ejecución de pruebas sustantivas de auditoría al sistema de información denominado CARMU, que permita evidenciar el mantenimiento óptimo de una seguridad física y lógica de los datos almacenados

La organización auditada se dedica a mantener actualizado el inventario permanente de todas las armas y de ejercer su control y fiscalización. Además, lleva por medio del Registro de Armas, la inscripción y el inventario permanente de las armas, las municiones y los explosivos propiedad del Estado.

Para ello el proyecto desarrolla una auditoría de la seguridad física de las instalaciones que almacenan las armas de fuego, propiedad del Estado y la seguridad lógica del sistema de información denominado "CARMU" (Control Armas y Munición).

Dentro de sus principales conclusiones se encuentra que la Administración no tiene conciencia de los activos tan relevantes para la seguridad nacional, que se resguardan en las instalaciones de la Dirección General de Armamento, los cuales no poseen la infraestructura física ni los mecanismos de seguridad pertinentes para el eficiente y eficaz desarrollo de su control y protección.

Con base en todo lo anterior, se recomienda que sensibilizar a las partes involucradas directamente e indirectamente con la Dirección General de Armamento, sobre implantar medidas y procedimientos de seguridad eficientes y eficaces para reguardar todos los activos (recurso humano, equipos de cómputo, armas, municiones, explosivos) asignados a esa Dependencia, así como diseñar e implementar un plan de contingencia con el fin de asegurar la continuidad de sus procesos en el momento que ocurra alguna eventualidad.

Palabras clave: Inventario de armas, CARMU, Dirección General de Armamento, Arsenal Nacional.

Director de la investigación:
Lic. Virgilio Siles Elizondo/ P.E.M

Unidad Académica:
Programa de Postgrado en Administración y Dirección de Empresas
Sistema de Estudios de Postgrado

INTRODUCCIÓN

Puesto que la información manipulada por la Dirección General de Armamento está clasificada como “secreto de Estado”; surge la necesidad de evaluar el estado de la seguridad física de las instalaciones que las resguardan, así como la seguridad lógica del sistema de información CARMU.

Al efectuar este estudio, se mostrará la situación actual de los controles utilizados para una seguridad efectiva en el resguardo y manipulación del Armamento Nacional. El producto obtenido de la evaluación será de ayuda al Ministerio de Seguridad Pública en la toma de decisiones, en caso de detectar aspectos sujetos de mejora, para no incurrir en los mismos errores cometidos anteriormente en el control de otros activos propiedad del Estado, como por ejemplo, el caso de los vehículos marca ARO, situación que salio a relucir en los medios de comunicación del país.

Para la Universidad de Costa Rica, la asignación de dicho estudio representa una forma de evaluar los conocimientos adquiridos por mi persona en los diferentes cursos recibidos en el programa de Maestría en Administración y Dirección de Empresas con Énfasis en Auditoría de Tecnologías de Información y además, es el proyecto final para la obtención del Postgrado.

Con la realización de este proyecto se pondrán en práctica las técnicas, procedimientos y metodologías impartidas por una amplia gama de profesionales expertos que fungieron como profesores de los cursos. Además, de la experiencia que he acumulado en la Auditoría Interna del Ministerio de Seguridad Pública, la cual me servirá para efectuar este proyecto de manera profesional.

Objetivo general

Comprobar la existencia y cumplimiento de procedimientos, políticas, normas y directrices organizacionales de seguridad, mediante la verificación y ejecución de pruebas sustantivas de auditoría al sistema de información denominado CARMU, que permita evidenciar el mantenimiento óptimo de una seguridad física y lógica de los datos almacenados.

Objetivos específicos

1. Comprobar si la Administración formula y mantiene políticas actualizadas de seguridad para los sistemas de información.

2. Comprobar que la seguridad física de las instalaciones en donde se resguarda el inventario de armas propiedad del Estado, están acordes con lo estipulado con la normativa general.

3. Verificar las políticas establecidas en cuanto a los controles de acceso al Arsenal Nacional, su autorización y difusión.

4. Comprobar la pertinencia del mantenimiento de la seguridad de las instalaciones.

5. Evaluar los controles de acceso del Sistema de Información CARMU.

6. Evaluar los resultados obtenidos de la revisión efectuada a la seguridad física de las instalaciones del inventario de armas, así como la seguridad lógica del sistema CARMU.

7. Emitir las conclusiones y recomendaciones sobre los aspectos sujetos de mejora encontrados en el estudio de auditoría.

En el primer capítulo se abordan conceptos generales de Seguridad como el concepto de Seguridad física y Seguridad lógica en los sistemas de información.

En el segundo capítulo se trata la situación actual de la Dirección General de Armamento, conceptualizando su origen, marco legal, aspectos y estructura orgánica.

En el tercer capítulo se centra en el análisis de la situación actual de la Dirección General de Armamento.

En el cuarto capítulo se desarrolla el Proceso de Auditoría, compuesto por todas las aspectos sujetos de mejora que se identificaron en el desarrollo del estudio de auditoría, a los cuales se les emite las respectivas recomendaciones para subsanarlos.

En el quinto capítulo se comunican las conclusiones generales obtenidas de la evaluación y las recomendaciones al respecto.

CAPÍTULO I . Aspectos Generales de Seguridad

1.1 Seguridad

1.1.1 Definición

Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en las redes de computadoras.

Mientras que por una parte Internet iba creciendo exponencialmente, por otra, el auge de la informática de consumo iba produciendo un aumento espectacular en el número de piratas informáticos.

Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso "Word" o gusano de Internet. Miles de computadoras conectadas a la red se vieron inutilizadas durante días, y las pérdidas se estimaron en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos, redes, seguridad física y lógica han sido un factor a tener muy en cuenta por cualquier organización.

¿Qué es seguridad?

Se puede entender como seguridad, una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es**,** en cierta manera, infalible.

Es muy difícil de conseguir seguridad total, entonces se puede hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él). Más que de seguridad, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:

· Confidencialidad

· Integridad

· Disponibilidad.

CONFIDENCIALIDAD:

Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

En áreas de seguridad gubernamentales el secreto asegura que los usuarios pueden acceder a la información que les está permitida con base en su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas.

En entornos de negocios, la confidencialidad asegura la protección con base en disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, contratos laborales que especifican este tema, etc.

Este aspecto de la seguridad es particularmente importante cuando se habla de organismos públicos, y más concretamente aquellos relacionados con la defensa. En estos entornos los otros dos aspectos de la seguridad son menos críticos.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

INTEGRIDAD:

Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado.

Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad:

- precisión,
- integridad
- autenticidad

El concepto de **INTEGRIDAD** significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado.

De hecho el problema de la integridad no sólo se refiere a modificaciones *intencionadas*, sino también a *cambios accidentales* o no intencionados.

En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la **AUTENTICIDAD**. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos.

En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos (mantener la confidencialidad).

En el campo de la criptografía hay diversos métodos para mantener/asegurar la autenticidad de los mensajes y la precisión de los datos recibidos. Se usan para ello códigos/firmas añadidos a los mensajes en origen y recalculadas/comprobadas en el destino. Este método puede asegurar no sólo la integridad de los datos (lo enviado es igual a lo recibido), sino la autenticidad de la misma (quién lo envía es quien dice que es).

DISPONIBILIDAD:

Se entiende por disponibilidad:

- El grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.
- La situación que se produce cuando se puede acceder a un SÍ en un período de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*). Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados:

- El ordenador puede estar estropeado o haber una caída del Sistema Operativo.
- No hay suficiente memoria para ejecutar los programas.
- Los discos, cintas o impresoras no están disponibles o están llenos.
- No se puede acceder a la información.

De hecho, muchos ataques, como el caso del gusano de 1988, no buscaban borrar, robar, o modificar la información, sino bloquear el sistema creando nuevos procesos que saturaban recursos.

¿Qué se quiere proteger?

Los tres elementos principales a proteger en cualquier sistema informático son:

· Software

· Hardware

· Datos

Por hardware se entiende el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CDROMs, diskettes) o tarjetas de red.

Por software se entiende el conjunto de programas lógicos que hacen funcionar al hardware, tanto sistemas operativos como aplicaciones.

Por datos el conjunto de información lógica que manejan el software y el hardware.
Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

1.1.2 Seguridad Física

La seguridad física de los sistemas informáticos consiste en *la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial*.

Por seguridad física se entiende todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema. Estos recursos son desde un simple teclado hasta una cinta de *backup* con toda la información que hay en el sistema, pasando por la propia cpu de la maquina.

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar de seguridad informática en general. En muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un

atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema.

Esto motiva que en determinadas situaciones un atacante se incline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él mediante fallos en el *software*. Se debe tener conciencia de que la seguridad física es demasiado importante como para no tenerla en cuenta: un ladrón que roba una computadora para venderla, un incendio o un pirata que accede sin problemas a la sala de operaciones pueden hacer mucho más daño que un intruso que intenta conectarse remotamente con una máquina no autorizada; no importa que se utilicen los más avanzados medios de cifrado para conectar a los servidores, ni que se haya definido una política de "*firewall" o muro de fuego* muy restrictiva: si no se tiene en cuenta factores físicos, estos esfuerzos para proteger la información no van a servir de nada. Además, en el caso de organismos con requerimientos de seguridad medios, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas: como casi todos los atacantes de los equipos de estos entornos son casuales (esto es, no tienen interés especifico sobre *nuestros* equipos, sino sobre *cualquier* equipo), si notan a través de medidas físicas que nuestra organización está preocupada por la seguridad, probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida. Pero hay que recordar que cada sitio es diferente, y por tanto también lo son sus necesidades de seguridad; de esta forma, no se pueden dar recomendaciones especificas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es el cerrar con llave la sala de operaciones cuando se sale de ella) hasta medidas mucho más complejas, como la prevención de radiaciones electromagnéticas de los equipos.

En entornos habituales suele ser suficiente con un poco de sentido común para conseguir una mínima seguridad física; de cualquier forma, en cada institución se debe analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

1.1.3 Seguridad Lógica

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La "seguridad lógica" involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. El *Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados* emitido por la Contraloría General de la República, establece en la norma Nº 305-03 sobre seguridad lógica, que el acceso a los archivos de datos y programas sólo se permitirá al personal autorizado. Los principales objetivos que persigue la seguridad lógica son:

- Restringir el acceso a los programas y archivos
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de ésta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado “virus” de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización (“piratas”) y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias “piratas” o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

CAPÍTULO II. Situación actual de la Dirección General de Armamento

2.1 Generalidades

2.1.1 Origen

Después de la abolición del ejército en 1948, se crea la Dirección General de Armamento, dependiente del Ministerio de Seguridad Pública, que se encargará de mantener actualizado el inventario permanente de todas las armas y de ejercer su control y fiscalización. Además, llevará, por medio del Registro de Armas, la inscripción y el inventario permanente de las armas, las municiones y los explosivos propiedad del Estado.

La Dirección estará integrada por el Departamento de Control de Armas y Explosivos, el Registro de Armas y el Arsenal Nacional.

2.1.2 Marco Legal

Por la necesidad de regular todo lo concerniente a las armas de fuego, como adquisición, inscripción, portación, venta, importación, exportación, así como también las regulaciones sobre municiones y explosivos.

Se creó la Ley N° 7530, denominada “Ley de Armas y Explosivos”, dada en la Presidencia de la República, a los diez días del mes de julio de mil novecientos noventa y cinco.

2.2 Aspectos administrativos

2.2.1 Estructura orgánica

La estructura organizacional de la Dirección General de Armamento está integrada por el Departamento de Control de Armas y Explosivos, el Arsenal Nacional y el Departamento de Registro de Armas

Los cuales tienen las siguientes competencias:

a. Departamento Control de Armas y Explosivos

Es el encargado de otorgar los permisos de venta, importación, exportación, inscripción y portación de armas permitidas[1] . También de los permisos de venta, fabricación, importación y exportación de explosivos permitidos, aditamentos y materias primas para fabricar explosivos.

Además, levanta y mantiene actualizados los registros de las armas permitidas que sean propiedad de particulares.

El departamento tiene facultades para comprobar, inspeccionar, supervisar, controlar y fiscalizar la fabricación, la compra, la venta, la importación, el desalmacenaje, el traslado, el almacenaje y el decomiso de armas, municiones, explosivos y afines

b. Arsenal Nacional

El Arsenal Nacional suministra, únicamente por orden directa y especifica del Director General de Armamento, las armas, los implementos y los recursos materiales que el Ministerio provee a las unidades policiales. De ese suministro se lleva un riguroso control de las fechas, el estado de las armas y los nombres de las personas que las retiran. Estas anotaciones son comunicadas al Departamento de Registro de Armas.

Además, es el responsable de custodiar las armas y las municiones del Gobierno de la República y de reparar y darles mantenimiento.

---

[1]a. Pistolas y revólveres con calibres de 5,6 mm (calibre 22") hasta 18,5 mm (calibre 12") que no sean automáticas.
b. Revólveres y pistolas semiautomáticas hasta calibre 45" (11,53 mm).
c. Escopetas hasta calibre 12" (18,5 mm).
d. Carabinas y rifles hasta calibre 460" (11,68 mm).
e. Las que integren colecciones de armas permitidas.
f. Las utilizadas por los deportistas de tiro, al plato y de cacería mencionadas en el articulo N° 60 de la Ley N° 7530.

2.2.2 Generalidades del Departamento de Registro de Armas

Funciones

El Departamento de Registro de Armas está conformado por dos funcionarios del Arsenal Nacional de la Dirección General de Armamento, los cuales realizan las siguientes actividades:

1. Confección de recibos de Salidas y Entradas de armas, cargadores, municiones, municiones químicas y equipos de limpieza para armas.

2. Asignación de códigos e ingreso al sistema CARMU, de todas aquellas armas que son patrimoniadas a favor del Estado, realizando la inclusión, ya sea al archivo de armas en buen estado, o al archivo de desecho.

3. Actualización en el sistema CARMU de cambio de estado de las armas, como asignación o cambio de número de check.

4. Actualización de los datos en el sistema CARMU de las armas que son extraviadas, sustraídas, decomisadas o puestos en custodia a la orden del Arsenal Nacional.

5. Actualización de los datos en el sistema CARMU, propiamente el traslado de armas al archivo histórico, cuando se dicta una resolución por parte del Departamento Disciplinario Legal, donde se le cambia la condición de sustraída, extraviada, por absolutoria pagada – repuesta o por prescripción, así también se trasladan aquellas armas que son devueltas a su propietarios, cuando así lo ordena un despacho Judicial.

6. Emisión de los listados tanto para la Auditoría Interna, como para el Arsenal Nacional, toda vez que se vaya a realizar un inventario en una unidad o institución.

7. Actualización del sistema CARMU, conforme al listado posterior a un inventario realizado en cualquier unidad o institución, que tengan armas del AN asignadas.

8. Confección de las Actas de Entrega en forma definitiva al AN a la Unidad correspondiente, posterior a que exista la orden de entrega en forma definitiva al AN por parte de un Despacho Judicial de aquellas armas propiedad del Estado y que se encontraban decomisadas.

9. De cada una de las actualizaciones en el sistema CARMU, se procede también a actualizar cada una de las tarjetas de control del arma, según el movimiento: salida, entrega, o cambio de estado: extravío, sustracción, decomiso, custodia, o cambio en su condición: absolutoria, prescripción, pagada, devuelta, o el pase de buena a desecho o destruida.

10. El Departamento de Registro de Armas, participa en las destrucciones de armas, propiamente en lo que es la verificación de las características y cantidades de las armas a destruir consignadas en los listados respectivos y posteriormente actualiza el sistema CARMU.

11. Emitir informes mensuales de los movimientos de entradas y salidas de armas durante el mes, además del total de armas ubicadas en las unidades policiales, Direcciones e Instituciones gubernamentales.

12. El archivo de todos los documentos cronológicamente de los trámites llevados a cabo por el Departamento de Registro.

13. Realizar otras funciones propias del Departamento.

Procedimientos de Trabajo

Cada una de las actividades se ejecuta por medio de los siguientes procedimientos:

Para el punto 1.

Para las salidas del armamento y otros equipos, la DGA comunica al Departamento de Registro de la salida mediante oficio, en el que se especifica el tipo de armamento y cantidad que sale, la unidad policial o institución que recibe, cuando hay salida de cargadores y/o municiones, los encargados de bodega (armas y cargadores, municiones y suministros), remiten una boleta al Departamento de Registro, en donde se consigna la cantidad, tipo y código del equipo que va a salir, estas boletas se adjuntan al oficio remitido por la DGA.

Para las entradas de armamento y otros equipos, se confecciona el recibo, solamente con la nota de entrega del interesado y la boleta de taller, posterior a la revisión física del armamento para determinar el estado.

Para el punto 2.

Las armas son patrimoniadas por el Departamento de Activos y una vez concluido el proceso ese departamento confecciona el acta respectiva, una vez recibidas las copias respectivas en la Dirección General de Armamento, le remite al Departamento de Registro de Armas mediante oficio el acta, para proceder a la inclusión de las armas al sistema CARMU en el archivo que corresponda, según su estado.

Para el punto 3.

Cuando existe el ingreso de las armas de las unidades al AN, a cada una se les debe consignar un numero de check, así también según criterio de taller, se les cambia el estado, para ello se trabaja con la boleta de “Cambio de Estado o asignación de Check”, que emite la bodega de armas y cargadores del gobierno, así como la boleta de taller sobre el cambio de estado.

Para el punto 4.

Por cada arma, que pasa al estado de sustraída, extraviada o decomisada, se confecciona un oficio por parte de la DGA, el cual es remitido al Departamento de Registro de Armas para el respectivo cambio.

Para el punto 5.

El Departamento Disciplinario Legal remite copia de la resolución en los distintos casos de sustracciones o extravíos de armas, a la DGA, quien a su vez mediante un oficio al Departamento de Registro de Armas le comunica del cambio de condición del arma, para que ésta sea trasladada al archivo histórico.

Para el punto 6.

El Departamento de Registro de Armas es el responsable de la impresión de los listados de armas, toda vez que se vaya a realizar un inventario en una unidad policial o institución, así también cuando lo requiera la Auditoría Interna.

Para el punto 7.

Posterior a la realización de un inventario por parte del personal del AN, ellos presentan el listado borrador con el cual se trabajó en la armería de la DGA, de donde se le remiten esos listados adjuntos al oficio correspondiente al Departamento de Registro de Armas, con el cual se procede a la actualización en el sistema CARMU.

Para el punto 8.

Cuando existe una orden de entrega definitiva por parte de un Despacho Judicial, le es notificado al Departamento de Registro de Armas, mediante un oficio del área legal, al cual se adjunta la copia de la orden de entrega y es cuando se procede a la confección del Acta de Entrega al AN del arma, o a la unidad correspondiente.

Para el punto 9.

Existe en el Departamento de Registro de Armas los archivos con los tarjeteros de control de cada arma, la cual se actualiza de conformidad a lo que indique el sistema CARMU, toda vez que se dé una actualización cualquiera que sea.

Para el punto 10.

El Departamento de Registro de Armas, participa en conjunto con el personal de la Auditoría y el Departamento de Activos, en la revisión de los listados de armas a destruir, verificando las características y cantidades de armas. Una vez concluida la destrucción, el Departamento de Activos procede a la remisión del Acta respectiva, con la cual el Departamento de Registro de Armas, procede al pase de las armas al archivo de armas destruidas.

Para el punto 11.

La capacitación se brinda a los armeros a nivel nacional, posterior a la coordinación que haya realizado el jefe inmediato con la DGA. El interesado recibe la respectiva capacitación con base en el Manual para el manejo y control de Armerías.

Para el punto 12.

Para la elaboración de los informes mensuales de salidas y entradas de armas, se toma como referencia cada recibo de movimiento durante el mes y se consignan los datos de las cantidades y tipos de armas que sufrieron movimiento.

Para el punto 13.

Diariamente el Departamento de Registro de Armas, recibe documentación, llámese boletas de movimientos o cambios de estado o “check” de las diferentes bodegas, oficios de la DGA o del área legal, además de los recibos que son confeccionados en el propio departamento, por lo que a diario se tiene que archivar en orden cronológico cada uno de estos documentos, en los respectivos campos.

CAPÍTULO III. Análisis de la Situación Actual de la Dirección General de Armamento

El Ministerio de Seguridad Pública tuvo la necesidad de administrar el inventario de las armas y municiones del Estado, por lo tanto se creo la dependencia denominada Dirección General de Armamento, la cual en sus inicios estuvo ubicada en las instalaciones de la antigua Penitenciaria Central en San José, después se trasladó a las instalaciones adjuntas al Servicio de Vigilancia Aérea en el Aeropuerto Juan Santamaría y de ahí se reubicó a Dulce nombre de Coronado donde se sitúa actualmente.

Con el fin de regular legalmente todo lo concerniente a las armas de fuego se dictó la ley N° 7530 en 1995 denominada Ley de Armas y Explosivos la cual vino a ayudar a todo lo que respecta a la adquisición, inscripción, portación, venta, importación y exportación de armas de fuego, tareas que fueron asignadas a dicha Dirección.

Para llevar a cabo estas actividades la Dirección General de Armamento está compuesta por dos Secciones, una es la de Control de Armas y Explosivos y el Arsenal Nacional.

En cuanto a Control de Armas y Explosivos se encarga de todo lo concerniente a los permisos de portación de armas tanto particulares como de los oficiales de policía de la Fuerza Pública, también controla lo que respecta a los permisos de importación, exportación y venta de armas en los lugares destinados para tal fin, como lo son las armerías. Para cumplir estas tareas la sección cuenta con recurso humano calificado además, del apoyo tecnológico de un sistema informático.

Otra dependencia de la Dirección General de Armamento es el Arsenal Nacional, la cual como su nombre lo indica se refiere a todas las armas de fuego y municiones con que cuenta el país. El Arsenal Nacional a su vez tiene el departamento de Registro de Armas, integrado por dos funcionarios que son los encargados de administrar el inventario de armas y municiones que se resguardan en las bodegas.

Para tal actividad cuenta con un sistema de información computadorizado denominado Control de Armas y Municiones (CARMU), este sistema es plataforma cliente-servidor, fue desarrollado en 1996 por un programador de la Dirección General de Informática del Ministerio de Seguridad Pública, dicho sistema se desarrolló con el lenguaje BBX y las principales transacciones que realizaba eran: registrar las entradas, salidas, traslados y el estado de las armas ubicadas en el Arsenal Nacional y de las que están asignadas a las unidades policiales y su modo de trabajo era por lotes.

Para el año 2000 el sistema se migró al lenguaje de desarrollo Visual Pro 5. Esta herramienta de desarrollo es la versión mejorada de BBX. Esta actividad estuvo a cargo del mismo programador, el cual es actualmente la única persona que le da mantenimiento y que como se menciona en los hallazgos encontrados en el desarrollo de la evaluación, el sistema no tiene ningún tipo de documentación técnica y para el usuario final.

Entre las tareas principales que ejecuta esta nueva versión, están las siguientes: Asignación de códigos para las armas que son patrimoniadas a favor del Estado, cambio de estado de las armas, ya sea de asignación o numero de código, también actualizado el estado de armas como extraviadas, sustraídas, decomisadas, o puestas en custodia. Emite reportes de la realización de inventarios físicos por parte de la DGA y de la Auditoría General del MSP y por supuesto las demás tareas que realizaba en la versión de BBX.

En cuanto a los usuarios, el sistema tiene registrado cinco usuarios, de los cuales dos son de perfil administrador y los restantes son usuario de consulta e ingreso de datos. En el caso de los usuarios administradores, uno corresponde al creador del sistema y el otro al funcionario encargado del Departamento de Registro de Armas. Los restantes usuarios corresponden uno al funcionario asistente del Departamento de Registro de Armas, otro al jefe del Arsenal Nacional y el último a un funcionario que lo utiliza cuando falta el asistente del departamento citado anteriormente.

En general el sistema CARMU, es una herramienta tecnológica que vino a facilitar los procesos de trabajo de la Dirección General de Armamento y en especial a su departamento de Registro de Armas, obteniéndose como resultado procesos de trabajo más eficientes y eficaces con el fin de cumplir con sus objetivos, para beneficio del Ministerio de Seguridad Pública y del país.

CAPÍTULO IV. Proceso de la Auditoria

4.1) Principales aspectos sujetos de mejora

Con la realización de la evaluación de la seguridad física de las instalaciones donde se resguarda el inventario de armas propiedad del Estado y de la seguridad lógica del sistema de información computadorizado denominado CARMU, el cual se utiliza para la administración del inventario, se identificaron las principales deficiencias, las cuales se detallan a continuación:

Deficiencia N°1
TÍTULO: Infraestructura física

CONDICIÓN: Las instalaciones actuales de la Dirección General de Armamento no son las óptimas para el mantenimiento y resguardo de los activos asignados (recursos humanos, equipos informáticos, sistemas de información, armas, municiones, explosivos) por su carácter sensible, crítico y de relevante importancia para el cumplimiento de los objetivos institucionales.

CRITERIO: Acerca de la importancia de las medidas de seguridad y de las condiciones de trabajo en la Dirección General de Armamento, es importante señalar el artículo No. 10 del "*Reglamento General de Seguridad e Higiene en el Trabajo",* que establece lo siguiente:

"De las Condiciones Generales de los Locales y Ambiente de Trabajo
ARTICULO 10°- Los locales de trabajo deberán llenar, en lo relativo a ubicación, construcción y acondicionamiento, los requisitos de seguridad e higiene que demanden la seguridad, integridad, salud, moral y comodidad de los trabajadores y

cumplir, en especial, lo que establecen el presente Reglamento y cualesquiera otras disposiciones reglamentarias sobre la materia".

CAUSA: Por situaciones de presupuesto la Dirección General de Armamento no posee las instalaciones físicas óptimas para el desarrollo de sus funciones y para brindar la seguridad que requieren tan importantes activos y que son de vital relevancia para la seguridad nacional.

EFECTO: La inexistencia de instalaciones físicas óptimas y adecuadas por la naturaleza de las actividades de la Dirección General de Armamento, permite que tenga un alto apetito de riesgo en cuanto a situaciones de desastres naturales u ocasionadas por el hombre como asaltos, sabotaje, secuestro, sin dejar de lado situaciones de incendio, por el mal estado de la red eléctrica.

CONCLUSIÓN: La Administración desconoce o no le ha dado la importancia requerida a las condiciones de seguridad de la Dirección General de Armamento, a pesar de la importancia y sensibilidad de los tipos de activos que ahí se resguardan.

RECOMENDACIÓN: La Administración debe procurar la implementación de las prácticas y medidas de seguridad física necesarias, para garantizar la protección y funcionamiento de los activos de la Dirección General de Armamento y para asegurar la optimización de las condiciones de trabajo.

Deficiencia N°2

TÍTULO: Seguridad física de los equipos de cómputo de la Dirección General de Armamento y el Arsenal Nacional.

CONDICIÓN: En la visita realizada a la Dirección General de Armamento, se verifico que los equipos de cómputo están expuestos a un alto grado de riesgo.

CRITERIO: El Manual de Normas Técnicas Computadorizadas, en la norma

305.02.02, dice: Se mantendrán procedimientos y medidas efectivas para la protección del hardware, del software y de los datos de los SIC.

Declaración interpretativa

"*La seguridad física de los SIC, además del control del acceso físico indicado en la norma anterior, incluye también disponer de procedimientos y medidas que contrarresten los riesgos a los daños que puedan causar el fuego, el agua, los cortes o variaciones de la corriente eléctrica que alimenta a los equipos, así como por la presencia de químicos y otros elementos que afecten el ambiente normal de operación de las máquinas y del estado físico de los archivos magnéticos. Recursos tan valiosos no sólo desde el punto de vista económico, sino también estratégico, como son los SIC, justifican el mantenimiento de sistemas de protección física que aseguren razonablemente la operación continua de tales sistemas. Se requieren, por lo tanto, procedimientos y dispositivos orientados a prevenir, detectar y combatir la presencia de los citados riesgos. En atención a lo anterior, deberá disponerse de dispositivos de detección de fuego y humedad, así como de extintores de fuego apropiados, todos los cuales deberán probarse periódicamente para asegurar su uso en el momento requerido, otorgándose el entrenamiento necesario al personal que garantice su adecuada utilización…"*

CAUSA: Debido a la falta de conciencia de la importancia que tiene la información almacenada en los equipos de cómputo, no hay procedimientos y medidas de seguridad implementadas.

EFECTO: A causa de la inexistencia de seguridad física de los equipos de cómputo, hay una exposición de riesgo de perdida de la información tan sensible para el país, asi como de un mal resguardo de los mismos.

CONCLUSIÓN: Actualmente la Dirección de Armamento y el Arsenal Nacional es una Dirección con alto apetito de riesgo por la falta de implementación de medidas y procedimientos de seguridad de los equipos de cómputo.

RECOMENDACIÓN: Se debe sensibilizar a las partes involucradas directa e indirectamente con la Dirección General de Armamento, sobre implantar medidas y procedimientos de seguridad de los equipos para el buen aprovechamiento y resguardo en beneficio de la Institución.

Deficiencia N°3

TÍTULO:

Plan de contingencia

CONDICIÓN:

La Dirección de Armamento no cuenta con un plan de contingencias para la continuidad de operación del sistema CARMU.

CRITERIO:

El Manual de Normas Técnicas relativas a los Sistemas de Información Computadorizados, en su norma N° 305.07 señala lo siguiente:

"305.07 Plan de contigencia.
Se elaborará un plan de contingencia que procure a la continuidad de la operación normal de los SIC, cuando se presenten eventualidades inesperadas que afecten su funcionamiento"

CAUSA:

Debido a la inexistencia de un plan de contigencia, no se podrá garantizar que el sistema CARMU pueda continuar operando en el momento de una eventualidad inesperada.

EFECTO:

Por el incumplimiento a la normativa que establece la elaboración de un plan de contingencia, el sistema CARMU no podrá satisfacer a cabalidad con las funciones que le atañen y por consiguiente las actividades que tengan relación con el sistema no se podrá llevar a cabo.

CONCLUSIÓN: Se determino que el sistema CARMU esta operando sin un plan de contingencia, para que en el momento de una eventualidad inesperada, el sistema pueda continuar operando normalmente para no atrasar las demás actividades de la Dirección de Armamento, vinculadas al mismo.

RECOMENDACIÓN:

La Jefatura debe priorizar la elaboración de un Plan de Contingencia para asegurar la operación continua del sistema CARMU y asi mitigar los efectos que surjan después de alguna eventualidad negativa inesperada.

Deficiencia N°4

TÍTULO: Documentación del desarrollo del sistema de Información computadorizado CARMU.

CONDICIÓN: El sistema de información computadorizado no cuenta con la respectiva documentación sobre el desarrollo y mantenimiento del sistema.

CRITERIO: El Manual de Normas Técnicas Computadorizadas, en la norma 304.02, dice: Desarrollo de la documentación de conformidad con el Manual de estándares.
La documentación de los SIC se desarrollará de acuerdo con lo establecido en el Manual de estándares.

Declaración interpretativa

"El Manual de estándares para el desarrollo de los SIC contiene los procedimientos básicos que guían a los analistas y programadores para desarrollar la documentación del sistema, del programa, del usuario, de las operaciones del computador y de otros procedimientos pertinentes al sistema de información computadorizado en particular. Esto permitirá que la organización disponga de documentación completa, adecuada y actualizada para todos los sistemas que se desarrollen.
La documentación es parte vital de todo SIC y debe elaborarse desde el inicio de su ciclo de vida, con el fin de que se incorporen todos los detalles necesarios que podrían perderse si se posterga para el final del proyecto.

CAUSA: En un momento dado que se dé la ausencia del diseñador y programador del sistema, se dificultarían las tareas de solventar errores, modificar y realizar actualizaciones al sistema, por la inexistencia de la documentación del mismo.

EFECTO: Las actividades que utilizan el sistema CARMU, se ven afectadas por las interrupciones que tenga el sistema por la falta de mantenimiento a causa de la inexistencia de manuales y el programador.

CONCLUSIÓN: No existe ningún tipo de documentación técnica sobre la programación del sistema y mucho menos, el manual para el usuario final, por lo tanto el sistema está ligado completamente a su creador y su mantenimiento depende de la disponibilidad del desarrollador.

RECOMENDACIÓN: Se deben realizar los manuales técnicos y de usuario final para cuando necesite hacer modificaciones o resolver problemas del sistema, lo pueda efectuar cualquiera de los analistas de sistemas asignados en la Dirección de Informática y no dependa de la disponibilidad del desarrollador creador del sistema.

4.2) Evidencias de las deficiencias sujetas a mejorar.

En el desarrollo del estudio se verificó que en la Dirección General de Armamento no cuenta con dispositivos ni procedimientos que garanticen una apropiada seguridad física de las instalaciones, del recurso humano y activos que se tienen asignados para el cumplimiento de sus objetivos institucionales.

Las condiciones encontradas se detallan a continuación:

a) En la actualidad la seguridad de las instalaciones de la Dirección General de Armamento cuenta con 4 funcionarios policiales con un rol de trabajo de 24 horas de trabajo por 48 horas de descanso, estos oficiales están ubicados tanto en la caseta de la entrada principal como frente a la entrada de las bodegas del Arsenal Nacional.
b) La Dirección General de Armamento cuenta con dos accesos, los cuales ante la falta de oficiales no se les brinda la óptima seguridad, estos son la parte norte y la parte trasera de las bodegas del Arsenal Nacional.
c) En cuanto a la entrada principal de ingreso a estas instalaciones se constató que no cuentan con la infraestructura adecuada para brindar la máxima seguridad que requiere esta institución por los activos tan valiosos e importantes (armas, municiones, explosivos, pólvora), que ahí se resguardan y que son de vital importancia para la seguridad nacional.

La caseta ubicada en la entrada principal y los dispositivos de seguridad (portones) para controlar el acceso a las instalaciones se encuentra en malas condiciones como se evidencia en la fotografía N°1 y N°2, en cuanto a los portones de restricción de acceso están con corrosión, mal instalados, se pueden infringir fácilmente, ya que sólo están asegurados con una aldaba y un candado corriente, los muros que resguardan el edificio son de poca altura y tiene verjas del mismo alto, lo que facilita el acceso con sólo el hecho de saltarlas.

Fotografía N°1. Entrada principal a las instalaciones de la Dirección General de Armamento.

Fotografía N°2. Portones que resguardan la entrada principal de las instalaciones de la Dirección General de Armamento

En cuanto a la caseta de seguridad tiene el espacio muy reducido, no tiene el mobiliario y equipo de seguridad como detector de metales de cuerpo completo, mesa para revisar y colocar los artículos que traen consigo las personas, estos aspectos no favorecen al oficial de seguridad al momento de realizar la revisión a fondo de las personas que ingresan y salen de las instalaciones. Fotografía N°3

Fotografía N°3. Caseta de seguridad De la entrada principal de acceso a las instalaciones de la Dirección General de Armamento.

Aunado a esto en la caseta de seguridad adjunta a la situada en la entrada principal se nota a simple vista como se muestra en la fotografía N°4, que su infraestructura está en mal estado, por lo tanto, está inhabilitada para el servicio de seguridad. Esta situación deja al descubierto el acceso a las instalaciones por ese sector ya que no cuenta con ningún tipo de portón que restrinja el paso, solamente hay unos tubos que pretenden obstaculizar el ingreso. Fotografía N°5

Fotografía N°4. Caseta de seguridad adjunta a la caseta de la entrada principal.

Fotografía N°5. Acceso por la entrada principal sin restricciones

de acceso efectivas.

Es importante mencionar que en la parte norte se ubica un terreno que está lleno de maleza y sin una división que garantice la restricción de ingreso de personas ajenas a las instalaciones. La fotografía N°6 es clara evidencia de la situación, la cual se adiciona al mismo problema de inseguridad del resto de las instalaciones.

Foto N° 6. Esta fotografía del terreno lleno de maleza que está situado en la parte norte de las instalaciones de la Dirección General de Armamento.

La parte trasera en el costado norte es custodiada por un oficial, pero la casetilla de seguridad no posee la visibilidad que requiere para brindar el resguardo necesario al perímetro que le corresponde, más aun que colinda con un lote baldío que a su vez pone en riesgo la custodia de los activos tan peligrosos y valiosos que se encuentran ubicados en las bodegas del Arsenal Nacional.

d) Se constató que los controles implementados por parte de los encargados de la seguridad interna para el acceso físico a las instalaciones son buenos, aún y cuando no tienen los dispositivos de seguridad apropiados mencionados anteriormente para efectuar su función.

Cabe señalar que no cuentan con ningún tipo de identificación de acceso por sección, para entregar a los visitantes y usuarios de los servicios que brinda la Dirección General de Armamento y el Arsenal Nacional durante el tiempo de permanencia en las instalaciones. Esto con el fin de distinguir a los funcionarios y las personas ajenas a la institución y como mecanismo de control de cuantas personas se encuentran adentro de las instalaciones y en qué secciones o departamentos.

Sobre la infraestructura física de las instalaciones.

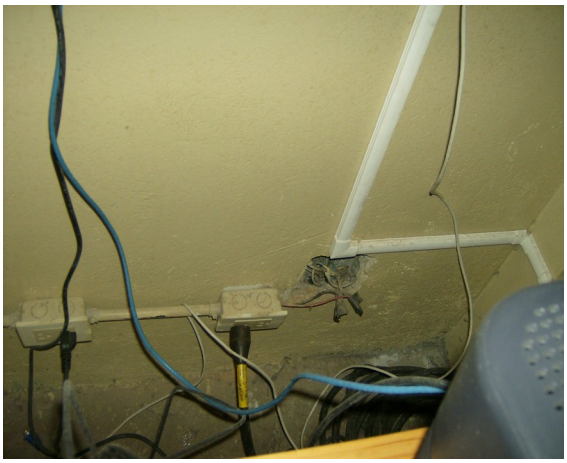
a) En la verificación que se realizó en las diferentes departamentos, se determinó que no existen salidas de emergencia, las escaleras que existen no son antideslizantes, la instalación eléctrica está en pésimo estado como se evidencia en las fotografías en donde se puede observar que existen cables expuestos, toma corrientes quebrados, pegas en los cables, cables sueltos, etc.

Fotografía N° 7. Evidencia del mal estado Instalación eléctrica

Fotografía N°8. Cables con pegas y expuestos.

Fotografía N°9. Escaleras sin antideslizantes.

Fotografía N°10. Caseta de seguridad con pegas entre los cables y expuestos al aire libre.



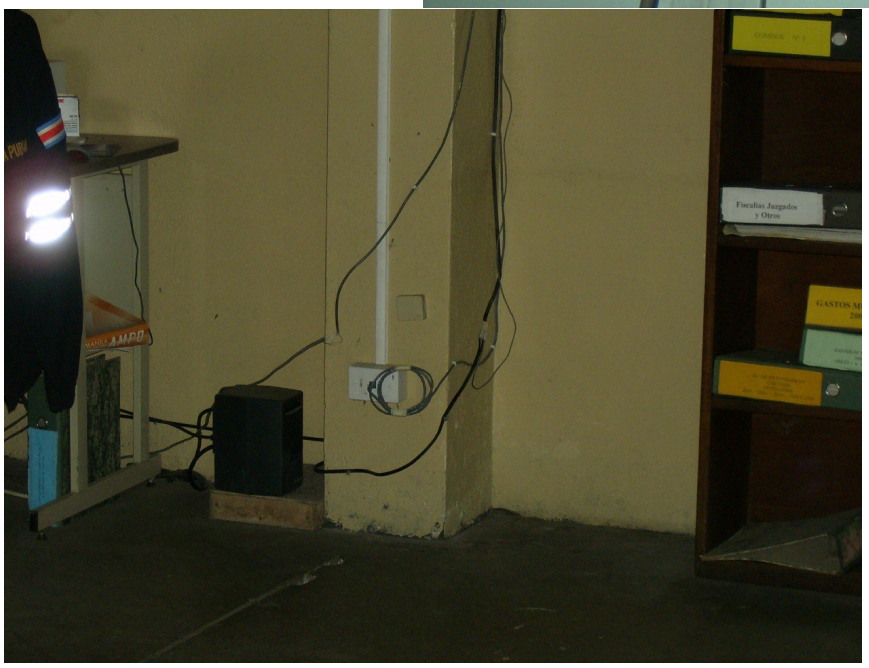
Fotografía N°11. Cables sueltos con pegas, los cuales alimentan los toma corrientes a los que está conectado un equipo de cómputo.

Fotografía N°12. Puertas de salida pero que no funcionan como salida de emergencia.

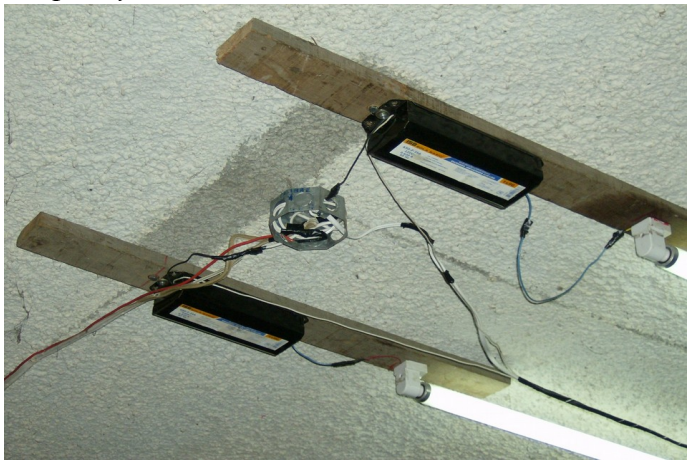
Fotografía N°13. Caja de "breaker" sin tapa.

b) En el caso de la fotografía N°13, es importante mencionar que el "techito" que está sobre la caja de "breaker" es para protegerla de las goteras que caen sobre ella, debido al mal estado del cielo raso como se evidencia en la fotografía N°14.

Fotografía N°14. Cielo raso en mal estado, se pasa el agua hacia la caja de "breaker" de la foto N°13.



Fotografía N° 15. Cables eléctricos expuestos que alimentan los tomas corrientes del equipo de cómputo y la UPS.



Fotografía N°16. Deficiente instalación eléctrica de lámparas fluorescentes.

c) La situación que presenta la infraestructura del Departamento de Registro de Armas no está ajeno a lo expuesto anteriormente, ya que igual no posee una instalación eléctrica exclusiva para los equipos de cómputo, no hay conexiones a tierra, los tomas no están polarizados ni identificados, los cables eléctricos y de señal no están en ductos.

Otra anomalía es que pasan ductos de agua sobre el departamento como se evidencia en la fotografía N° 17.

Fotografía N°17. Ductos de agua que pasan encima en el departamento de Registro y Control de Armas.

d) Otras deficiencias encontradas en la verificación de las instalaciones fue que no existen detectores de humo, hay únicamente dos deshumecedores para las 4 bodegas, pero no funcionan adecuadamente, los extinguidores están vencidos o se encuentran descargados como se puede observar en la fotografía N° 18.

Fotografía N°18. Extinguidor con más de un año de vencimiento de la carga.

La alarma de seguridad no funciona adecuadamente, por lo tanto, está desconectada.

Fotografía N°19. Sensor de la alarma de seguridad

CAPÍTULO V. Conclusiones y Recomendaciones

5.1 Conclusiones

Después de analizar la situación actual que presenta la Dirección General de Armamentos, en cuanto a la seguridad física de las instalaciones que resguardan el inventario de las armas propiedad del Estado y la seguridad lógica del sistema de información computadorizado CARMU, se pueden emitir las siguientes conclusiones:

1. La Dirección General de Armamento no tiene implementadas medidas y procedimientos de seguridad para los equipos de cómputo que tienen asignados para facilitar el desarrollo de sus actividades.

2. La Dirección General de Armamento no cuenta con un plan de contingencia para garantizar la continuidad de sus procesos de trabajo en el momento de una eventualidad.

3. No existe ningún tipo de documentación técnica sobre la programación del sistema CARMU y mucho menos el manual para el usuario final, por lo tanto, el sistema está ligado completamente a su creador y su mantenimiento depende de la disponibilidad del mismo.

4. La instalación eléctrica en las instalaciones de la Dirección General de Armamento, no se encuentra en buen estado y está propensa a que produzca un corto circuito que podría tener consecuencias nefastas para el personal, para los bienes allí custodiados y para la comunidad en donde se ubican.

5. Las limitaciones de las instalaciones físicas donde se encuentra ubicada la Dirección General de Armamentos constituye un alto riesgo para la seguridad e integridad no sólo de las personas que ahí laboran, sino también de la información, activos y documentación que ahí se resguarda.

5.2 Recomendaciones

Con el propósito de subsanar las deficiencias encontradas en el desarrollo de esta evaluación se emiten las siguientes recomendaciones:

1. Sensibilizar a las partes involucradas directa e indirectamente con la Dirección General de Armamento, sobre implantar medidas y procedimientos de seguridad eficientes y eficaces para resguardar todos los activos (recurso humano, equipos de cómputo, armas, municiones, explosivos) custodiados en esa Dependencia.

2. Priorizar por parte de la Administración, la elaboración de un Plan de Contingencia para asegurar la operación continua del sistema CARMU y así mitigar los efectos que surjan después de alguna eventualidad negativa inesperada.

3. Realizar toda la documentación (manuales técnicos y de usuario) pertinente del sistema CARMU, para cuando se necesite hacer modificaciones o resolver problemas lo pueda efectuar cualquiera de los analistas de sistemas asignados en la Dirección de Informática y no dependa de la disponibilidad del desarrollador, creador del sistema.

Bibliografía

Libros

1. Whittington, O. Ray. Auditoría un Enfoque Integral. Mc Graw-Hill, Doceava edición. Santa Fe de Bogotá, Colombia. 2000.

Códigos

2. EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2004-03-05.

PROGRAMA DE TRABAJO

EVALUACION DE LA SEGURIDAD FISICA DE LAS INSTALACIONES QUE ALMACENAN LAS ARMAS DE FUEGO, PROPIEDAD DEL MINISTERIO DE SEGURIDAD PUBLICA Y LA SEGURIDAD LOGICA DEL SISTEMA DE INFORMACION DENOMINADO "CARMU"

Procedimientos	***Hecho por:***	***Ref.***
1. REVISION PRELIMINAR		
1.1 Realice una revisión preliminar del área donde se ubican las bodegas del Arsenal Nacional.		
1.2 Solicite información referente a los procedimientos del mantenimiento de la Seguridad física y lógica de las Instalaciones y del sistema de información CARMU.		
2. EVALUACION DE CONTROL INTERNO		
2.1 Verifique la existencia de manuales de políticas, estándares y procedimientos relacionados con la seguridad en general.		
2.2 Verifique si se han divulgado las políticas, estándares y procedimientos de seguridad.		
2.3 Indague si existen documentos en que se asignen los compromisos y responsabilidades de todos los involucrados en la seguridad.		
2.4 Indague si hay planes de contingencias.		
2.5 Verifique si existen planos de construcción del inmueble.		
2.6 Verifique si existen planos de la instalación eléctrica.		
2.7 Compruebe la existencia de dispositivos de autorización de entrada a las instalaciones.		
2.8 Verifique si existen esquemas de seguridad lógica.		
3. PROCEDIMIENTOS DE APLICACION Y REVISION DE PRUEBAS		
3.1 Políticas de seguridad para sistemas de información.		

Procedimientos	*Hecho por:*	*Ref.*
Objetivo: Comprobar si la Administración formula y mantiene políticas de seguridad para los sistemas de información.		
3.1.1 Solicite y revise los manuales de políticas, estándares y procedimientos relacionados con la seguridad en general.		
3.1.2 Entreviste a quién considere necesario.		
3.1.3 Solicite y revise los documentos en que se asignen las labores de administración de la seguridad.		
3.2 Seguridad física de las instalaciones.		
Objetivo: Comprobar la seguridad física de las instalaciones en donde se resguarda el inventario de armas propiedad del gobierno.		
3.2.1 Indague, mediante documentos u observación que tipo de coordinación se lleva a cabo entre la seguridad interna y la Dirección de Armamento y el Arsenal.		
3.2.2 Solicite y revise los documentos que contienen los planes de seguridad.		
3.2.3 Solicite los planos de la instalación eléctrica y revise que:		
a. Se identifiquen todos los cables en sus diferentes recorridos.		
b. Las cajas de interruptores y circuitos tengan una buena disposición.		
c. Se identifiquen las protecciones que deben tener los cables.		
d. Existan indicaciones claras de conexiones a tierra.		
e. Se identifiquen las tomas generales y las de cómputo.		
3.2.4 Entreviste al personal encargado del mantenimiento del edificio, equipos y de las redes eléctricas.		
3.2.5 Revise y verifique todos los aspectos relacionados con las UPS y con la planta eléctrica.		

Procedimientos	*Hecho por:*	*Ref.*
3.3 Mantenimiento de la seguridad de las instalaciones.		
Objetivo: Comprobar la pertinencia del mantenimiento de la seguridad de las instalaciones.		
3.3.1 Cerciórese mediante inspección física, de la existencia y funcionamiento de:		
a. Detectores de humo		
b. Deshumecedores		
c. Extintores, verifique su mantenimiento y el material		
d. Recolectores de papel y basura		
e. Rótulos indicadores de prohibiciones		
f. Las alarmas		
g. Las anotaciones de números de teléfono de emergencias y autoridades competentes.		
h. Luces de emergencias		
i. Cobertores para los equipos		
j. Medidores de temperatura		
3.4 Controles de acceso físico		
Objetivo: Verificar las políticas establecidas en cuanto a los controles de acceso, su autorización y difusión.		
3.4.1 Cerciórese mediante observación e inspección, de las restricciones de acceso físico a los lugares no permitidos.		
a. Verifique si las puertas permanecen cerradas.		
b. Revise las identificaciones de los funcionarios y asegúrese que sean originales y pertenecen a quien las porta.		
c. Revise el procedimiento de asignación de las identificaciones.		
3.5 Controles de acceso al sistema CARMU		
Objetivo: Evaluar los controles de acceso del Sistema de Información CARMU.		
3.5.1 Solicite los documentos que contienen los diagramas y esquemas de seguridad de acceso.		

Procedimientos	***Hecho por:***	***Ref.***
3.5.2. Solicite los documentos que contienen los procedimientos para incluir o excluir un usuario, así como para modificar sus privilegios.		
3.5.3 Revise si los perfiles de usuarios están debidamente definidos y documentados.		
3.5.4 Resuma en hojas de hallazgo los aspectos sujetos de mejora.		

Hecho por:_____ Fecha:_____

Revisado por:_____ Fecha:_____

Aprobado por:_____ Fecha:_____

Cuestionario de Control Interno

Funcionario entrevistado
Puesto que ocupa:

Auditor encargado:
Fecha:

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
C. Seguridad Física				
a) Construcción				
1) ¿Es la construcción del centro de cómputo especial?				
2) ¿Qué especialidad tiene? ¿Paredes grandes y fuertes? ¿Material no inflamable? ¿Cielo raso reforzado? ¿Anti-magnetismo? ¿Varias puertas de acceso? ¿Que función cumplen las puertas de acceso?				
3) ¿Cuentan con salidas de emergencia? ¿De qué tipo son? ¿A qué lugar llevan?				
4) ¿Son seguros los accesos y las salidas de emergencia? ¿Abren sus puertas hacia afuera? ¿Son puertas corredizas? ¿Son las puertas de vidrio? ¿Las escaleras son firmes y antideslizantes? ¿Ha sucedido algún accidente?				
5) ¿Se han probado las salidas de emergencia? ¿Fueron los resultados positivos? ¿Se documentaron los pormenores?				

	Respuestas			
6) ¿Tienen instalaciones especiales en el cielo raso para instalar dispositivos de seguridad?				
7) ¿Pasan ductos de agua directamente encima del centro de cómputo, o de las bodegas?				
8) ¿Posee instalación eléctrica exclusiva para los equipos de cómputo? ¿Tiene medidor independiente? ¿Esta red cubre todo el edificio? ¿Cumple con los estándares generales y los específicos? ¿Está conectada a tierra? ¿Están todos los tomas polarizados? Están identificados los cables y los tomas?				
9) ¿Están los cables de poder y de señal en ductos? ¿Son los ductos de material especial? ¿Están separados de los cables de señal? ¿Cada uno va en un ducto diferente?				
10) ¿Se revisa la red y se le da mantenimiento constantemente? ¿Se anotan los resultados de la revisión? ¿Se efectúan correcciones? ¿Existen “pegas” y añadidos en los cables?				
11) ¿Existe una buena disposición de los interruptores y circuitos? ¿Son de fácil localización?				

	Respuestas			
¿Están a mano en caso de emergencia?				

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	**Observaciones**
12) ¿Existen y están disponibles los planos de la instalaciones eléctrica y de señal? ¿Están actualizados? ¿Tienen copias en lugares protegidos?				
13) ¿Cuentan con personal especializado para las pruebas, revisiones, el mantenimiento y las correcciones de todo lo relacionado con las instalaciones de cables, tendidos y otros?				
14) ¿Están las regletas o tomas adosadas a las paredes? ¿Se protegen los cables que están en el piso o que atraviesan oficinas?				
15) ¿Cuentan con protección de UPS (baterías)? ¿Cuantas y de qué tipo? ¿Existe una para el equipo principal? ¿Se midieron las potencias para determinar la protección adecuada? ¿Existe un plan de sustitución? ¿Se le da mantenimiento preventivo y correctivo?				
16) ¿Tienen planta eléctrica propia? ¿Está coordinada con la UPS? ¿Se conecta automáticamente? ¿Se le proporciona mantenimiento				

	Respuestas			
preventivo y correctivo? ¿Es solo para emergencias y para cómputo?				
17) ¿Cuentan con reguladores de voltaje? ¿Están los aires acondicionados conectados en la misma red que los equipos de cómputo? ¿Aplican las medidas de protección, revisión y atención, tanto para los cables de señal, como para los de poder?				
B. Ambiente				
1) ¿Cuentan con aire acondicionado en las instalaciones de equipo de cómputo? ¿Para el equipo de cómputo principal? ¿Se midió la cantidad de calor a disipar? ¿Cumplen los aires con la medida?				
2) ¿Tienen detectores de humo? ¿Funcionan automáticamente? ¿Accionan alguna alarma? ¿Llaman la atención del operador?				
3) ¿Pueden detectar y medir la humedad, especialmente en la oficina del equipo servidor y en las bodegas? ¿Tienen deshumecedores? ¿Funcionan adecuadamente?				
4) ¿Es adecuada la iluminación del centro de cómputo?				

	Respuestas			
¿Tienen luces especiales? ¿Tienen luces de emergencia?				

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	**Observaciones**
5) ¿Cuentan con extintores bien dispuestos? ¿Los saben utilizar? ¿Se les da mantenimiento? ¿Se han probado?				
6) ¿Tienen alarmas? ¿De que tipo? ¿Son automáticas o se activan manualmente? ¿Están conectadas con los bomberos?				
7) ¿Disponen de medidas de seguridad en caso de rayerías, tormentas, temblores e inundaciones?				
8) ¿Manejan material inflamable de algún tipo?				
9) ¿Se prohíbe el consumo de alimentos y bebidas en los lugares en donde están instalados equipos de cómputo, periféricos y especiales? ¿Existen rótulos indicadores de esas prohibiciones?				

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	**Observaciones**
C. Acceso				
1) ¿Existen restricciones de acceso físico a: Cuarto del servidor? Las bodegas? Ubicación de terminales de usuarios? Equipos especiales?				
2) ¿Permanecen cerradas las puertas de acceso? ¿Indefinidamente? ¿Bajo que condiciones se abren?				
3) ¿Utilizan códigos, identificaciones o combinaciones para ingresar?				
4) ¿Cuentan con bitácoras de visitas?				
5) ¿Existen restricciones de acceso para horas o días no hábiles?				
D. Seguros				
1) ¿Existen pólizas de seguros para la protección de los activos de cómputo y otros?				
2) ¿Son adecuadas las coberturas?				

	Respuestas			
¿Que criterios utilizaron para establecerlas?				
3) ¿Se actualizan las pólizas de seguros cada vez que se incluye o se excluye, algún activo de cómputo?				

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	**Observaciones**
4) ¿Incluyen las pólizas, coberturas por: Incendio? Temblor o terremoto? Inundaciones? Sabotaje? Robo? Daño? Tormenta o Huracán? Disturbios civiles?				
E. Mantenimiento				
1) ¿Se han firmado contratos de mantenimiento preventivo y correctivo para los equipos principales, dispositivos y equipos especiales?				
2) ¿Se han negociado favorablemente estos contratos?				
3) ¿Se les proporciona verdadero mantenimiento a esos equipos? No solo limpieza.				
4) ¿Incluye el mantenimiento correctivo los repuestos o no? ¿Si no los incluye, se cotizan de acuerdo con el procedimiento de compras normal?				

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	**Observaciones**
5) ¿Se tienen planes de mantenimiento por escrito? ¿Se especifica en ellos los días y las horas, en que a los equipos se les dará mantenimiento? ¿Es conocido este plan por las personas que tienen equipos a su cargo? ¿Funciona el plan efectivamente?				
6) ¿Se lleva una bitácora para el mantenimiento de cada equipo? ¿Se anotan en ella los pormenores del mantenimiento?				
7) ¿Cuando deben llevarse equipos a reparar, se entrega el mismo bajo un inventario, con anotaciones de números de serie, incluso de los dispositivos y tarjetas internos?				

	Respuestas			
8) ¿Cuando regresan los equipos se revisan y cotejan con e inventario con que fueron entregados?				
9) ¿Se toman las medidas de seguridad pertinentes con respecto a la información que contengan los discos duros de los equipos a reparar?				

Ministerio de Seguridad Pública
Auditoría General

Cuestionario de Control Interno

Funcionario entrevistado: Auditor encargado:
Puesto que ocupa: Fecha:

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
A. Seguridad general				
1) ¿Están centralizadas las funciones de administración de la seguridad lógica del sistema CARMU? ¿Quién o quienes realizan estas funciones?				
2) ¿Cuentan con un procedimiento formal y por escrito para incluir o excluir un usuario, así como para modificar sus privilegios?				
3) ¿Se le ha dado divulgación a este procedimiento? ¿Lo conocen todos los funcionarios de la organización?				
4) ¿Disponen de un estándar, como tiempo de respuesta para incluir, excluir o modificar usuarios? ¿Cuál es ese tiempo de respuesta?				
5) ¿Existen perfiles definidos y por escrito de cada uno de los usuarios del sistema? ¿Existe un formulario estándar para la definición de esos perfiles? ¿Quién define los perfiles?				

Ministerio de Seguridad Pública
Auditoría General

Cuestionario de Control Interno

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
6) ¿Se cambian las claves de acceso con frecuencia? ¿Cada cuánto tiempo?				
7) ¿Pueden los usuarios cambiar sus claves de acceso? ¿Lo están haciendo? ¿Con qué frecuencia?				
8) ¿Vencen de manera automática los tiempos de uso o aplicación de las claves de acceso?				
9) ¿Está supeditado el uso de las claves de acceso a horarios de trabajo diarios y a días hábiles? ¿Qué horario y cuáles días?				
10) ¿Tienen en operación un plan de contingencia? ¿Contiene los aspectos de toda la organización? ¿Esta por escrito, revisado y aprobado? ¿Se ha probado y se prueba por lo menos una vez al año? ¿Contiene todos los procedimientos necesarios? ¿Contiene el plan de recuperación en caso de desastre?				

Ministerio de Seguridad Pública
Auditoría General

Cuestionario de Control Interno

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
B. Seguridad Lógica				
1) ¿Cuentan con diagramas de los esquemas de seguridad? ¿Forman parte de la documentación de los sistemas?				
2) ¿Incluyen los esquemas de seguridad: Los códigos de usuario?. Las claves de acceso? ¿Las terminales autorizadas? ¿Los diferentes niveles de seguridad? ¿Los derechos y privilegios de cada usuario?				
3) ¿Describe el procedimiento correspondiente, los pasos a seguir para establecer los conceptos anteriores?				
4) ¿Se utilizan estándares para la asignación de códigos de usuario y claves de acceso?				
5) ¿Incluyen estos estándares aspectos como: ¿Caracteres a utilizar? ¿Tamaños de los conceptos? ¿Prohibiciones?				
6) ¿Se asignan las claves de acceso mediante la aplicación de un algoritmo complejo? ¿Puede el usuario cambiar su propia clave de acceso?				

Ministerio de Seguridad Pública
Auditoría General

Cuestionario de Control Interno

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
7) ¿Incluye el procedimiento de asignación de claves, aspectos como: ¿Una solicitud del usuario jefe con indicaciones claras de los accesos autorizados? ¿Los tiempos vigentes de duración de las claves? ¿Si vencen automáticamente después de ese tiempo? ¿Qué hacer en caso que el usuario olvide su clave? ¿Cómo proceder cuando un usuario deja la organización?				
8) ¿Existe algún manual de seguridad lógica?				
9) ¿Existen perfiles predefinidos para los usuarios? ¿Quién genera estos perfiles?				
10) ¿Existe un sistema de encríptamiento para las claves? ¿Se desarrollo internamente o se compró? ¿Quién o quienes lo conocen? ¿En donde se custodia?				
11) ¿Existen acceso privilegiados? ¿De qué tipo?				

Cuestionario de Control Interno

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
12) ¿Conocen todos los usuarios la responsabilidad que asumen al tener una clave de acceso? ¿Se les ha comunicado? ¿Está en la descripción de funciones? ¿La respetan? ¿Se aplican sanciones para quién haga uso indebido de su clave, o que utilice la clave de otra persona?				
13) ¿Se cuenta con una lista actualizada de los usuarios, con: ¿Los sistemas, módulos, menús, opciones de menú, a que tienen acceso? ¿Los códigos de usuario? ¿Oficina, departamento o área en que trabaja? ¿Funciones que desempeña? ¿Terminales autorizadas?				
14) ¿Están ligadas las claves de acceso a: -Días hábiles de uso? -Horas hábiles de uso? -Terminales autorizadas?				
15) ¿Seguridad del Sistema Operativo, se utiliza la seguridad que tienen: -El sistema operativo? -El Administrador de la bases de datos? -El sistema operativo de redes? -Las herramientas de desarrollo? -Los dispositivos de comunicaciones?				

Ministerio de Seguridad Pública
Auditoría General

Cuestionario de Control Interno

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
16) ¿Cuentan con alguna(s) herramienta(s) adicional(es) para seguridad lógica? ¿De qué tipo es? ¿Qué nivel de seguridad brinda? ¿Es complementaria a la seguridad existente o es la principal? ¿Su adquisición se debió a debilidades en la seguridad principal, o como soporte adicional? ¿Requiere de mucho almacenamiento y recursos?				
17) ¿Existen restricciones de acceso a directorios, bibliotecas o espacios para tablas? ¿De que tipo? ¿Se protegen con un programa de seguridad especial? ¿Es un paquete o un programa hecho a la medida? ¿Se controlan los accesos a estos elementos?				
18) ¿Tienen bitácoras automatizadas en donde queden registrados todos los eventos relacionados con todos los accesos autorizados y los intentos rechazados? ¿Están activadas ¿Las revisa algún funcionario autorizado? ¿Se han detectado anomalías en los accesos? ¿Se ha tomado alguna acción al respecto?				

Ministerio de Seguridad Pública
Auditoría General

Cuestionario de Control Interno

	Respuestas			
Preguntas	**SI**	**NO**	**N/A**	
19) ¿Proporcionan esas bitácoras, toda la información relacionada con los accesos?				
20) ¿Se guarda la información de las bitácoras por un tiempo determinado? ¿Por cuanto tiempo? ¿Se desecha la información de las bitácoras de ese tiempo? ¿Se guarda en algún dispositivo magnético por un tiempo adicional? ¿Cuanto? ¿Se lista el contenido de las bitácoras en algún momento? ¿Utiliza algún funcionario estos listados?				