Deja sin vigencia DGG N° 02-GG-2020 del 24.02.2020

DIRECTIVA DE GERENCIA GENERAL

NORMAS Y PROCEDIMIENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

DGG N° 11-GG-2021

San Isidro, 19/08/2021

1. FINALIDAD

Establecer las disposiciones, actividades y responsabilidades referidas al Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C) en la Caja de Pensiones Militar Policial (CPMP), respecto a los requisitos de la NTP ISO/IEC 27001:2014.

2. REFERENCIA LEGAL Y NORMATIVA

- Decreto Ley Nº 21021 – Ley de Creación de la Caja de Pensiones Militar-Policial y sus modificatorias
- Decreto Supremo Nº 005-75-CCFA – Reglamento del Decreto Ley Nº 21021 y sus modificatorias
- Decreto Ley Nº 19846 – Ley de Pensiones Militar Policial
- Decreto Supremo Nº 009-DE-CCFA – Reglamento de la Ley de Pensiones Militar - Policial
- Decreto Legislativo Nº 1133 – Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial y sus modificatorias
- Decreto Supremo Nº 101-2021-EF – Normas Reglamentarias y Complementarias del Decreto Legislativo N° 1133, Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial
- Circular SBS Nº G-140-2009 – Gestión de la Seguridad de la Información
- NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información. Requisitos
- Resolución Ministerial Nº 004-2016-PCM – Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática y sus modificatorias
- Resolución Ministerial N° 119-2018-PCM – Disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública y sus modificatorias

- Resolución SBS Nº 504-2021 – Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad
- Ley Nº 29733 – Ley de Protección de Datos Personales y sus modificatorias
- Decreto Supremo Nº 003-2013-JUS – Reglamento de la Ley de Protección de Datos Personales y sus modificatorias
- Manual de Organización y Funciones de la Caja de Pensiones Militar Policial
- Manual de Descripción de Cargos de la Caja de Pensiones Militar Policial
- Directiva de Consejo Directivo DCD Nº 10-2021 – "Políticas y Objetivos de Seguridad de la Información y Ciberseguridad"

3. ALCANCE

Las disposiciones contenidas en la presente directiva comprenden a la Gerencia de Informática, al Departamento de Riesgos Operacionales, al Departamento de Planeamiento y Organización y a todas las demás unidades orgánicas de la CPMP.

4. DISPOSICIONES GENERALES

4.1 Contexto de la CPMP

4.1.1 Conocimiento de la CPMP y su contexto

a) El análisis de contexto es el entendimiento de la CPMP y de sus objetivos, así como la determinación de aspectos internos y externos que son relevantes para este propósito y que puedan afectar (favorecer o perjudicar) la capacidad de lograr los resultados deseados del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C).

b) Se definen los siguientes factores externos e internos que influyen en la CPMP:

- Externos: partes interesadas externas, entorno reglamentario y legal, entorno competitivo, entorno cultural, tendencias en tecnología, entre otros.
- Internos: partes interesadas internas, normativa interna, procesos, recursos y tecnología.

4.1.2 Requisitos de seguridad de las partes interesadas

Los requisitos son las obligaciones o metas que la CPMP tiene respecto a la seguridad de información, provienen de diversas partes interesadas. Estos pueden originarse en leyes, normas internas, contratos, metas establecidas o expectativas de las partes interesadas.

4.1.3 Determinación del alcance del SGSI-C

El alcance establece los límites y aplicabilidad del Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSI-C), el cual comprende los procesos, activos y personas que están involucrados.

4.1.4 El SGSI-C cuenta con las siguientes etapas de operación:

a) Establecimiento:

- Establecer políticas, procedimientos y responsabilidades en seguridad de información y ciberseguridad.
- Definir los requisitos y objetivos de seguridad de información y ciberseguridad.
- Definir el alcance del SGSI-C.

b) Implementación:

- Gestionar los riesgos relacionados a la seguridad de información y ciberseguridad.
- Realizar la capacitación y concientización en seguridad de información y ciberseguridad.
- Implementar los controles requeridos por la CPMP.

c) Mantenimiento:

- Medición de indicadores.
- Auditorías internas al SGSI-C.
- Revisiones por el Consejo Directivo.

d) Mejora:

- Ejecutar acciones correctivas y de mejora.

4.2 Liderazgo

4.2.1 Liderazgo y compromiso

a) El liderazgo y compromiso con la seguridad de información y ciberseguridad y el SGSI-C, se evidencian con la aprobación de la documentación requerida por su función y facilita los recursos para mantener la operación del SGSI-C, empoderando a los responsables de dirigir y participar de la operación del SGSI-C y promoviendo su mejora continua.

b) El Consejo Directivo revisa y aprueba la documentación requerida por el SGSI-C: políticas, lineamientos, planes, objetivos y la estructura organizacional.

c) El Comité Especializado en Seguridad de la Información y Ciberseguridad tiene las siguientes responsabilidades:

- Solicita los recursos para la realización de las actividades del SGSI-C:

  i. Participación del personal en la gestión de riesgos, capacitaciones, auditorías y otras reuniones de trabajo del SGSI-C.
  ii. Las actividades y proyectos relacionados a fortalecer la seguridad de información.

- Presenta un informe, al finalizar cada periodo de la operación del SGSI-C, para la revisión de la Gerencia General y Comité de Riesgos y, si es necesario, solicita modificaciones sobre el SGSI-C.

d) El Oficial de Seguridad de la Información y Ciberseguridad realiza la supervisión y cumplimiento que el SGSI-C se implemente conforme a los requisitos de seguridad de la información y ciberseguridad. Asimismo, realiza la supervisión y cumplimiento de la presente directiva.

e) El Consejo Directivo aprueba el presupuesto para la disposición de los recursos técnicos, de personal, financieros requeridos para la implementación y adecuado funcionamiento del SGSI-C.

4.2.2 Política

La política de seguridad de información y ciberseguridad establece las disposiciones que norman la seguridad de información y ciberseguridad en la CPMP, y está enfocada en el negocio y sus metas, en ese sentido, incorpora los objetivos de seguridad de información y ciberseguridad, y se compromete con la protección de la información, los datos personales y los ciberactivos, con los requisitos de seguridad aplicables; y con la mejora continua del SGSI-C.

4.2.3 Roles, responsabilidades y autoridades de la CPMP

Los roles y responsabilidades implican la asignación de responsables para llevar a cabo tareas específicas de seguridad de la información por parte de

las personas adecuadas dentro de la CPMP. Asimismo, comprenden las actividades operativas y de dirección en relación a la gestión de la seguridad de información y ciberseguridad, la cual se realiza, para los procesos dentro del alcance definido en el SGSI-C.

4.3 Planificación

4.3.1 Acciones para tratar los riesgos y las oportunidades

a) Generalidades

Entendiendo el contexto de la CPMP y las necesidades de las partes interesadas previamente determinadas se establecen actividades encaminadas a establecer los riesgos y oportunidades que será necesario tratar.

b) Evaluación de riesgos de seguridad de la información y ciberseguridad

La evaluación de riesgos comprende la definición y selección de aquellos riesgos más significativos para la CPMP, respecto a la seguridad de información y ciberseguridad.

c) Tratamiento de riesgos de la seguridad de la información y ciberseguridad

El tratamiento de riesgos consiste en planificar y realizar la atención de los riesgos priorizados (definidos como no aceptables) en la evaluación de riesgos.

4.3.2 Objetivos de seguridad de la información y planificación para alcanzarlos

Los objetivos de seguridad de información establecen las metas que tiene la CPMP sobre la confidencialidad, integridad y disponibilidad de su información. Toman como base los objetivos estratégicos institucionales, alineados a la Directiva de Consejo Directivo sobre Políticas y Objetivos de Seguridad de la Información y Ciberseguridad, y son formulados tomando en cuenta los requisitos de seguridad de información y ciberseguridad más importantes.

4.4 Soporte

4.4.1 Recursos

Comprende los recursos técnicos, de personal y financieros requeridos para la implementación, adecuado mantenimiento y mejora continua del SGSI-C, los cuales se ven reflejados en sus planes.

4.4.2 Competencias

Las competencias se asocian a los roles principales del SGSI-C y la capacidad que estos tienen para asumirlos, las cuales son obtenidos mediante capacitaciones, evaluaciones y la práctica en sus funciones.

4.4.3 Sensibilización

La sensibilización informa y predispone al personal para el cumplimiento de la política de seguridad de la información y ciberseguridad, y los objetivos de la CPMP. Se realiza periódicamente y se centra en el personal que forma parte del alcance del SGSI-C.

4.4.4 Comunicación

Las comunicaciones establecen aquellos intercambios de información que, necesariamente, deben realizarse entre los operadores del SGSI-C como resultado de su operación y se establece los actores, medios, circunstancias y demás condiciones.

4.4.5 Información documentada

a) Generalidades

El SGSI-C deja constancia de la efectividad de su operación mediante los registros obtenidos al ejecutar todas las actividades.

b) Creación y actualización

El SGSI-C establece formatos para la normalización de los registros de operación, algunos de los cuales están sujetos a la aprobación mediante firmas y control de versiones.

c) Información documentada

El SGSI-C tiene definida la ubicación donde aloja la documentación que recibe y produce, así como también restricciones relacionadas al manejo de aquellos registros que sean considerados como confidenciales, de esta manera controla su disponibilidad cuando sea necesaria y que se encuentre adecuadamente protegida.

El Oficial de Seguridad de la Información y Ciberseguridad administra el acceso a la carpeta (digital) del SGSI-C.

4.5 Operación

4.5.1 Planificación y control operacional

El control sobre la operación del SGSI-C implica:

a) Implementar lo establecido en el plan de objetivos de seguridad de información y ciberseguridad.

b) Realizar seguimiento a los cambios realizados mediante el plan de acciones correctivas.

c) Plan de acciones de mejora.

4.5.2 Evaluación de los riesgos de seguridad de la información y ciberseguridad

La evaluación de riesgos implica realizar periódicamente las actividades definidas en el numeral 5.2.2.

4.5.3 Tratamiento de los riesgos de seguridad de la información y ciberseguridad

El tratamiento de riesgos implica realizar periódicamente las actividades definidas en el numeral 5.2.3.

4.6 Evaluación del desempeño

4.6.1 Monitoreo, medición, análisis y evaluación

Las métricas definidas desde el SGSI-C aplican a medir: objetivos de seguridad de información y ciberseguridad, estado de controles de seguridad de información y ciberseguridad relevantes, estado de la operación del SGSI-C.

4.6.2 Auditorías internas

La Unidad de Auditoría Interna evalúa el cumplimiento del SGSI-C respecto a los requisitos de la NTP ISO/IEC 27001:2014, además, de otros requisitos aplicables a la CPMP sobre la seguridad de su información en relación a objetivos específicos. Inicia con la preparación del plan de auditoría, la ejecución de las actividades establecidas en dicho plan, el reporte de los resultados mediante el informe de auditoría y la generación posterior de acciones correctivas (para las no conformidades) y de mejora (para las recomendaciones).

4.6.3 Revisión

El Comité de Riesgos revisa periódicamente el informe presentado por el Comité Especializado en Seguridad de la Información y Ciberseguridad, respecto a los resultados del SGSI-C.

Los resultados del SGSI-C son presentados al Consejo Directivo para su conocimiento, al menos de manera anual.

4.7 Mejoras

4.7.1 No conformidad y acción correctiva

Una no conformidad es un incumplimiento de algún requisito de la Norma Técnica Peruana ISO/IEC 27001:2014 o por los propios requisitos de la seguridad de información y ciberseguridad, establecidos en su política o determinado por alguna de las partes interesadas, se puede originar en un incidente, una métrica con bajo valor, el hallazgo de una auditoría o una revisión del Consejo Directivo. Para subsanarla se crea una acción correctiva que cuenta con un responsable, recursos y un plazo para su implementación (plan de acciones correctivas).

4.7.2 Mejora continua

Una mejora puede provenir de una recomendación de alguna parte interesada, una recomendación del Jefe de Auditoría Interna de la CPMP, un acuerdo de los participantes de la revisión por la dirección e incluso de lecciones aprendidas debido a la ocurrencia de incidentes de seguridad de la información y ciberseguridad. Para implementarla se crea una acción correctiva que cuenta con un responsable, recursos y un plazo para su implementación (plan de acciones correctivas).

5. DESCRIPCIÓN DE LOS PROCEDIMIENTOS

5.1 Establecimiento de políticas, alcance y responsabilidades

5.1.1 Conocimiento de la CPMP, contexto y requisitos de seguridad de las partes interesadas

a) El Oficial de Seguridad de la Información y Ciberseguridad, al iniciar cada ciclo de operación del SGSI-C, con apoyo del Departamento de Planeamiento y Organización y la Gerencia de Informática, indaga los cambios significativos a nivel de procesos y tecnología en la CPMP.
Si existe algún cambio relevante, actualiza el análisis de contexto.

b) El Oficial de Seguridad de la Información y Ciberseguridad revisa si existen nuevos requisitos normativos o si los anteriores siguen vigentes y son relevantes para la CPMP.

Si existe algún cambio relevante en la CPMP, actualiza los requisitos de seguridad de la información y ciberseguridad.

5.1.2 Determinación del alcance del SGSI-C

a) El Oficial de Seguridad de la Información y Ciberseguridad o las unidades orgánicas reevalúan el alcance en función al análisis del contexto y a los requisitos de seguridad de la información y ciberseguridad; y proponen, si fuera necesario, una actualización, documentando cómo se determinó el nuevo alcance.

b) Si existe una nueva propuesta de alcance, el Comité Especializado en Seguridad de la Información y Ciberseguridad revisa y aprueba o descarta el nuevo alcance propuesto.

5.1.3 Determinación de políticas, roles y responsabilidades

a) El Oficial de Seguridad de la Información y Ciberseguridad al cambiarse, suprimirse o desdoblarse una función del SGSI-C, actualiza la presente directiva, si corresponde, el contenido de la política de seguridad de la información y ciberseguridad, que norma el rol modificado.

b) Cuando se dispone cambios sobre la Directiva de Consejo Directivo de Políticas y Objetivos de Seguridad de Información y Ciberseguridad, el Oficial de Seguridad de la Información y Ciberseguridad realiza las siguientes actividades:

- Propone la actualización de la directiva.
- Realiza seguimiento a su aprobación por el Consejo Directivo.
- Solicita la publicación en la Intranet y en el portal previsional de la CPMP.

5.2 Gestión de riesgos relacionados a la seguridad de la información y ciberseguridad

5.2.1 Acciones para tratar los riesgos y las oportunidades

a) El Oficial de Seguridad de la Información y Ciberseguridad organiza un equipo multidisciplinario compuesto, por lo menos, por personal del Departamento de Riesgos Operacionales, personal de la Gerencia de Informática y personal de los procesos sobre los cuales se realizará la gestión de riesgos.

b) El Oficial de Seguridad de la Información y Ciberseguridad establece un cronograma para ejecutar la gestión de riesgos.

c) El Oficial de Seguridad de la información y Ciberseguridad, identifica con las unidades orgánicas involucradas, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y la necesidad de operar.

d) El Oficial de Seguridad de la Información y Ciberseguridad, en coordinación con la Gerencia de Informática, identifica los dispositivos que se conectan a la red interna y todo *software* que se encuentre instalado en la infraestructura tecnológica, y asegura que se encuentren acorde a una configuración segura previamente establecida.

e) El Oficial de Seguridad de la Información y Ciberseguridad, en coordinación con la Gerencia de Informática, identifica las cuentas de usuarios con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar *software* a la infraestructura, y mantener el principio de mínimos privilegios otorgados.

f) El Oficial de Seguridad de la Información y Ciberseguridad, en coordinación con la Gerencia de Informática, implementa, y mantiene una línea base de seguridad en sistemas operativos y aplicaciones utilizadas, incluidos los correspondientes a dispositivos móviles, estaciones de trabajo, servidores y dispositivos de comunicaciones. Asimismo, identifica y evalúa la habilitación de las funciones de seguridad integradas en los sistemas operativos.

g) El Oficial de Seguridad de la Información y Ciberseguridad, prioriza y gestiona las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios.

h) El Oficial de Seguridad de la Información y Ciberseguridad, desarrolla una campaña de orientación para la adopción de prácticas seguras dirigida a los colaboradores, plana gerencial y miembros del Consejo Directivo.

i) El Oficial de Seguridad de la Información y Ciberseguridad, en caso la CPMP provea alguna de las operaciones por canal digital, en lo que corresponda a su implementación, cumple con la implementación de los procesos de autenticación.

j) El Oficial de Seguridad de la Información y Ciberseguridad, en el caso utilice servicios significativos provistos por terceros, en lo que corresponda a su implementación, en aspectos referidos a gestión de tecnología de la información, a gestión de seguridad de la información o a procesamiento de datos, debe:

i. Evaluar las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios e implementar medidas de tratamiento.
ii. Asegurar que el arreglo contractual con el proveedor y su implementación le permiten cumplir con las obligaciones establecidas en la presente directiva.
iii. Establecer los roles y responsabilidades que el proveedor asume contractualmente sobre la seguridad de la información y asegurar que la CPMP efectúe las implementaciones complementarias correspondientes para la atención de los requerimientos de la presente directiva.

Cabe señalar que, para fines de la presente directiva, un proveedor es considerado como un tercero contratado para brindar bienes y/o servicios a la CPMP, incluso bajo la modalidad de subcontratación. Las empresas que forman parte del Grupo Corporativo de la CPMP, también son consideradas como terceros.

k) La CPMP mantiene con carácter permanente un programa de ciberseguridad aplicable a las operaciones, procesos y otros activos de información asociados.

El programa de ciberseguridad debe prever un diagnóstico y un plan de mejora sobre sus capacidades de ciberseguridad, que le permita cuando menos lo siguiente:

i. Identificación de los activos de información.
ii. Protección frente a las amenazas a los activos de información.
iii. Detección de incidentes de ciberseguridad.
iv. Respuesta con medidas que reduzcan el impacto de los incidentes.
v. Recuperación de las capacidades o servicios tecnológicos que pudieran ser afectados.
vi. Reporte de incidentes de ciberseguridad significativas.

l) El Oficial de Seguridad de la Información y Ciberseguridad inicia la gestión de riesgos tomando como referencia la metodología de gestión de riesgos de seguridad de la información y ciberseguridad, y las acciones descritas desde el literal c) a la k) del numeral 5.2.1.

5.2.2 Evaluación de riesgos de seguridad de la información y ciberseguridad

a) El Oficial de Seguridad de la Información y Ciberseguridad evalúa si se van a modificar los criterios y umbrales para valorizar y estratificar los riesgos en la metodología (parametrización).

b) El Oficial de Seguridad de la Información y Ciberseguridad identifica los riesgos de seguridad de información y ciberseguridad y sus propietarios:

- Identifica activos.
- Valoriza activos.
- Identifica riesgos.

c) El Oficial de Seguridad de la Información y Ciberseguridad analiza los riesgos identificados:

- Identifica controles.
- Evalúa la probabilidad.
- Evalúa el impacto de consecuencias.

d) El Oficial de Seguridad de la Información y Ciberseguridad valoriza los riesgos analizados:

- Calcula nivel de riesgo.

5.2.3 Tratamiento de riesgos de seguridad de la información y ciberseguridad

a) El Oficial de Seguridad de la Información y Ciberseguridad propone, valida y documenta las alternativas de tratamiento de riesgos con los propietarios del riesgo.

b) El Oficial de Seguridad de la Información y Ciberseguridad propone medidas mínimas de seguridad de la información a adoptar por la CPMP, para el tratamiento de:

- Seguridad de los recursos humanos.
- Controles de acceso físico y lógico.
- Seguridad en las operaciones.
- Seguridad en las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de ciberseguridad.
- Seguridad física y ambiental.
- Gestión de activos de información.

c) El Oficial de Seguridad de la Información y Ciberseguridad actualiza los controles aplicables en la "Declaración de Aplicabilidad de Controles" (anexo 1).

5.3 Realización de capacitaciones y sensibilización

5.3.1 El Oficial de Seguridad de la Información y Ciberseguridad, al incorporar a nuevo personal a la operación del SGSI-C o si ha transcurrido un periodo considerable desde la última capacitación o charla de sensibilización:

a) Realiza las charlas establecidas en el plan de capacitación y sensibilización.

b) Evalúa al personal participante en las charlas para verificar su competencia.

c) Entrega el material de reforzamiento de capacitación.

5.4 Mantenimiento

5.4.1 El plan de auditoría interna del SGSI-C es ejecutada por la unidad de auditoria interna.

5.4.2 La auditoría externa del SGSI-C puede ser ejecutada cuando lo determine el ente de control o el supervisor.

5.4.3 Revisión del Comité de Riesgos

a) El Oficial de Seguridad de la Información y Ciberseguridad elabora el informe trimestral de operación del SGSI-C.

b) El Comité Especializado en Seguridad de la Información y Ciberseguridad participa en la revisión del informe, el mismo que contiene como mínimo: el inventario de activos de información, la identificación y evaluación de los riesgos de seguridad, el seguimiento a los planes de acción, e indicadores de gestión. Asimismo, opina, toma decisiones y brinda conformidad respecto a los resultados presentados.

c) El Comité de Riesgos revisa el informe entregado por el Comité Especializado en Seguridad de la Información y Ciberseguridad, y suscribe el acta.

5.5 Mejoras

5.5.1 No conformidad y acción correctiva

a) Si se presenta un incidente que afecte a la CPMP, un resultado adverso en las métricas, un hallazgo no conforme durante la auditoría o un cuestionamiento durante la revisión del Consejo Directivo, el Oficial de Seguridad de la Información y Ciberseguridad propone y valida con el Comité Especializado en Seguridad de la Información y Ciberseguridad y con las partes interesadas una estrategia de acción.

b) El Oficial de Seguridad de la Información y Ciberseguridad documenta la estrategia de acción en los planes de acciones correctivas y de mejora.

c) El Oficial de Seguridad de la Información y Ciberseguridad realiza el seguimiento al plan hasta que sea implementado.

5.5.2 Mejora continua

a) Si se presenta una propuesta de mejora, una observación o recomendación durante la auditoría, o a pedido del Consejo Directivo, el Oficial de Seguridad de la Información y Ciberseguridad propone y valida con la parte interesada una estrategia de acción.

b) El Oficial de Seguridad de la Información y Ciberseguridad, documenta la estrategia en los planes de acciones correctivas y de mejora.

c) El Oficial de Seguridad de la Información y Ciberseguridad, realiza el seguimiento al plan hasta que sea implementado.

6. DISPOSICIONES COMPLEMENTARIAS

Quedan sin efecto la Directiva de Gerencia General DGG Nº 02-GG-2020 y otras disposiciones que contravengan la presente directiva.

7. ANEXOS

- Anexo 1: Declaración de aplicabilidad de controles.

CAJA DE PENSIONES MILITAR POLICIAL

RICARDO MEDINA PALOMINO
Gerente General (e)

DGG N° 11-GG-2021
Anexo 1

DECLARACIÓN DE APLICABILIDAD DE CONTROLES

Lista de controles requeridos por la CPMP, la razón de su necesidad, así como también el estado que cada uno de estos presenta en la actualidad. En cada caso se muestra la relación que existe con el Anexo A del estándar NTP ISO/IEC 27001:2014.

A continuación, se declaran todos los controles implementados y en proceso de implementación (subrayados) los cuales son identificados como necesarios para la CPMP:

Dominio	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)