Deja sin vigencia DCD N° 10-2021 del 23.07.2021

DIRECTIVA DE CONSEJO DIRECTIVO

POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

DCD N° 01-2026

San Isidro, 12/02/2026

ÍNDICE

1. FINALIDAD

Establecer los lineamientos generales y compromisos de la Caja de Pensiones Militar Policial (CPMP) para el diseño, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de su Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C), garantizando la confidencialidad, integridad, disponibilidad de la información de acuerdo con los principios de la normativa de Gobierno Digital. Esta política proporciona un marco para el establecimiento de los objetivos de seguridad de la información y reafirma el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

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 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 Nº 1133, Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial, y sus modificatorias
- Decreto Ley Nº 19846 – Ley de Pensiones Militar Policial y sus modificatorias
- Decreto Supremo Nº 009-DE-CCFA – Reglamento de la Ley de Pensiones Militar Policial y sus modificatorias
- Decreto Supremo Nº 126-2025-PCM – Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento
- Decreto de Urgencia N° 007-2020 – Aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y sus modificatorias
- Decreto Supremo N° 002-97-TR Texto Único Ordenado del D. Leg. Nº 728 – Ley de Formación y Promoción Laboral.
- Decreto Supremo Nº 021-2019-JUS - Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública
- Decreto Supremo Nº 007-2024-JUS - Reglamento de la Ley de Transparencia y Acceso a la Información Pública
- Resolución de Contraloría General Nº 320-2006-CG – Normas de Control Interno
- Resolución Directoral N° 022-2022-INACAL/DN que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.
- Resolución SBS Nº 2116-2009 – Reglamento para la Gestión del Riesgo Operacional y sus modificatorias
- Resolución SBS Nº 272-2017 – Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos y sus modificatorias

- Resolución SBS Nº 504-2021 – Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad y sus modificatorias
- Resolución Ministerial Nº 119-2018-PCM – Disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública y sus modificatorias
- Resolución de Secretaría de Gobierno y Transformación Digital Nº 003-2023-PCM/SGTD - Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas
- Resolución SBS Nº 877-2020 – Reglamento para la Gestión de la Continuidad del Negocio
- Resolución Ministerial Nº 320-2021-PCM - Lineamientos para la gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de gobierno
- Resolución Secretarial de Gobierno y Transformación Digital Nº 002-2023-PCM/SGTD que aprueban la Directiva Nº 001-2023-PCM/ SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital
- Resolución Secretarial Nº 001-2018-PCM/SEGDI, que aprueba los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano
- Resolución de Gerencia General Nº 042-2023-/CPMP-GG - Reconformación del Comité de Gobierno y Transformación Digital de la CPMP
- Resolución de Gerencia General Nº 001-2024/CPMP-GG - Designación del Jefe de Infraestructura y Seguridad Informática de la Gerencia de Informática - Oficial de Seguridad y Confianza Digital de la CPMP
- Resolución de Gerencia General Nº 011-2024/CPMP-GG - Reconformación del Equipo de respuestas ante incidentes de seguridad digital de la CPMP
- Resolución de Gerencia General Nº 031-2024/CPMP-GG – Designación del Gerente de Informática como Oficial de Gobierno de Datos de la CPMP
- Ley Nº 29733 - Ley de Protección de Datos Personales y sus modificatorias
- Decreto Supremo Nº 016-2024-JUS – Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales
- Resolución Directoral N° 019-2013-JUS/DGPDP que aprueba la Directiva de seguridad para el tratamiento de datos personales
- Resolución Directoral Nº 100-2025-JUS-DGTAIPD que aprueba la Directiva que establece las disposiciones para la designación, desempeño y funciones del Oficial de Datos Personales.
- Ley Nº 30096 - Ley de Delitos Informáticos y sus modificatorias
- Ley Nº 31572 - Ley del Teletrabajo y sus modificatorias
- Decreto Supremo Nº 002-2023-TR - Reglamento de la Ley Nº 31572 – Ley del Teletrabajo
- Manual de Organización y Funciones de la Caja de Pensiones Militar Policial
- Manual de Descripción de Cargos de la Caja de Pensiones Militar Policial
- Reglamento Interno de Trabajo de la Caja de Pensiones Militar Policial
- Directiva de Consejo Directivo DCD Nº 14-2024 – Reglamento del Comité de Riesgos
- Directiva de Consejo Directivo DCD Nº 15-2020 – Políticas y Objetivos de Continuidad del Negocio

- Directiva de Gerencia General Nº 08-GG-2020 – Normas y Procedimientos del Sistema de Gestión de Continuidad del Negocio (SGCN)
- Directiva de Gerencia General Nº 01-GI-2015 – Normas y Procedimientos para la Gestión de Incidentes en la Infraestructura Informática
- Directiva de Gerencia General Nº 02-GI-2024 – Normas y Procedimientos para la Administración de Accesos a los Servicios Informáticos
- Directiva de Gerencia General Nº 03-GI-2024 – Normas y Procedimientos para la Administración de Hardware, Software y Servicios Informáticos
- Directiva de Gerencia General Nº 04-GI-2024 – Plan de Seguridad Informática Institucional
- Directiva de Gerencia General Nº 02-GAF-2024 – Normas para la Entrega de Cargos del Personal
- Directiva de Gerencia General Nº 05-GI-2021 – Plan de Continuidad de Servicios Informáticos

3. ALCANCE

Los lineamientos contenidos en la presente directiva son de cumplimiento obligatorio por parte de todas las unidades orgánicas de la CPMP, así como de las personas naturales o jurídicas que brindan servicios o prestaciones a la entidad y tengan acceso a la información que se genera, procesa, resguarda y/o administra.

4. DEFINICIONES

4.1 Acceso remoto: Acceso desde un equipo de cómputo hacia un recurso informático de la CPMP ubicado físicamente en otro lugar, puede darse a través de diferentes técnicas como VPN, escritorio virtual, u otro autorizado.

4.2 Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

4.3 Activos de información: Información y otros activos asociados de los que dependen la información como bienes, servicios tangibles o intangibles y personas, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos de negocio los cuales están alineados a sus objetivos planteados.

4.4 Activos de TI: Está referido a los activos de Tecnologías de la Información, que son los recursos tecnológicos con los que cuenta una organización como el software, hardware y servicios.

4.5 Anonimización: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

4.6 Amenaza: Es el evento que puede afectar adversamente la operación de la CPMP y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

4.7 Banco de datos personales: Conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

4.8 Centro Nacional de Seguridad Digital (CNSD): El CNSD gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital en el país, a fin de fortalecer la confianza digital. El CNSD es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

4.9 Ciberseguridad: Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su confidencialidad, integridad o disponibilidad en el ciberespacio, el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

4.10 Clasificación de la información: La clasificación de la información de realiza de acuerdo con lo establecido en el Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública.

4.11 Código fuente: El código fuente es el conjunto de instrucciones escritas en un lenguaje de programación que los desarrolladores crean para que un programa informático funcione.

4.12 Confidencialidad de la información: La información sólo es disponible para la entidad o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria.

4.13 Controles de seguridad de la información: En seguridad de la información, los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos: salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control.

4.14 Custodio del activo de información: Es el encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copia de seguridad, asignación de privilegios de acceso, modificación y borrado.

4.15 Datos personales: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.

4.16 Datos sensibles: Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.

4.17 Disponibilidad de la información: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

4.18 Dispositivo móvil: Es una computadora lo suficientemente pequeña como para sostenerla y operarla en la mano, o que puede ser transportada fácilmente. Se caracteriza por su portabilidad y su capacidad de conectividad inalámbrica (Wi-Fi, Bluetooth, redes móviles, etc.).

4.19 Enmascaramiento de datos: Es el proceso de ocultar datos personales modificando sus letras y números originales con la finalidad de proteger su confidencialidad.

4.20 Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

4.21 Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

4.22 Identidad: Es la colección de atributos que definen de forma exclusiva a una entidad.

4.23 Incidente de seguridad: Uno o varios eventos no deseados o inesperados que comprometan la confidencialidad, integridad o disponibilidad de la información o los sistemas tecnológicos de la organización.

4.24 Información: Son los datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.

4.25 Información confidencial: Son excepciones al ejercicio de derecho de información, incluye datos personales, información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil.

4.26 Integridad de la información: Es asegurar el no repudio de la información y su autenticidad, y evitar su modificación o destrucción indebida.

4.27 IP - Internet Protocol o Protocolo de Internet. - La IP es una dirección única que identifica a un dispositivo en Internet o en una red local.

4.28 Líder de Gobierno y Transformación Digital: Persona responsable de coordinar las políticas, objetivos, planes y acciones para desplegar la transformación digital y el desarrollo del Gobierno Digital en la entidad. El Líder de Gobierno y Transformación digital recae en el Gerente de Informática de la CPMP. En la conformación del Comité de Gobierno y Transformación Digital, el Líder de Gobierno y Transformación Digital actúa como Secretario Técnico de dicho Comité.

4.29 Logueo: Acción de ingresar a un sistema de información o servicio informático.

4.30 Medios removibles de almacenamiento: Se refiere a un tipo de soporte de almacenamiento de datos que está diseñado para ser fácilmente insertado y retirado de un dispositivo (como una computadora, una cámara, un reproductor de música, etc.) sin la necesidad de apagar el equipo. Su principal característica es la portabilidad, permitiendo transportar información de un lugar a otro o entre diferentes dispositivos.

4.31 Mejora continua: Es la actividad recurrente para mejorar el desempeño de los procesos.

4.32 PIN: De las siglas en inglés, Personal Identification Number, es un número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema.

4.33 Propietario del activo de información o sistemas de información: Individuo o entidad de forma responsable, que cuenta con la aprobación de la entidad, para el control de la producción, desarrollo, mantenimiento, utilización y seguridad de los activos. El término propietario no significa que la persona disponga de los derechos de propiedad reales del activo.

4.34 Propietario del riesgo: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo, dentro del alcance de sus competencias.

4.35 Proveedor: Persona natural o jurídica que brinda un servicio o producto a la CPMP. En el marco de la norma de contrataciones recibe la denominación de contratista.

4.36 Proyecto: Proceso único, que consiste en un conjunto de actividades coordinadas y controladas con fechas de inicio y finalización, llevadas a cabo para lograr un objetivo conforme con requisitos y requerimientos específicos, incluyendo las limitaciones de tiempo, coste y recursos.

4.37 Riesgo de seguridad de la información y ciberseguridad: Se refiere a la posibilidad de que una amenaza explote una vulnerabilidad en los activos de información, sistemas tecnológicos, procesos o personas de la organización, generando un impacto negativo sobre la confidencialidad, integridad y disponibilidad de la información.

4.38 Seguridad de la información: Característica de la información que se logra mediante una adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas especializadas, a efectos que dicha información cumpla con los criterios de confidencialidad, integridad y disponibilidad.

4.39 Seguridad digital: Es la confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas y sistemas de información.

4.40 Siglas:

Abreviatura	Descripción
ANPD	Autoridad Nacional de Protección de Datos Personales
ODP	Oficial de Datos Personales
OSCD	Oficial de Seguridad y Confianza Digital
CNSD	Centro Nacional de Seguridad Digital
CSIRT	Del término inglés *Computer Security Incident Response Team*, cuya correspondencia equivale a Equipo de respuestas ante incidentes de seguridad digital
GAF	Gerencia de Administración y Finanzas
DRO	Departamento de Riesgos Operacionales
SGL	Subgerencia de Logística
DISI	Departamento de Infraestructura y Seguridad Informática
DGP	Departamento de Gestión de Personas
DDMSI	Departamento de Desarrollo y Mantenimiento de Sistemas de Información
CPMP	Caja de Pensiones Militar Policial
PCM	Presidencia del Consejo de Ministros
UO / UUOO	Unidad Orgánica / Unidades Orgánicas
UPS	Del término inglés *Uninterruptible Power Supply*, Sistema de Alimentación Ininterrumpida.
SGSI-C	Sistema de Gestión de Seguridad de la Información y Ciberseguridad
TI	Tecnologías de Información

4.41 Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C): Es un marco estratégico que permite a una organización gestionar, proteger y mejorar de manera continua la seguridad de su información y activos

tecnológicos frente a riesgos y amenazas. Este sistema integra políticas, procesos, roles, tecnologías y controles diseñados para garantizar que los objetivos de seguridad de la información se cumplan de manera eficaz.

4.42 Teletrabajo: Modalidad especial de prestación de labores, de condición regular o habitual. Se caracteriza por el desempeño subordinado de aquellas labores sin presencia física del trabajador o servidor civil en el centro de trabajo, con la que mantiene vínculo laboral.

4.43 Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

4.44 Transformación digital: La transformación digital es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

4.45 Tercero: Toda persona que no cuentan con vínculo laboral con la CPMP, pero requiere hacer uso de sus activos de información ya sea para la prestación de un servicio (proveedores), en calidad de visitante o administrado (empresa operadora o usuario de servicio de telecomunicaciones).

4.46 Unidades Orgánicas: Están compuestas por los gerentes, subgerentes, jefes, custodio del activo de información, propietario del activo de información, usuarios o dueños de proceso.

4.47 Vulnerabilidad: Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de información, y a otros de los que forma parte o con los que interactúa.

5. PRINCIPIOS

La Política de Seguridad de la Información de la CPMP se sustenta en los siguientes principios:

5.1 Principio de confidencialidad: Garantizar que la información sea accesible solo para aquellas personas autorizadas a tener acceso a la misma.

Principio de colaboración y cooperación: Se promueve el intercambio y transferencia de información, mejores prácticas, recursos y experiencias a nivel nacional e internacional, a fin de identificar, prevenir y mitigar riesgos en el entorno digital que afecten la continuidad de funciones u operaciones de las entidades públicas, organizaciones del sector privado, el bienestar de las

personas y el desarrollo sostenible del país.

5.3 Principio de gestión de riesgos: La gestión de riesgos se sustenta en la aplicación de estándares y mejores prácticas que permitan reducir los incidentes de seguridad. El diseño, implementación y mejora de las medidas y controles de seguridad digital se basan en la evaluación de riesgos.

5.4 Principio de privacidad y seguridad desde el diseño: Se promueve la adopción de medidas preventivas de tipo tecnológico, organizacional, legal, humano y procedimental en todas las etapas del ciclo de vida de los servicios digitales, que preserven la disponibilidad, integridad, y confidencialidad de los datos personales e información y, cuando corresponda, la autenticidad de los datos y no repudio de la información proporcionada.

5.5 Principio de Recuperación y resiliencia digital: Implica la capacidad por la que se adoptan medidas a fin de anticipar, responder, recuperarse y aprender ante incidentes de seguridad digital.

5.6 Principio de respeto de los derechos humanos: El diseño, implementación y mantenimiento de medidas y controles de seguridad digital en la prestación de servicios digitales, deben respetar los derechos humanos, garantizando que no existan efectos adversos a derechos como la vida, la libre expresión, la autodeterminación de la persona, la igualdad de trato, la protección de los datos personales y la no discriminación, entre otros, establecidos en los instrumentos internacionales sobre derechos humanos.

5.7 Principio de responsabilidad: Implica el compromiso a rendir cuenta sobre las medidas y controles para gestionar los riesgos de la seguridad digital en base a sus capacidades y contexto.

5.8 Principio de transparencia: Se promueve que la provisión de datos o información a través del uso de tecnologías digitales en entornos digitales, independientemente de donde se encuentren almacenados, sea efectiva, clara, visible, confiable, comprensible, coherente para el ciudadano y personas en general; para lo cual se busca que toda información o datos que se gestionan en sistemas o plataformas digitales sean fidedignos, completos, íntegros, coherentes, consistentes y precisos, de conformidad con las normas legales vigentes.

5.9 Principio de integridad: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento. En la interacción en el entorno digital o cualquier proceso de diseño, producción, despliegue y operación de plataformas, servicios digitales o uso de la tecnología digital, las personas deben tener una conducta proba, imparcial, honesta y ética en el uso de las tecnologías digitales, contribuyendo al fortalecimiento de la confianza digital, de conformidad con las disposiciones normativas vigentes.

5.10 Principio de disponibilidad: Garantizar que los usuarios autorizados tengan accesos a la información y a los recursos necesarios con la misma, toda vez que lo requieran.

5.11 Principio de no repudio: Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

5.12 Principio de auditabilidad: Asegurar que los eventos de un sistema deben poder ser registrados para su control posterior.

5.13 Principio de legalidad: Garantizar el cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la institución.

5.14 Principio de calidad: Salvaguardar la veracidad, exactitud y actualización de la información que administra.

5.15 Principio de seguridad: Adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos y la información.

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La CPMP como entidad pública administradora de fondos de pensiones del personal militar y policial considera a la información como un activo valioso para el cumplimiento de sus funciones y alcance de sus objetivos estratégicos, por esta razón, gestiona la seguridad de la información física y digital bajo su responsabilidad y se compromete a:

6.1 Preservar la confidencialidad, integridad y disponibilidad de la información y sus procesos de acuerdo con el marco normativo y regulatorio vigente.

Preservar la confidencialidad, integridad y disponibilidad de la información y sus procesos de acuerdo con el marco normativo y regulatorio vigente.

6.3 Fortalecer la cultura de seguridad de la información a través de programas de concienciación y capacitación.

6.4 Promover la gestión eficaz de sus riesgos, eventos e incidentes de seguridad de la información, con la finalidad de garantizar la disponibilidad de los servicios y recursos informáticos.

6.5 Apoyar los objetivos y disposiciones de seguridad de la información designando los recursos necesarios para la ejecución de sus planes, así como el establecimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

7. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

7.1 Fortalecer la cultura de seguridad de la información y ciberseguridad en los funcionarios y colaboradores de la CPMP.

7.2 Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información y ciberseguridad.

7.3 Implementar controles para asegurar la confidencialidad, integridad y disponibilidad de la información de la CPMP, así como la continuidad de los servicios.

7.4 Asegurar el cumplimiento de requerimientos legales y regulatorios en materia de seguridad y confianza digital

7.5 Establecer, implementar operar, evaluar y mejorar el Sistema de Gestión de Seguridad de la Información y Ciberseguridad de la CPMP.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

En el contexto de la implementación del SGSI de la CPMP, siguiendo los requisitos y controles de la NTP ISO/IEC 27001:2022 "Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos", 3ª Edición, se definen las Políticas Específicas de Seguridad de la Información en este documento. En este sentido, la CPMP manifiesta su compromiso, a través del OSCD, de llevar a cabo lo siguiente:

a) Difundir periódicamente las Políticas Específicas de Seguridad de la Información de la CPMP entre los colaboradores.

b) Evaluar el cumplimiento de la implementación de los controles de seguridad de la información, como resultado de la aplicación de las Políticas Específicas de Seguridad de la Información.

c) Revisar y actualizar, de ser necesario, las Políticas Específicas de Seguridad de la Información de la CPMP en un plazo de un año, contado a partir de la aprobación y publicación de este documento o antes, en caso de producirse cambios significativos que afecten la seguridad de la información.

Las siguientes políticas específicas se encuentran agrupadas en cuatro secciones de acuerdo con la categorización de controles de seguridad proporcionada en la NTP ISO /IEC 27002:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información”, 3ª Edición.

8.1 Controles organizacionales

8.1.1 Roles y responsabilidades en seguridad de la información

Se han establecido los siguientes roles para efectuar la implementación, mantenimiento del SGSI y la operación de los controles de seguridad de la información.

- Consejo Directivo
- Comité de Riesgos
- Gerencia General
- Comité del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C)
- Oficial de Seguridad y Confianza Digital (OSCD)
- Gerente de Riesgos y Desarrollo
- Jefe de Departamento de Riesgos Operacionales
- Jefe de Departamento de Planeamiento y Organización
- Comité de Gobierno y Transformación Digital (CGTD)
- Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT)
- Gerente de Informática
- Gerente de Administración y Finanzas
- Jefe de Departamento de Presupuesto
- Oficial de Gobierno de Datos
- Oficial de Datos Personales
- Propietario de la Información
- Custodios de la Información

Las responsabilidades de cada rol se encuentran en el numeral 9, así mismo, las actividades específicas de cada rol se encontrarán en los documentos normativos que designan el rol, directivas y procedimientos.

8.1.2 Segregación de funciones

Los propietarios de los procesos deben evaluar las actividades y responsabilidades de cada rol de los colaboradores para asegurar que se encuentran separadas las funciones conflictivas entre diferentes individuos para reducir el riesgo de modificación no autorizada, error, evasión de controles o mal uso de los activos de información de la CPMP.

8.1.3 Responsabilidades de la dirección

La Alta Dirección de la CPMP demuestra su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C). Así mismo, establece los mecanismos para respaldar la difusión y actualización, tanto de la presente política como de los demás componentes del SGSI-C.

8.1.4 Contacto con autoridades

El CSIRT y el OSCD son los encargados de la gestión de la "Lista de contactos con autoridades". Esta lista debe ser actualizada de manera periódica con el fin de reportar oportunamente los eventos e incidentes de seguridad de la información.

8.1.5 Contacto con grupos especiales de interés

El OSCD en coordinación con el DISI, el CSIRT, y los propietarios de los procesos, en caso corresponda es responsable de crear y mantener actualizada una "Lista de contactos con grupos especiales de interés" en los que participan a fin de realizar consultas o recibir alertas tempranas sobre vulnerabilidades relacionadas a seguridad de la información.

8.1.6 Inteligencia de amenazas

El CSIRT de la CPMP recopila información de las amenazas provenientes de los eventos de seguridad sobre los activos críticos de la entidad, reportes externos de amenazas y/o comunicaciones del CNSD. El DISI analiza la información recopilada y ejecuta actividades para prevenir que las amenazas reportadas puedan afectar la seguridad de la información de la CPMP.

El OSCD utiliza la información de amenazas reportadas para mejorar y ajustar el proceso de gestión de riesgos de seguridad de la información, incluyendo la identificación y mitigación de riesgos emergentes.

8.1.7 Seguridad de la información en la gestión de proyectos

Las UUOO que tenga bajo su responsabilidad la ejecución de un proyecto, independientemente de su naturaleza (informático o no), deben incluir en la gestión de proyectos la identificación de los requisitos y riesgos de seguridad de la información para que sean tratados.

Los responsables de los proyectos deben comunicar al OSCD sobre el alcance del proyecto de forma que se cuente con su acompañamiento y en conjunto se definan los requisitos necesarios para preservar la seguridad de la información de los activos de información involucrados.

8.1.8 Inventario de información y otros activos asociados

Los responsables de las UUOO, que son propietarios de activos de información, deben mantener el inventario de sus activos de información actualizado de acuerdo con la directiva "Normas y Procedimientos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad".

8.1.9 Uso aceptable de la información y activos asociados

a) Todo colaborador y/o tercero debe proteger la información y otros activos asociados asegurándose de evitar la exposición, alteración, eliminación y/o transferencia no autorizada de la información.

b) Los colaboradores que tengan asignado información y/o activos de TI deben hacer uso de estos en estricto cumplimiento a sus funciones y/o actividades asignadas.

c) Los colaboradores cuentan con carpetas compartidas en red donde deben almacenar sólo información institucional evitando la duplicidad de datos por ser un uso incorrecto del almacenamiento.

d) Los colaboradores deben proteger los activos de TI y la información albergada o procesada en estos, contra el acceso (físico y lógico) no autorizado, robo, daño, saturación de recursos, consumo excesivo del ancho de banda, exposición de datos personales, u otras situaciones que puedan exponer su confidencialidad, integridad o disponibilidad.

e) El DISI es responsable de implementar mecanismos técnicos para brindar seguridad a los activos de TI por ello norma su uso a través de la directiva “Normas y Procedimientos para la Administración de Hardware, Software y Servicios Informáticos”.

f) Los activos de TI son parte de patrimonio de la CPMP, por tanto, el DISI en coordinación con la SGL realizan el proceso de asignación formal.

g) El servicio de correo electrónico se encuentra disponible para los colaboradores como herramienta de apoyo para el cumplimiento de sus funciones y realización de actividades.

h) El DISI es responsable de brindar el servicio de correo a través de mecanismos seguros y confiables para lo cual implementa controles y filtros que pueden implicar la restricción parcial o total de cuentas de correo que remiten información potencialmente peligrosa. Así mismo, a través de la directiva “Normas y Procedimientos para la Administración de Hardware, Software y Servicios Informáticos”, entre otras normas, establece las pautas para su adecuada gestión.

i) El software cliente de correo electrónico autorizado es el Gmail de Google Workspace. El acceso a cuentas de correo personal debe ser restringido.

j) Los colaboradores no deben divulgar o publicar información confidencial en sitios web o en servicios de almacenamiento en la nube (Dropbox, Google Drive, etc.) o aplicaciones de mensajería instantánea gratuita (Whatsapp, Telegram u otros). El canal oficial para la comunicación de la información (no considerando información confidencial) es el aplicativo Chat del Google Suite de la CPMP.

k) Los colaboradores no deben enviar información confidencial de la CPMP por correo electrónico hacia cuentas de terceros y/o gratuitos. Está prohibido el envío de publicidad, correos masivos, suplantación de identidad, correos cadenas, virus, código malicioso, contenido inapropiado u ofensivo, entre otros) y/o que ponga en peligro la información almacenada o transmitida por el servicio de correo, así como su infraestructura, está prohibida y será considerada como un ataque.

l) Los colaboradores que remitan información a cuentas grupales o listas de correo deben asegurarse de que los destinatarios tienen necesidad de conocer la información a remitir, entendiéndose que esta información es estrictamente laboral.

m) Los colaboradores no deben remitir información de su entorno privado a través de cuentas de correo electrónico de la CPMP, tampoco deben usar su cuenta de correo institucional para suscribirse a boletines, revistas, programas u otros medios de notificaciones de carácter personal.

n) Los colaboradores y/o UUOO que requieran enviar comunicaciones a todo el personal de la CPMP deberán coordinarlo con el DISI.

o) Los colaboradores deben hacer uso de firmas (resumen de datos) estandarizadas que lo identifiquen en el intercambio de correos electrónicos. La estructura de la firma seguirá lo normado por la administración.

p) Los colaboradores son responsables controlar el espacio de almacenamiento en su correo de forma que garantice su disponibilidad contando con opciones de eliminación, copia a carpetas del equipo local, entre otras.

8.1.10 Devolución de activos

El personal, al término de su relación laboral con la CPMP, debe:

a) Poner a disposición de su jefe inmediato (o a quien este designe formalmente), todos los documentos físicos o en formato digital

que le fueron entregados o hayan sido generados, como parte del cumplimiento de sus actividades.

b) En el caso de los equipos informáticos como computadoras, laptop, teléfonos celulares, entre otros que utilizaba para el desempeño de sus funciones, deberá ser gestionado con la Subgerencia de Logística de acuerdo con el procedimiento establecido para tal fin.

c) Otros activos relacionados con el tratamiento de la información que le fueron entregados, de acuerdo con las disposiciones establecidas.

También corresponde a los jefes de cada UO tomar las acciones necesarias para asegurar la transferencia del conocimiento del personal que ya no labora.

8.1.11 Clasificación de la información

Los propietarios de activos de la información (dueños del proceso) son los responsables de:

a) Clasificar su información de acuerdo con lo establecido en la Ley de Transparencia y Acceso a la Información Pública: confidencial y/o pública.

b) Clasificar toda información producida, transferida o recibida o bajo su control dentro del ámbito de sus responsabilidades, ya sea lógica (información que se genera y que se encuentra almacenada en Internet o medio electrónico como disco duro, USB, CD, DVD, entre otros) o física (información contenida en papel).

El DRO debe definir los mecanismos de clasificación de la información e informar el inventario de activos de información a los dueños del proceso.

El OSCD debe verificar los controles, supervisar su correcta implementación y recomendar mejoras de los controles requeridos en concordancia con su clasificación.

Los responsables de las UUOO deben asegurar que la información sea tratada y protegida a nivel físico y lógico en concordancia con su clasificación.

Para Información clasificada como Confidencial:

a) Se debe ubicar en un ambiente que cuente con acceso restringido, registrándose los accesos a estos ambientes.

b) Su almacenamiento debe ser mínimamente bajo llave (o algún otro mecanismo de seguridad similar) y ser cifrado (con la última versión tecnológica compatible con los sistemas institucionales), según corresponda.

c) Se debe controlar las copias físicas o electrónicas registrándose, como mínimo, la fecha de la copia y de la persona que lo recibe.

d) Su comunicación digital se debe dar por canales seguros de transmisión, cifrados con la última tecnología vigente y a direcciones de correos electrónicos institucionales autorizados por el propietario del activo de información.

Para la difusión o divulgación de la información clasificada como "Confidencial" se requiere el consentimiento previo, informado, expreso e inequívoco del Propietario del activo de información.

8.1.12 Etiquetado de la información

Los propietarios de activos de la información son los responsables de etiquetar la información ya sea almacenada en papel o medio electrónico.

Los responsables de las UUOO deben:

a) Asegurar que la información sea etiquetada en concordancia con su clasificación.

b) Para el etiquetado se puede utilizar sellos, etiquetas físicas, encabezados y pies de página, metadatos, marca de agua, entre otros.

c) Toda información física o digital que es considerada como confidencial, debe ser etiquetada (marcada), siempre y cuando los activos sean de propiedad del CPMP.

d) La información, documentos o activos que no tienen la clasificación de confidencial o reservado o secreto, no amerita etiquetado.

e) Se excluye de etiquetar la salida de información de los sistemas de información.

8.1.13 Transferencia de la información

Corresponde al propietario de la información analizar, evaluar y definir el alcance de la transferencia de la información que realizarán con otras entidades para darle los controles de seguridad, al transferir

información que no sea de carácter público. Así mismo, asegurar el uso de un acuerdo o cláusula de confidencialidad y no divulgación previa a la transferencia de información que no sea de carácter público ya sea dentro del CPMP o con otra entidad externa.

El DISI debe proteger el intercambio de información por medio electrónico, en concordancia con su clasificación.

a) Las solicitudes de información por parte de organismos externos deben ser autorizadas por los propietarios de los activos de información y cuando corresponda debe ponerse en conocimiento de la Gerencia General. Los listados de los activos de información son identificados y clasificados por el DRO en conjunto con los propietarios de los activos de información.

b) Los colaboradores deben evitar tener conversaciones verbales confidenciales en lugares públicos o por medios de comunicación inseguros (mensajes de voz, contestadoras), ya que pueden ser escuchados por personas no autorizados.

c) La información confidencial contenida en documentos físicos no debe ser transferida fuera de las instalaciones de la CPMP y debe ser almacenada en lugares seguros y/o gabinetes con llave, evitando accesos no autorizados.

d) La información confidencial contenida en documentos digitales, que requiera ser transferida a entidades externas debe seguir los siguientes lineamientos bajo la supervisión del OSCD:

- Uso de medios de transmisión seguros haciendo uso de cifrado (por ejemplo: *SFTP*, *HTTPS*, entre otros).
- Mecanismos de autenticación o contraseña.
- El almacenamiento debe contar con controles de acceso lógico y mecanismos de autenticación o contraseña
- Checksum para validación de archivos enviados.
- Temporalidad de la información remitida a través de enlaces temporales.
- Identificación de receptores de la información.

e) La transferencia de información por medios informáticos desde o hacia organismos externos se deberá realizar usando mecanismos seguros (*SFTP*, *IPSEC*, etc.), bajo el control y supervisión del OSCD.

f) La publicación de documentos en el portal web institucional (.docx, .xlsx, .pdf, etc.) se realizarán previa eliminación de los metadatos que puedan contener, a cargo del DDMSI.

g) Toda publicación web que haga referencia a información autorizada de la CPMP debe utilizar los dominios y subdominios de lacaja.com.pe, no se acepta publicaciones que usen direcciones *IP* directamente.

h) La UO que cuente con autorización para realizar transferencia de información confidencial y/o datos personales deberá coordinar con el DISI que se mantienen registros (*logs* de auditoría) sobre las operaciones realizadas en los repositorios de información con un periodo de retención de noventa (90) días.

8.1.14 Control de acceso

Todo acceso otorgado a los sistemas de información, servicios informáticos debe considerar la premisa de mínimo privilegio ("Todo está prohibido a menos que esté expresamente permitido"), los principios de necesidad de saber ("sólo acceso a la información necesaria para sus actividades") y necesidad de uso ("sólo acceso a la infraestructura que requiere para sus actividades").

a) El acceso a la información, a los recursos y servicios de TI debe ser controlado con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad.

b) Los propietarios de los activos de información son los responsables de definir las reglas de acceso y restricciones que son requeridas, así como la revisión periódica de los derechos de acceso a los mismos.

c) El DISI es responsable de normar e implementar los mecanismos técnicos para controlar el acceso lógico a los recursos y servicios de TI, por tanto, no debe existir equipamiento informático y/o software que no cumpla con las condiciones de seguridad exigidos por este.

d) La GAF debe comunicar al DISI la relación de personal de los entes de supervisión / control que requieren acceso a los sistemas de información con la debida autorización para la auditoría, así también comunicar la culminación de la auditoría para las bajas correspondientes en los accesos.

e) El acceso a los activos de TI se realiza a través de una cuenta de acceso a red, la misma que es habilitada por el DISI.

8.1.15 Gestión de identidades

El DISI, debe considerar en las directivas y procedimientos referido al acceso a los sistemas de información y servicios informáticos lo siguiente:

a) Solo una identidad específica se pueda asignar a una persona.

b) En el caso se requiera asignar una identidad a más de una persona (identidades compartidas), esta debe ser justificada y autorizada por el responsable de la UO propietaria del proceso.

c) De requerirse asignar identidades a entidades no humanas, estás deben ser aprobadas por el Jefe de DISI.

d) Guardar todos los eventos relacionados al uso y gestión de identidades de usuario.

El OSCD debe supervisar identidades a entidades humanas y no humanas de manera periódica.

8.1.16 Información de autenticación

El DISI, debe asegurar que el procedimiento, los sistemas de información y servicios informáticos consideren lo siguiente:

a) Todo acceso a recursos y servicios de TI se realiza con una cuenta de usuario que es un identificador único compuesto por un usuarios y contraseña.

b) El uso de cuentas genéricas solo está permitido para el uso de servicios específicos, previa autorización de la UO responsable y en coordinación con el DISI.

c) La contraseña está clasificada como información confidencial por lo cual no se debe compartir o mantener anotaciones de esta, ya sea en papeles o archivos digitales.

d) Los colaboradores o terceros tienen prohibido usar una cuenta de usuario de otra persona o suplantar su identidad.

e) Las cuentas de usuario serán bloqueadas ante tres (3) intentos de autenticación fallida.

f) Las contraseñas deben ser robustas para mitigar riesgos de acceso no autorizado, por lo cual debe ser de una longitud mínima de

catorce (14) caracteres cumpliendo una combinación de números, símbolos, letras mayúsculas y minúsculas.

g) Las contraseñas almacenadas deben hacer uso de cifrados robustos. Si la tecnología lo permite, se debe implementar la Autenticación de doble factor (MFA).

h) Las cuentas de usuario deben permitir que los colaboradores realicen cambio de contraseña con una frecuencia máxima de cuarenta y cinco (45) días, no se podrán reutilizar contraseñas anteriores. El usuario de una nueva cuenta de acceso debe cambiar su contraseña la primera vez que inicie sesión.

i) El colaborador es responsable de que su contraseña cumpla con la fortaleza o robustez establecida en la presente política.

j) El DISI, dentro de las características técnicas de las herramientas involucradas, establecerá los mecanismos para el cumplimiento de la fortaleza o robustez de la contraseña, bloqueo de intentos de autenticación fallida, cifrado robusto, tiempo de vigencia, reutilización y cambio de contraseña por defecto.

k) El restablecimiento de contraseña por olvido debe ser solicitada al DISI que es responsable de realizar la validación de la identificación del solicitante bajo los mecanismos que establezca y asignando una contraseña temporal que cumpla con las características de fortaleza ya definidas.

l) La entrega de la primera contraseña o clave temporal deben ser brindadas en cumplimiento del procedimiento establecido por el DISI.

m) Todos los equipos y/o dispositivos conectados a la red de la CPMP (*routers*, *firewalls*, *switches*, etc.) deben contar con contraseñas u otro mecanismo superior de control de acceso. El DISI es responsable de la seguridad de la red de la CPMP por tanto norma los procedimientos adecuados para su cumplimiento.

n) Ningún equipo o dispositivo conectado a la red de la CPMP debe mantener contraseñas por defecto u omisión, incluyendo aquellas provistas por fabricantes o proveedores de equipamiento o software.

8.1.17 Derechos de acceso

El DISI es responsable, de crear, actualizar y dar de baja a las cuentas de usuario y sus accesos a los sistemas de información y servicios informáticos, previa autorización del responsable de la UO en el que labora el usuario, cualquiera que sea la modalidad de contractual (incluido proveedores y terceros); y del responsable de la UO propietaria del sistema de información y servicio informático.

Los responsables de las UUOO propietaria de un sistema de información y servicio informático, debe coordinar que el DISI mantenga un inventario actualizado de las identidades y accesos a los sistemas de información y servicios informáticos del cual son propietarios, así como se guarde el registro de la autorización de acceso de los usuarios (activación, modificación o bajas de cuentas de acceso).

El Departamento de Gestión de Personas o quien haga sus veces, debe comunicar al DISI, la relación de los colaboradores que finalizan su relación laboral, tienen una licencia mayor o igual a tres (3) meses o un desplazamiento de personal, en un plazo máximo de un (01) día hábil de acontecido el evento, a través del procedimiento establecido.

Para el caso de la baja de las cuentas de acceso a los sistemas de información que utilizaban los colaboradores y/o proveedores o terceros que laboraron o prestaron servicios o tienen una licencia mayor o igual a tres (3) meses, corresponde al responsable de la UO en el que trabajaron, solicitar la baja de las cuentas a la Unidad Orgánica propietaria del sistema de información en un plazo máximo de un (01) día hábil.

El DISI, debe atender la solicitud de inactivación de las cuentas de acceso a la red de datos y a los servicios tecnológicos de la CPMP que administra en un plazo de un (1) día hábil a partir de la comunicación.

Así mismo, las cuentas de red, sistemas y correo electrónico deben ser eliminadas hasta cinco (5) días como máximo, posterior al cese del colaborador.

También, corresponde al responsable de la UO en el que laboró el personal, remover los accesos físicos, por ejemplo: llaves de puertas o de armarios, accesos con lectores biométricos.

El responsable del sistema de información o quien este designe, debe revisar trimestralmente la gestión de las cuentas de acceso de los usuarios de los sistemas de información. En caso de que haya observaciones, puede realizarlas directamente en los sistemas usados.

El OSCD debe revisar trimestralmente, a nivel de muestra, las cuentas de acceso a los sistemas de información y servicios informáticos.

8.1.18 Seguridad de la información en las relaciones con los proveedores

a) Todo contrato de servicio especialmente relacionado a un servicio crítico deberá incluir acuerdos de confidencialidad de la información.

b) Todo proveedor o contratista se asegurará que su personal designado para formar parte o brindar el servicio conozca y cumpla la presente política.

c) Todo personal del proveedor o contratista que en prestación de su contrato esté involucrado o en contacto con información, recursos o servicios tecnológicos de la CPMP, debe protegerlos del acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o robo, cumpliendo con los lineamientos de la presente política y con toda aquella normativa que sea aplicable a estos. Asimismo, se deberá aplicar el principio de mínimo privilegio, otorgando solo el acceso necesario y asegurando la revocatoria cuando finalice la relación contractual.

d) Toda información albergada en la red corporativa, de forma estática o circulando a través de ella mediante elementos de comunicación o transmisión, es propiedad de la CPMP y debe ser tratada como confidencial por todo proveedor o contratista.

e) Todo personal del proveedor o contratista de servicio con responsabilidades en áreas de operación o administración de sistemas y redes debe:

- Asegurar que la integridad, autenticación, control de acceso, auditoría y registro se contemplan e incorporan al diseñar, implantar y operar los Sistemas de Información y Redes de Comunicaciones.

- Asegurar la confidencialidad de la información almacenada, tanto en formato electrónico como físico.

f) Todo personal del proveedor o contratista que tenga contacto o haya obtenido conocimiento de información de la CPMP debe guardar absoluta confidencialidad, esta obligación permanece vigente aún posterior a la extinción del contrato y por tiempo indefinido.

g) Toda información (física o digital) que haya sido puesta a disposición del personal del proveedor o contratista es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

h) Todo personal del proveedor debe notificar inmediatamente a la CPMP cualquier evento o incidente de seguridad o violación de datos que involucre información de la CPMP a través del correo electrónico, y colaborar en la mitigación y resolución del incidente, en caso sea necesario.

i) Todo proveedor o contratista que tenga acceso a las instalaciones de la CPMP deberá cumplir con lo especificado en el numeral 8.3.6 "Trabajo en áreas seguras" de la presente directiva. Así mismo, deberán cumplir con otros numerales, según la naturaleza del producto o servicio que brinden a la CPMP, y que sean relevantes y esenciales para asegurar la seguridad de la información de la CPMP.

j) Se deberá efectuar auditorías periódicas para verificar el cumplimiento de los controles de seguridad.

8.1.19 Abordar la seguridad de la información dentro de los acuerdos de proveedores

a) El acceso a los activos de información por parte del personal del proveedor o contratista debe ser autorizado por el propietario del activo de información de la CPMP.

b) Las UUOO solicitantes de servicios o productos suministrados por proveedores o contratistas deben de coordinar con la SGL para que se garantice la inclusión de cláusulas de seguridad de la información en los contratos.

c) La SGL brinda a los proveedores o contratistas la documentación necesaria relacionada al SGSI-C.

Se pueden considerar como parte de los requisitos de seguridad en los términos de referencia del servicio lo siguiente:

a) La incorporación de requerimientos de seguridad de la información (organizativos, legales y técnicos) en las especificaciones técnicas y/o términos de referencia; para ello podrá solicitar el apoyo de la Gerencia de Informática y/o del OSCD de la CPMP.

b) Establecer en los acuerdos contractuales cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, cláusulas respecto a las leyes de derecho de autor o protección de datos personales; según corresponda. Dichos acuerdos contractuales deben estar vigentes hasta la finalización del contrato; según sea necesario.

c) Derecho a auditar los procesos y controles del proveedor relacionados con la seguridad de la información dentro del marco del contrato.

d) Procedimientos para la autorización y revocación de accesos y uso de información de la CPMP y otros activos asociados.

e) Procedimientos para la notificación y gestión de incidentes de seguridad de la información.

f) Cumplimiento de las políticas y normas referidas a seguridad de la información de la CPMP por parte del proveedor.

De haber algún cambio en la provisión de servicios por parte de los proveedores se debe realizar una reevaluación de los riesgos de seguridad de la información con apoyo del DRO, tomando en cuenta la criticidad de la información, sistemas y procesos involucrados.

8.1.20 Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)

El DISI, cuando requieran la contratación de bienes y servicios TIC, debe:

a) Incorporar requerimientos o requisitos de seguridad de la información en los Términos de referencia del servicio.

b) Solicitar que los proveedores de servicios de tecnología de la información y comunicaciones, que requieran subcontratar a otros proveedores, cumplan los requisitos de seguridad.

c) Validar que los productos y servicios TIC cumplan con los requisitos de seguridad establecidos, así como la funcionalidad solicitada.

d) Implementar medidas para garantizar que los componentes de los productos o servicios no son alterados o modificados sin autorización del DISI, por ejemplo: etiquetas anti-manipulación, verificaciones hash criptográficas o firmas digitales.

e) Gestionar el ciclo de vida de los componentes TIC, incluyendo riesgos de seguridad como la obsolescencia.

8.1.21 Seguimiento, revisión y gestión del cambio de los servicios de proveedores

a) La UO usuaria en calidad de supervisor de la ejecución contractual deberá asegurarse que aquellos proveedores o contratistas y/o su personal que brindan servicio dentro de las instalaciones de la CPMP y/o realizan actividades donde se involucre el manejo de información y servicios informáticos, participen en una actividad de sensibilización en seguridad de la información.

b) La UO usuaria en su calidad de supervisor de la ejecución contractual deberá revisar de forma trimestral la relación de sus proveedores o contratistas con acceso remoto y con acceso a los sistemas de información de la CPMP y validar su correspondencia ante el DISI.

c) La UO usuaria en su calidad de supervisor de la ejecución contractual será la encargada de monitorear y revisar el cumplimiento de los servicios o productos brindados por el proveedor o contratista, en coordinación con la SGL.

8.1.22 Seguridad de la información en el uso de servicios en la nube

a) Todo colaborador y tercero que requiera el uso de servicios en la nube en el ámbito del cumplimiento de sus funciones o actividades debe contar con la autorización del responsable de la UO a la que pertenece o brinda servicio.

b) El responsable de la UO que autoriza el uso de servicios en la nube lo realiza en base a los servicios en la nube autorizados por el DISI.

c) El DISI establece los requisitos para los servicios en la nube contratados por la CPMP y las responsabilidades del proveedor de servicios en la nube, garantizando que cumplan con los controles de seguridad y la normativa establecida por la Secretaria de Gobierno y Transformación Digital[1] (SGTD) u otro ente rector para el sector público.

d) Todo colaborador o tercero que cuente con autorización para gestionar el acceso a información institucional en un servicio en la nube es responsable de aplicar el principio de menor privilegio, otorgando solo los permisos necesarios a cada usuario para desempeñar sus funciones o actividades.

[1] https://www.gob.pe/institucion/pcm/informes-publicaciones/268665-lineamientos-para-el-uso-de-servicios-en-la-nube-para-entidades-de-la-administracion-publica-del-estado-peruano

e) La CPMP se reserva el derecho de realizar auditorías (con auditores internos o externos) o revisiones a sus proveedores de servicios en la nube para verificar el cumplimiento continuo y garantizar que los estándares de seguridad se mantengan alineados con las últimas regulaciones y mejores prácticas, la eficacia de los procesos de gestión de riesgos y la preparación para incidentes de segundad.

f) Los proveedores de servicio en la nube son responsables como mínimo de:

- Implementar mecanismos de autenticación como múltiple factor de autenticación (MFA) o alternativas robustas de seguridad para asegurar que solo usuarios autorizados accedan a los recursos en la nube.

- Utilizar algoritmos de cifrado fuertes como (*Advanced Encryption Standard*), o superiores, para garantizar la seguridad de los datos almacenados y transmitidos.

- Implementar técnicas de borrado seguro de información garantizando la eliminación completa y segura de los datos de la CPMP de sus sistemas en la nube al finalizar el contrato de servicio o en caso de una solicitud específica.

- Implementar políticas de respaldo y recuperación robustas considerando los lineamientos brindados por el DISI con la finalidad de garantizar la disponibilidad y la integridad de los datos y utilizando métodos de cifrado para proteger la información confidencial durante el proceso de respaldo.

- Cumplir la Política de Seguridad de la Información de la CPMP y demás documentos normativos de la institución que les aplique. La CPMP deberá solicitar al proveedor una declaración de aplicabilidad de las medidas, certificaciones o acreditaciones en materia de seguridad de la información.

- Cumplir con las medidas de seguridad aplicables para las entidades del Estado, como la NTP ISO/IEC 27001 (en su versión vigente) y las disposiciones señaladas en la Directiva de Seguridad emitida por la ANPD del Ministerio de Justicia (cuando corresponda).

8.1.23 Planificación y preparación de la gestión de incidentes de seguridad de la información

Se deben establecer los procedimientos y responsabilidades para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. Este procedimiento debe considerar:

a) El monitoreo y reporte de los eventos de seguridad de la información para decidir si son clasificados como incidentes de seguridad de la información en conjunto con el DRO.

b) Clasificar, priorizar y analizar los incidentes de seguridad de la información, determinando mínimamente su causa raíz, impacto, probabilidad de ocurrencia, la solución a la causa raíz, responsable de la atención y el periodo de implementación de la solución.

c) Seguimiento de la atención de los incidentes hasta su conclusión, incluyendo el escalamiento requerido y la comunicación a las partes interesadas.

d) Informar al OSCD todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata.

e) Informar al OSCD las debilidades y eventos de seguridad de la información que podrían comprometer la continuidad de los servicios informáticos de la CPMP.

f) Identificación y registro de las lecciones aprendidas y mejoras a los controles de seguridad de la información.

8.1.24 Evaluación y decisión sobre eventos de seguridad de la información

Los trabajadores deben reportar los eventos y/o debilidades de seguridad de la información relacionada a los servicios informáticos al DRO, de acuerdo con los procedimientos establecidos.

El DRO debe dar tratamiento a los eventos y/o debilidades de seguridad de la información reportadas, asimismo, evaluar, clasificar, priorizar el evento y determinar si es un incidente; en caso afirmativo deberá comunicar al OSCD y/o al CSIRT de acuerdo a los procedimientos establecidos.

8.1.25 Respuesta a incidentes de seguridad de la información

El DRO, debe comunicar los procedimientos establecidos para el reporte y la atención de los incidentes de seguridad de la información en forma

rápida, efectiva y ordenada. Las UUOO en el marco de su competencia, deben dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos elaborados y establecidos por el DRO.

8.1.26 Aprendizaje de los incidentes de seguridad de la información

Corresponde al DRO, en coordinación con el OSCD, considerar en el procedimiento de gestión de incidentes de seguridad de la información la cuantificación de los tipos, volúmenes y costos de los incidentes de seguridad de la información que permita:

a) Mejorar los protocolos de atención de los incidentes.

b) Identificar incidentes recurrentes o graves y sus causas para analizarlos e incluirlos en la evaluación de riesgos de seguridad de la información y así reducir la probabilidad o las consecuencias de futuros incidentes similares.

c) Mejorar los programas o planes de concienciación en seguridad de la información del usuario.

El OSCD, debe:

a) Comunicar al CSIRT los incidentes de seguridad digital que le fueron reportados.

b) Comunicar al Responsable del Tratamiento los incidentes de seguridad de la información relacionados a bancos de datos personales a fin de que, de considerarlo, pueda comunicarlo a la ANPD.

c) Revisar trimestralmente el proceso de gestión de incidentes del DRO.

El OSCD en calidad de coordinador del CSIRT, debe comunicar al CNSD los incidentes identificados a través de los medios que indique la Secretaría de Gobierno y Transformación Digital y la ANPD *(*https://reporte.cnsd.gob.pe/home/minjus*).*

8.1.27 Recolección de evidencia

El DISI deberá definir un procedimiento para la identificación, recolección y conservación de la información que puede servir como evidencia para propósitos de acción disciplinaria y legal. La evidencia corresponde a logs de auditoría de accesos a los sistemas y recursos tecnológicos de la CPMP. En general, las evidencias deben recopilarse de una manera que sea admisible.

8.1.28 Seguridad de la información durante la interrupción

En situaciones adversas, la CPMP establece los siguientes lineamientos de seguridad de la información y de continuidad para la gestión de seguridad de la información:

a) Mantener el uso de credenciales de acceso a los sistemas de información de acuerdo con los lineamientos establecidos en el numeral 8.1.16 “Información de autenticación” de la presente política.

b) Mantener activados los *logs* de auditoría, en cumplimiento de lo establecido en el numeral 8.4.15 “Registro” de la presente política.

c) El acceso a las copias de respaldo solo está permitido al DISI.

d) Mantener la configuración de copias de respaldo de archivos y bases de datos.

e) Verificar que la documentación (física o digital) con clasificación confidencialidad esté protegida durante los traslados o restauración, incluyendo copias de respaldo.

f) Mantener la misma configuración de los perfiles y usuarios de las aplicaciones en el ambiente de contingencia.

g) En caso de verse afectados equipos de usuario final y estos requieran ser reemplazados, se debe mantener la configuración base.

h) Los planes de continuidad del negocio deben reflejar los principios y directrices definidos en la directiva “Políticas y Objetivos de Continuidad del Negocio” y en la directiva “Normas y Procedimientos del Sistema de Gestión de Continuidad del Negocio (SGCN)”, tales como: Priorización de procesos críticos, Tiempos máximos aceptables de interrupción, Niveles de pérdida de datos tolerables, Cumplimiento de requisitos legales, regulatorios y contractuales.

8.1.29 Preparación para las TICs para la continuidad del negocio

a) El DISI establece un Plan de Contingencia Informático detallado en el Plan de Continuidad de Servicios Informáticos, que describe las acciones a realizar ante escenarios adversos definidos.

b) La CPMP cuenta con un CSIRT ante incidentes de seguridad digital y es responsable de la gestión de incidentes de seguridad digital que afectan los activos de información.

c) La CPMP cuenta con un Grupo de Comando que es el órgano técnico interdisciplinario responsable de la planificación, coordinación y ejecución de las acciones operativas orientadas a garantizar la continuidad operativa y la resiliencia institucional.

8.1.30 Requisitos legales, estatutarios, regulatorios y contractuales

Las UUOO de la CPMP deben:

a) Identificar todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes.

b) Implementar procedimientos para asegurar el cumplimiento de lo señalado en las normas legales, estatutarias, regulatorias o documentos contractuales relacionados con el tratamiento de la información, derechos de propiedad intelectual y uso de producto de software propietario.

Corresponde al DISI implementar los controles de seguridad criptográficos o de enmascaramiento, en cumplimiento con todos los acuerdos, legislación y regulación vigente.

El OSCD, debe verificar la implementación de los controles para recomendar mejoras. Para el caso de los controles de seguridad en los bancos de datos personales de la CPMP debe coordinar con el ODP y Responsable del Tratamiento.

8.1.31 Derechos de propiedad intelectual

a) La CPMP es titular legítima de los activos de propiedad intelectual utilizados, y su uso está restringido a fines autorizados.

b) La CPMP establecerá a través de acuerdos de confidencialidad la protección de los derechos de propiedad intelectual.

c) La CPMP reconoce como activo de propiedad intelectual al software y código fuente desarrollado internamente, patentes, diseños industriales, documentación técnica, manuales y materiales formativos, *know-how* corporativo, en tal sentido, el DISI deberá:

- Catalogar los recursos sujetos a derecho de propiedad intelectual (código fuente, patentes, marcas, secretos comerciales, etc.).

- Implementar mecanismos de autenticación y autorización para limitar el acceso a la propiedad intelectual.

d) La Gerencia de Informática es la unidad responsable de asumir las siguientes funciones vinculadas al software empleado por la CPMP:

- Mantener un registro actualizado de todas las licencias de software utilizadas en la entidad, junto con la documentación que acredite su correcta adquisición.

- Ejecutar revisiones periódicas para confirmar que únicamente se haya instalado software autorizado y debidamente licenciado.

- Gestionar la inscripción y/o registro, ante Indecopi y a nombre de la CPMP, del software desarrollado incluyendo aquel creado por terceros para la institución en el registro de propiedad intelectual correspondiente.

8.1.32 Protección de registros

Las UUOO de la CPMP deben proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, por lo tanto, deben incorporar en los lineamientos y procedimientos de operativos o de tratamiento de información, las normas a seguir para el almacenamiento, custodia y eliminación de los registros de acuerdo con el esquema de clasificación.

8.1.33 Privacidad y protección de la información de identificación personal (IIP)

En estricto cumplimiento del marco normativo de protección de datos personales, la CPMP gestiona la información bajo los principios de confidencialidad, integridad y disponibilidad. Dicho tratamiento se limita estrictamente a las finalidades declaradas en la "Política de Privacidad y Protección de Datos Personales", asegurando la máxima protección de los derechos de sus titulares.

En tal sentido, las unidades orgánicas de la CPMP deben:

a) Designar a un responsable por cada banco de datos personales, así como un responsable del tratamiento de estos.

b) Garantizar el ejercicio de los derechos ARCO de los datos personales, a través del enlace en su página web – https://www.lacaja.com.pe/arco.

c) Promover la toma de conciencia del personal responsable sobre la protección de los datos personales.

d) Cumplir con los requisitos legales, normativos y regulatorios aplicables.

e) Fomentar la mejora continua sobre las medidas adoptadas en protección de los datos personales a fin de minimizar los riesgos e incidentes de seguridad relacionados a los datos personales.

f) Establecer la necesidad de evaluaciones de impacto de privacidad (DPIA/PIA) para nuevos tratamientos de datos personales o cambios significativos en los existentes.

g) Identificar y documentar los bancos de datos personales que existan dentro de su ámbito de responsabilidad, y proceder a registrarlos ante la ANPD conforme a la normativa vigente.

h) Establecer mediante cláusulas contractuales u otros instrumentos jurídicos aplicables, la obligación de que los terceros cumplan con las disposiciones legales y regulatorias sobre el tratamiento de datos personales a los que pudieran acceder durante la prestación de sus servicios.

El DISI debe implementar los controles de seguridad de la información para la protección de los bancos de datos localizados en el Centro de Datos. El OSCD, en coordinación con el ODP y el Responsable del Tratamiento, debe verificar los controles, supervisar la correcta implementación, recomendar mejoras de los controles requeridos para la seguridad y gestión de los bancos de datos de la CPMP.

8.1.34 Revisión independiente de la seguridad de la información

El OSCD, debe:

a) Elaborar y proponer al Comité de Gobierno y Transformación Digital para su aprobación, el programa de auditoría interna o externa al menos una vez por año, de los procesos que forman parte del alcance del SGSI.

b) Coordinar la ejecución de las auditorías internas o externas por personas independientes a los procesos o UUOO a revisar.

c) Realizar revisiones de la seguridad de la información al menos una vez al año, a los controles de seguridad de la información implementadas en el DISI.

d) La revisión incluye los procesos relacionados con el procesamiento de la información, como son desarrollo de software, base de datos, redes, entre otros y debe realizarse tomando como criterios los controles del Anexo A de la NTP ISO/IEC 27001:2022 NTP Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.

e) Informar al Comité de Gobierno y Transformación Digital los resultados de las revisiones y auditorías.

El Comité de Gobierno y Transformación Digital, debe revisar los informes de los resultados de la auditoría interna, externa o de las revisiones realizadas o coordinadas por el OSCD.

8.1.35 Cumplimiento con políticas, reglas y normas de seguridad de la información

Los jefes de las UUOO de la CPMP deben asegurar que el personal y los terceros dentro de la UO que lideran, cumplen la política de la seguridad de la información. De existir incumplimientos, deben reportarlo, analizar las causas, implementar las acciones correctivas y verificar la efectividad de las acciones tomadas.
El OSCD debe:

a) Revisar las políticas, directivas y procedimientos de seguridad de la información al menos una vez al año o cuando existan cambios en las normas o procesos de la institución.

b) Revisar, a nivel de muestra, que el personal y los terceros cumplan la política de la seguridad de la información al menos una vez al año.

8.1.36 Procedimientos operativos documentados

El DISI debe elaborar procedimientos documentados como mínimo para las actividades operativas que represente un riesgo de no realizarse de manera correcta. Estos procedimientos deben:

a) Establecer las actividades y responsabilidades para la gestión y operación de los medios de procesamiento y almacenamiento de la información, por ejemplo: monitoreo de la capacidad y desempeño de los recursos informáticos, instalación y configuración de los sistemas, entre otros.

b) Asegurar la segregación de funciones en la operación para reducir el riesgo de un mal uso.

Corresponde al DISI, registrar, controlar e identificar el impacto de los cambios que se realicen en los procesos de tecnología de la información y comunicaciones y las instalaciones de procesamiento de la información que afecten la seguridad de la información.

8.2 Controles de Personal

8.2.1 Selección

El Departamento de Gestión de Personas, debe comprobar los antecedentes del personal que ingresa a laborar en la CPMP, de acuerdo con las leyes y regulaciones vigentes, independientemente de su modalidad de contratación.

8.2.2 Términos y condiciones del empleo

El Departamento de Gestión de Personas, debe:

a) Establecer en los acuerdos contractuales de empleo, cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, cumplimiento a la política de seguridad de la información y documentos normativos institucionales, cláusulas respecto a las leyes de derecho de autor o protección de datos personales; según corresponda. Dichos acuerdos contractuales deben estar vigentes hasta la finalización del contrato; según sea necesario.

b) Comunicar que el incumplimiento de la Política de Seguridad de la información podrá ser objeto de sanción administrativa disciplinaria, previo procedimiento administrativo disciplinario.

El personal debe:

a) Cumplir con lo dispuesto en las Políticas de Seguridad de la Información; así como con toda normativa relacionada con la seguridad de la información emitida por la CPMP.

b) Informar las vulnerabilidades detectadas y violaciones de seguridad de la información al OSCD de la CPMP.

8.2.3 Toma de conciencia, educación y entrenamiento sobre la seguridad de la información

a) El nuevo colaborador de la CPMP participa del proceso de inducción organizado por el Departamento de Gestión de Personas, con la participación del OSCD o quién él delegue.

b) Todos los colaboradores deben asistir a las charlas, entrenamientos o capacitaciones en Seguridad de la Información, así como cumplir con las políticas de seguridad de la información y ciberseguridad.

c) Todos los colaboradores deben atender las recomendaciones de seguridad de la información que son remitidas a través de los medios de comunicación institucionales.

8.2.4 Proceso disciplinario

a) La CPMP cuenta con un Reglamento Interno de Trabajo (RIT) que norma las relaciones y condiciones laborales de los servidores de la CPMP, durante el desempeño de sus funciones, conforme a las normas legales.

b) Todo colaborador debe aplicar el RIT, teniendo en cuenta, que, para el SGSI-C, es fundamental el cumplimiento del art. 42º del RIT referidas a la seguridad de la información.

c) El Departamento de Gestión de Personas debe difundir que el incumplimiento de la Política del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, podrá ser objeto de sanción administrativa disciplinaria, previo procedimiento administrativo disciplinario; como también los medios de presentación de la denuncia para reportar tal incumplimiento.

8.2.5 Responsabilidades después del cese o cambio de empleo

a) Todos los colaboradores antes de su desvinculación realizan la entrega de cargo incluyendo la información contenida en la cuenta de correo electrónico institucional, ello conforme a lo dispuesto en la directiva “Normas para la entrega de cargos del personal”.

b) El Departamento de Gestión de Personas debe comunicar al DISI y la GAF sobre las rotaciones, licencias mayores o iguales a tres (3) meses, y ceses que se produzcan en la CPMP, hasta con tres (3) días de anticipación, de forma que el DISI y la GAF tomen las medidas de control sobre la revocación de accesos a las instalaciones físicas, recursos y servicios informáticos. Los procedimientos relacionados se encuentran normados en la directiva “Normas y Procedimientos para la Administración de Accesos a los Servicios Informáticos”.

c) Las cuentas de usuario de colaboradores con licencia mayor o igual a tres (3) meses serán deshabilitadas salvo autorización expresa del responsable de la UO. En los casos de cese, las cuentas serán inicialmente deshabilitadas por quince (15) días, posterior a ello el

buzón del correo será eliminado de los servidores. El DISI mantiene el respaldo de la información histórica de acuerdo con la directiva "Plan de Seguridad Informática Institucional".

d) Todos los colaboradores están sujetos a cláusulas de confidencialidad, las cuales se mantienen vigentes aun cuando haya finalizado el vínculo laboral con la CPMP.

8.2.6 Acuerdos de confidencialidad o no divulgación

Corresponde a los jefes de las UUOO identificar a los colaboradores que acceden a información confidencial, reservada o secreta para supervisar la aplicación de los controles de seguridad en el tratamiento de la información a la que acceden, entre ellos, la firma de un acuerdo de confidencialidad.

8.2.7 Teletrabajo

El colaborador que preste labores de teletrabajo o requiera acceso remoto debe cumplir con la presente política, la Directiva de Gerencia General "Normas y procedimientos para la aplicación del Teletrabajo", y cualquier otra normativa interna relacionada a seguridad de la información, protección de datos personales y confidencialidad de la información.

El colaborador que cuente con acceso remoto ya sea por teletrabajo o porque ha sido autorizado para su uso, debe proteger la información a la que tiene acceso de amenazas como el acceso no autorizado, alteración indebida o software malicioso cumpliendo con lo siguiente:

a) Asegurarse que en el sitio donde realizarán el teletrabajo sea un ambiente en donde se reduzca la probabilidad de accesos no autorizados a información o recursos.

b) Utilizar redes privadas para el acceso a internet.

c) Verificar que el Sistema Operativo y el antivirus o antimalware del equipo con el que trabaja, cuente con las últimas actualizaciones.

d) Verificar que los equipos asignados cuenten con bloqueo automático por inactividad. No utilizar otra herramienta de comunicación o de videoconferencia a la establecida por la CPMP.

e) Guardar confidencialidad de la información proporcionada por la CPMP para la prestación de las labores.

El DISI es el responsable de habilitar el acceso remoto a la red de datos de la CPMP a través de un software VPN previa autorización del responsable de la UO y del Jefe de Departamento de Gestión de Personas. También debe implementar las medidas necesarias para:

a) Capacitar y concientizar a los usuarios sobre las medidas de seguridad y confianza digital que deben tener para la protección de la información a la que acceden, como la protección de sus credenciales de acceso a los recursos de información y los cuidados en los equipos de cómputo asignados.

b) Verificar que los equipos de teletrabajo tengan instalado el software VPN, el software antivirus o antimalware, el firewall activado y el sistema operativo actualizado.

Se encuentra prohibido cualquier otro mecanismo técnico de acceso remoto no autorizado que permita el acceso desde redes externas a la red de la CPMP o viceversa.

8.2.8 Reporte de eventos de seguridad de la información

a) Todos los colaboradores tienen la responsabilidad de reportar incidentes, eventos y/o debilidades de seguridad de la información que se identifican o se genere duda al respecto.

b) Los colaboradores que reciban un correo electrónico con contenido malicioso, fraudulento o donde se alerte situaciones que comprometan la seguridad de la información deberá remitir el mensaje a través de un correo electrónico al DISI con la finalidad de que se brinde el tratamiento adecuado, así como evitar su difusión o reenvío a otros destinatarios.

8.3 Controles físicos

8.3.1 Perímetros de seguridad física

El Departamento de Servicios Inmobiliarios debe supervisar que el servicio de vigilancia privada brinde la seguridad de forma permanente, al interior y en el sector perimétrico de las sedes de la CPMP a fin de prevenir actos ilícitos o incidentes que puedan generar riesgos contra la integridad de los colaboradores, usuarios y patrimonio de la CPMP.

8.3.2 Ingreso Físico

a) Toda persona que ingrese a las instalaciones de la CPMP debe identificarse y ser registrado tanto en el ingreso como en la salida. Los colaboradores y los terceros deben usar en todo momento su

fotocheck o el identificador que se les haya sido asignado, portándolo en un lugar visible.

b) El DISI es el responsable de normar e implementar los mecanismos técnicos para asegurar el control del acceso físico a las instalaciones y a través de su Especialista en Seguridad de Información, o quien haga sus veces, establece los procedimientos necesarios para cumplir con tal fin.

c) El personal de seguridad debe asegurarse que se registre los dispositivos del tipo *tablet* o *laptop* y los dispositivos de almacenamiento externo como discos duros portátiles que ingresen o salgan de las instalaciones de la CPMP.

d) El acceso al Centro de Datos está permitido sólo al personal técnico autorizado del DISI. El ingreso y salida es previa identificación biométrica.

e) Los terceros que requieran ingresar al Centro de Datos deben contar con autorización del responsable del Centro de Datos.

8.3.3 Asegurar oficinas, salas e instalaciones

El Departamento de Servicios Inmobiliarios debe dar cumplimiento a la Directiva de Normas Internas y Procedimientos de Seguridad de la CPMP vigente con la finalidad de garantizar la seguridad de los colaboradores, usuarios y los bienes patrimoniales de la CPMP. El personal de la CPMP, proveedores y el personal de terceros autorizados, deben portar siempre su identificación (fotocheck o pase especial) en un lugar visible al permanecer en las instalaciones de la CPMP, incluyendo en el Centro de Datos. Corresponde a los responsables de las UUOO verificar que las personas dentro de las instalaciones bajo su responsabilidad cumplan con portar su identificación.

8.3.4 Supervisión de la seguridad física

El Departamento de Servicios Inmobiliarios es responsable del monitoreo de la seguridad física de las instalaciones de la CPMP. Para este fin, cuenta con personal de vigilancia, sistemas de videovigilancia, panel de control de alarmas, entre otros.

Las directrices de monitorización de seguridad física se establecen en la Directiva Nº 01-2020-JUS/DGTAIPD - Tratamiento de Datos Personales mediante sistemas de videovigilancia.

8.3.5 Protección contra amenazas físicas y ambientales

Las instalaciones de la CPMP cuentan con extintores operativos y cargados, sistema de alarma contra incendios y rutas de salida y zonas seguras señalizadas.

El Departamento de Servicios Inmobiliarios, así como las UUOO responsables de las instalaciones de procesamiento y/o almacenamiento de información, deben tomar las acciones para:

a) Realizar evaluaciones de riesgo a las instalaciones de procesamiento y/o almacenamiento de información que permita identificar las amenazas físicas y ambientales a las que están expuestas, por ejemplo, incendio, inundación, disturbios civiles, entre otras, según lo establecido en el Plan de Continuidad Operativa de la CPMP.

b) Implementar los controles adecuados para el tratamiento de los riesgos identificados e informar al DRO para la actualización del Plan de Continuidad Operativa o situaciones no contempladas en el mismo.

c) Realizar pruebas periódicas y/o revisiones a los controles ambientales implementados como sensores de humedad, detectores de humo, entre otros.

8.3.6 Trabajo en áreas seguras

a) Las oficinas o instalaciones donde se almacene o procese información confidencial (Centro de Datos, Archivo, entre otras) son instalaciones críticas por lo cual deben contar con acceso restringido y deben ser monitoreadas con cámaras de videovigilancia. El ingreso y salida de los colaboradores autorizados debe ser registrado por las UUOO responsables de dichos ambientes y, de ser el caso, emplear mecanismos biométricos.

b) Todo tercero que ingrese al Centro de Datos debe estar acompañado por un personal técnico autorizado del DISI quién supervisará los trabajos o actividades a realizar.

c) Todo equipamiento que sea instalado debe ser inspeccionado antes de la entrega a fin de determinar si su contenido representa un peligro para la seguridad del Centro de Datos, de igual manera, esta tarea será supervisada por un personal técnico autorizado del DISI.

d) No se encuentra permitido tomar fotografías o filmar dentro de los ambientes donde se almacene o procese información confidencial,

como los archivos de las UUOO, el Archivo Central y el Centro de Datos.

e) Las oficinas o instalaciones que contengan equipos de comunicaciones (*switches*, *PBX*, *routers*, *firewalls*) y consolas de administración, deben contar con acceso restringido y monitoreado con cámaras de videovigilancia.

8.3.7 Escritorio y pantalla limpios

a) Los colaboradores deben bloquear su equipo de cómputo cuando se ausenten de su puesto de trabajo, así como guardar en un sitio seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial. Si los colaboradores están ubicados cerca de zonas de atención al público, deben guardar también los documentos y medios que contengan información de uso interno.

b) AI finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.

c) Los colaboradores que usen las impresoras deberán retirar los documentos inmediatamente después de su impresión.

d) El colaborador debe mantener su escritorio virtual con la menor cantidad de archivos o accesos directos debido a que estos generan degradación del performance de los equipos de usuario.

8.3.8 Ubicación y protección de los equipos

El DISI, debe implementar controles que permitan:

a) Evitar la apertura de los equipos informáticos. Solo el personal de soporte técnico del DISI podría hacerlo en caso corresponda.

b) La apertura de equipos debe estar controlada con etiquetas o algún tipo de hardware de seguridad.

Para el caso de los equipos ubicados en el Centro de Datos de la CPMP, corresponde al DISI monitorear las condiciones ambientales como la temperatura y humedad que puedan afectar el funcionamiento de los equipos.

8.3.9 Seguridad de los activos fuera de las instalaciones

a) Los colaboradores que requieran retirar activos de TI de las instalaciones de la CPMP deberán solicitarlo a la SGL (Control Patrimonial), según los formatos establecidos y contar con la autorización previa del responsable de la UO correspondiente.

b) El colaborador que haya sido autorizado para retirar los activos de TI debe hacer sellar el formato patrimonial por personal de vigilancia cada vez que se retire y/o ingrese.

c) El personal de vigilancia debe verificar el activo de TI antes de su retiro y/o ingreso a las instalaciones de la CPMP.

d) La SGL coordinará con el DISI para garantizar que los equipos de cómputo que serán entregados a los colaboradores en calidad de préstamo y retirados de las instalaciones de la CPMP, tengan los puertos bloqueados para el uso de medios removibles. Estos puertos sólo se habilitarán cuando exista la necesidad y se cuente con la autorización del responsable de la UO.

e) Todo colaborador que tenga asignado un equipo de cómputo para su uso fuera de las instalaciones es responsable de su resguardo, evitando dejarlo sin vigilancia y exponerlo a ambientes con condiciones extremas (temperatura, humedad, polvo).

8.3.10 Medios de almacenamiento

a) El DISI es responsable de establecer los requisitos técnicos y de seguridad para la adquisición de medios removibles.

b) Todo colaborador que, para el cumplimiento de sus funciones, requiera conectar un medio removible a un equipo de cómputo de la CPMP deberá asegurarse que sea analizado previamente por el software antimalware/antivirus.

c) El colaborador que tenga asignado un medio removible debe resguardarlo y evitar el acceso no autorizado o uso indebido.

d) El colaborador que haga uso de un medio removible debe evitar dejarlo conectado a equipos desatendidos.

e) La movilización y salida de medios removibles que contengan información confidencial, fuera de las oficinas de la CPMP se encuentra prohibida, salvo con autorización expresa del Gerente de Informática o en su defecto del DISI. Esta prohibición no incluye el

traslado de las cintas de respaldo hacia su lugar de custodia gestionado por el DISI.

f) Los medios removibles que requieran ser dados de baja, deberán pasar por un proceso de borrado seguro.

g) El DISI es responsable de implementar el procedimiento de borrado seguro y destrucción de los medios removibles (en caso corresponda), antes que se realice la baja o reutilización de este.

8.3.11 Servicios de suministro de apoyo

El Departamento de Servicios Inmobiliarios, dentro del marco de sus competencias y en coordinación con el DISI, debe:

a) Programar los mantenimientos de los equipos de respaldo de energía eléctrica (como grupo electrógeno y UPS) para asegurar el funcionamiento de los componentes del centro de datos, ante la pérdida del servicio de suministro eléctrico.

b) Asegurarse que los equipos de respaldo de energía eléctrica se inspeccionen y prueben periódicamente para garantizar su correcto funcionamiento.

El DISI debe disponer de un servicio de conexión a Internet de contingencia que permita la operatividad de los servicios informáticos de la CPMP ante la interrupción del servicio de conexión principal.

8.3.12 Seguridad del cableado

El DISI debe implementar controles que permitan asegurar que los cables que transportan datos se encuentren debidamente protegidos contra la interferencia o posibles daños.

8.3.13 Mantenimiento de equipos

El DISI debe:

a) Programar y realizar en forma periódica mantenimientos preventivos de los equipos informáticos de los colaboradores de la institución de acuerdo con las recomendaciones del fabricante.

b) Asegurar que se efectúe el mantenimiento de los equipos informáticos que conforman la infraestructura de tecnología del Centro de Datos de la CPMP como son equipos de servidores, UPS, sistema de aire acondicionado de precisión, entre otros.

8.3.14 Eliminación segura o reutilización de equipos

El DISI debe:

a) Asegurar que, la información clasificada como no pública, almacenada en los medios de almacenamiento que van a ser reutilizados, reemplazados o puestos a disposición (baja), sea borrada de manera segura; así como también en el caso que contengan software propietario.

b) De acuerdo a una evaluación de riesgos de acceso a información no pública, determinar si los medios de almacenamiento deberían destruirse físicamente.

Corresponde a la Subgerencia de Logística, retirar las etiquetas y marcas que identifican a la CPMP de los equipos o medios de almacenamiento antes de ser puestos a disposición para donación o eliminación.

Corresponde los responsables de las UUOO que, en el caso que se requiera eliminar documentos físicos que ya no se utilicen, estos deben ser destruidos, por ejemplo, triturados, para evitar que puedan ser reconstruidos. Para la eliminación de grandes volúmenes de información física, se debe utilizar proveedores certificados y aprobados de servicios de eliminación segura.

8.4 Controles Tecnológicos

8.4.1 Dispositivos terminales del usuario

a) Todo colaborador o tercero que ingrese o retire dispositivos móviles del tipo *Tablet* o *laptop* y los dispositivos de almacenamiento externo como discos duros portátiles, de las instalaciones de la CPMP, debe coordinar su registro con el personal de seguridad de la entidad.

b) Todo colaborador o tercero debe configurar mecanismos de autenticación como PIN, clave, patrón, etc. En los dispositivos móviles bajo su responsabilidad, asignados por la CPMP o de su propiedad, que almacenen o guarden información de la CPMP.

c) Los colaboradores que hagan uso de dispositivos móviles de propiedad de la CPMP podrán conectarlos a internet a través de medios autorizados como plan de datos, red cableada, modem inalámbrico o la red inalámbrica privada del colaborador, quedando prohibido el acceso a traces de redes inalámbricas públicas como parques, cafeterías, aeropuertos, etc.

d) EL colaborador que tenga asignado un dispositivo móvil de la CPMP debe evitar dejarlo en cajones sin seguro, lugares de reunión, autos o ambientes sin supervisión, manteniéndolo en lugares que ofrezcan seguridad.

e) El colaborador que tenga asignado un dispositivo móvil de la CPMP debe ser responsable de su cuidado general, debiendo reportar al DSI cualquier tipo de siniestro.

f) Se encuentra prohibido descargar, guardar o almacenar información clasificadas como confidencial en dispositivos móviles personales.

Corresponde al OSCD:

a) Dar a conocer las políticas y procedimientos de seguridad establecidos en la CPMP, así como las responsabilidades de los usuarios en seguridad de la información.

b) Concientizar a los usuarios sobre las amenazas más comunes a la seguridad de la información.

8.4.2 Derechos de acceso privilegiados

a) Las cuentas de usuarios del tipo administrador, súper administrador y/o administradores del dominio son de uso exclusivo del DISI y deben ser usados solo para labores de mantenimiento, configuración y/o soporte de la plataforma tecnológica institucional.

b) Las cuentas de administración local deberán ser desactivadas por defecto para los equipos de cómputo de usuario final.

c) Los colaboradores o terceros que gestionen bases de datos con información confidencial y/o datos personales deben contar con controles que prevengan la pérdida de confidencialidad de la información como una adecuada gestión de accesos, controles en el equipo de usuario, controles de red, entre otros.

d) El OSCD debe supervisar el cumplimiento de asignación de acceso privilegiados, así como realizar una revisión trimestral de las cuentas con privilegios administrativos en los sistemas de información.

8.4.3 Restricción de acceso a la información

El DISI debe asegurar que se implementen los controles de acceso a la información como:

a) Accesos a los sistemas de información y servicios informáticos de la CPMP mediante mecanismos de autenticación.

b) No permitir el acceso a información sensible mediante los sistemas de información o servicios a identidades de usuario desconocidas o de forma anónima.

c) Permitir la restricción de accesos a los datos o información, así como a las acciones que puede realizar sobre ellos.

d) Mecanismos para proteger la información contra cambios, copias y distribución no autorizada, como uso de credenciales fuertes, restringir accesos por periodos de tiempo, uso del cifrado para información confidencial y registro de quien accede a la información.

8.4.4 Acceso al código fuente

El DDMSI debe incluir en las directivas de desarrollo de software lo siguiente:

a) Restringir de acceso al código fuente, así como a la documentación del proyecto solo al personal y/o terceros involucrados en la construcción del sistema de información o aplicativo, previa autorización del Jefe de DDMSI.

b) Se debe almacenar el código fuente en una herramienta centralizada que permita:

- Controlar los accesos a modo de lectura o escritura y mantener registros de auditoría de todos los accesos y de todos los cambios realizados al código fuente.

- Controlar las versiones del código fuente y de sus componentes asociados como manuales técnicos y documentos del proyecto.

c) Mantener copias de seguridad del código fuente de acuerdo con la programación aprobada por el DISI.

8.4.5 Autenticación segura

El DISI debe asegurar la implementación de tecnologías o controles de autenticación a los sistemas de información que considere:

a) El uso de un mecanismo de autenticación fuerte, si la tecnología lo permite, para verificar la identidad del usuario con métodos de autenticación adicionales a la contraseña (autenticación multifactor), sobre todo para el acceso a los sistemas críticos de la CPMP o aquellos que permiten el acceso a datos personales.

b) De utilizar autenticación biométrica incluir alguna técnica de autenticación alternativa que permita la disponibilidad del acceso en caso de falla.

c) Para los sistemas críticos o que contienen información confidencial, verificar que cuenten con controles para la restricción de acceso a los sistemas de información y servicios.

d) En el inicio de sesión a los aplicativos y/o sistemas de información de la CPMP no se debe:

- Brindar mensajes que permitan identificar el dato incorrecto.

- Mostrar información confidencial o del sistema antes de la autenticación exitosa para evitar exponer información a un usuario no autorizado.
- Mostrar el texto de la contraseña sin enmascarar mientras esté siendo ingresada por el usuario.

e) Implementar medidas de seguridad para proteger los aplicativos y/o sistemas de información de intentos de inicio de sesión por fuerza bruta, como el uso de *captcha*, o aplicando el bloqueo al usuario después de tres (3) errores.

f) Almacenar la información de autenticación, tanto de los intentos exitosos como de los fallidos.

g) Transmitir las contraseñas cifradas por la red para evitar que esta sea capturada por ciberdelincuentes.

En el caso de los servicios tecnológicos se deben configurar el uso de mecanismos de autenticación fuertes y otros controles dependiendo de la herramienta y la información que contiene.

8.4.6 Gestión de capacidad

El DISI debe analizar y aplicar controles para la supervisión de la demanda de capacidad de sus recursos administrados, por ejemplo, monitorear el consumo de recursos de procesadores, memorias, servicios de almacenamiento, servicios de impresión, anchos de banda, servicio de internet, servicios externos requeridos a otras instituciones, tráfico de las redes de datos, entre otros, y realizar proyecciones de crecimiento de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.

8.4.7 Protección contra programas maliciosos (malware)

El DISI debe implementar reglas y controles que detecten el uso de software no autorizado, el acceso a sitios web maliciosos y detección de malware. Estos controles deben considerar:

a) Asegurar que los equipos informáticos cuenten con herramientas de seguridad contra códigos maliciosos y se actualicen periódicamente.

b) Realizar charlas de concientización apropiada a los usuarios y colaboradores, sobre los riesgos a los que estamos expuestos en Internet y cómo afrontar un evento u ocurrencia de infección de virus o malware.

c) Todo equipo que se encuentre operativo y que no cuente con una herramienta de protección contra software malicioso no podrá ser conectado a la red de datos de la CPMP.

d) Todo contrato de arrendamiento de equipos informáticos debe incluir el requisito de una herramienta de protección contra software malicioso. Mantener los sistemas operativos y software, con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e) La plataforma de comunicaciones debe contar con equipamiento de seguridad que otorgue la protección necesaria ante amenazas y controle el tráfico de entrada y de salida para la red de datos de la CPMP.

No está permitido por el personal de la CPMP:

a) La desinstalación y/o desactivación de software y herramientas de seguridad implementadas por el DISI.

b) Instalar y ejecutar programas ya sean propios u obtenidos a través de internet, correo u otro medio, en los equipos de la institución sin la debida autorización del DISI.

8.4.8 Gestión de vulnerabilidades técnicas

El DISI incluye dentro de los requisitos de adquisición o mantenimiento de software pruebas o análisis de vulnerabilidades.

El DRO realiza periódicamente pruebas de vulnerabilidades sobre los servicios e infraestructura tecnológica y comunicará los resultados a las UO encargadas de la remediación para que planifiquen las acciones necesarias.

El DISI como responsable de la seguridad de los recursos y servicios informáticos, realiza tareas de actualización periódica sobre el software de los servidores, equipos de cómputo, comunicaciones o seguridad perimetral.

Los colaboradores o terceros que detecten vulnerabilidades o debilidades que puedan poner en peligro la información, recursos o servicios de TI, debe comunicarlo al OSCD siguiendo las disposiciones y actividades establecidas en la directiva “Normas y Procedimientos para la Gestión de Incidentes en la Infraestructura Informática”.

Los colaboradores o terceros que detecten vulnerabilidades no deben aprovecharse de estas para acceder o difundir información no autorizada, así como producir alguna interrupción o daño en los recursos y servicios de TI.

8.4.9 Gestión de la configuración

El DISI establece controles para documentar, implementar, monitorear y revisar las configuraciones de seguridad de sus activos críticos (hardware, software, servicios y redes). Así mismo, es el encargado de revisar periódicamente y actualizar la configuración del hardware, software, servicios y redes de acuerdo con las buenas prácticas de seguridad definida por los proveedores o las organizaciones de seguridad como el CNSD de la PCM. En la revisión y actualización se debe considerar las nuevas amenazas, debilidades, así como su viabilidad y aplicabilidad de la actualización de las versiones de acuerdo a contexto de la CPMP.

Solo los administradores del hardware, software, servicios y redes del DISI, son los responsables de realizar una actualización en la configuración siguiendo el procedimiento de gestión de cambio.

8.4.10 Eliminación de información

Los responsables de cada UO, en coordinación con el DISI, deben asegurar que la eliminación de la información clasificada como confidencial se realice de manera segura guardando evidencia de la actividad y resultados de la eliminación: información del lugar, fecha, hora, personas que intervinieron, método y herramienta utilizada.

Corresponde al DISI:

a) Identificar el método de eliminación de información apropiada para cada tipo de medio de almacenamiento, por ejemplo, uso de un software de eliminación segura, desmagnetizado de unidades de disco duro o de disco de almacenamiento externo.

b) Registrar los resultados de la eliminación como evidencia

c) Asegurarse que la información confidencial almacenada en la nube se elimine de forma segura cuando no se requiera.

8.4.11 Enmascaramiento de datos

No está permitido el uso de data de producción para desarrollos, pruebas, salvo que esta sea previamente enmascarada para evitar la pérdida de confidencialidad de la información.

Los responsables de las UUOO deben proteger la información, incluyendo datos personales y sensibles, a la que acceden de acuerdo con su clasificación, considerando mecanismos de enmascaramiento, anonimización o disociación.

El DISI implementa técnicas adicionales para el enmascaramiento de datos en los sistemas de información (anular, eliminar o sustituir caracteres) con la finalidad de limitar la exposición de datos confidenciales.

8.4.12 Prevención de fuga de datos

Los responsables de las UUOO deben identificar, clasificar y registrar en el inventario de activos la información contenida en los procesos y sistemas de información del cual son propietarios.

El DISI debe implementar herramientas que permitan monitorear y/o prevenir la fuga de datos en servicios como el correo electrónico, transferencia de archivos a través servicios de almacenamiento en la nube, discos de almacenamiento externo, entre otros.

8.4.13 Copia de seguridad de la información

El respaldo de la información debe almacenarse en lugares distantes de la sede principal para evita cualquier daño en caso de desastre en las instalaciones de la CPMP.

El DISI establece los requisitos necesarios para la protección ambiental y física de las copias de respaldo.

Se realiza copias de respaldo de la información de los servicios de ambiente de producción, desarrollo y pruebas de la CPMP, los cuales incluyen bases de datos y unidades de red y se encuentran administrados por el DISI.

El DISI revisará periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

El DISI realizará pruebas periódicas (mínimo anual) de recuperación del respaldo, para asegurar que son confiables, para lo cual seleccionará una muestra de información coordinará la verificación con la correspondiente UO propietaria.

Adicionalmente, en caso un área usuaria requiera la restauración de una copia de respaldo, esta será considerada como una prueba de recuperación de respaldo.

8.4.14 Redundancia de las instalaciones de procesamiento de información

Los propietarios de los sistemas de información y procesos, en coordinación con el DISI, deben establecer los requisitos de disponibilidad de la información y servicios informáticos y sistemas de información, en el caso de la materialización de situaciones adversas.

El DISI debe:

a) Asegurar la redundancia de los principales componentes tecnológicos (servidores, base de datos y otros), que permitan la continuidad de los sistemas de información que se considere crítico para la institución.

b) Determinar la infraestructura alterna de tecnología de información, la cual debe localizarse geográficamente en un lugar diferente a la sede principal, asegurando que presente seguridad en los siguientes aspectos: calidad de suelos y del entorno, riesgo de inundación, calidad de la construcción, disponibilidad de servicios básicos, entre otros.

c) Elaborar un plan de contingencia informático que permita definir las actividades a seguir para la activación de los componentes tecnológicos redundantes, incluyendo las instalaciones de procesamiento alterno.

d) Contar con dos proveedores diferentes de los servicios críticos para la continuidad de los sistemas de información, por ejemplo, el servicio de Internet.

El DRO es el encargado de probar de manera anual y documentar los resultados del plan de contingencia informático.

8.4.15 Registro

Se deben contar con registros (*logs* de auditoría) de acceso a las bases de datos que contengan datos personales, así como registro de las acciones relevantes sobre estas.

El DISI es responsable de la custodia de los registros y de implementar sistemas de monitoreo continuo y detección de amenazas para identificar y responder rápidamente a posibles incidentes de seguridad sobre los componentes informáticos, así mismo, deberá analizar los registros para validar la integridad y disponibilidad de estos.

El OSCD es responsable de validar y/o recomendar el análisis de los registros.

8.4.16 Actividades de monitoreo

El DISI debe:

a) Identificar los recursos informáticos críticos que deben ser monitoreados, estableciendo una línea base de comportamiento del recurso, la frecuencia de monitoreo y el periodo de retención de las evidencias.

b) Se debe implementar una herramienta que permita monitorear y enviar alertas automáticas de:

- El tráfico de la red y los sistemas de información, entrante y saliente.
- El acceso a los sistemas de información, equipos de la red de datos y demás servicios críticos.
- Uso de recursos como CPU, disco duro, memoria y ancho de banda, incluyendo su rendimiento.

- Así como almacenar y revisar los registros del monitoreo para realizar proyecciones de futuros requisitos de capacidad, que aseguren el desempeño requerido por los servicios informáticos y sistemas de información.

8.4.17 Sincronización de reloj

El DISI, debe sincronizar los relojes de todos los sistemas de procesamiento de información y servicios informáticos tomando como referencia una única fuente confiable de transmisión del tiempo, basándose en protocolos estándares de sincronización reconocidos cómo el Protocolo de Tiempo de Red (PTR o NTP *Network Time Protocol*) o el Protocolo de Tiempo de Precisión (PTP).

8.4.18 Uso de programas de utilidad privilegiados

Toda instalación de programas de utilidad privilegiados en los equipos informáticos de la red de datos de la CPMP debe contar con la autorización del responsable de la UO en la que labora el usuario y del Jefe de DISI.

DISI debe:

a) Mantener un inventario actualizado de los programas privilegiados instalados en el CPMP.

b) Establecer controles de acceso en los equipos y servicios informáticos para limitar la instalación y uso de programas privilegiados solo a los usuarios autorizados.

Corresponde a los usuarios que cuenta con la autorización de uso de programas de utilidad privilegiados:

a) Utilizar los programas solo para las actividades autorizadas.

b) Mantener la confidencialidad de la información a la que puedan acceder con dichos programas privilegiados.

8.4.19 Instalación de software en sistemas operativos

Los colaboradores o terceros no deben ejecutar o instalar software en los equipos informáticos, esta actividad es exclusiva del personal técnico del DISI.

El colaborador que requiera la instalación de software adicional a lo instalado en su equipo de cómputo deberá solicitarlo a través del Sistema de Solicitud de Trabajo previa autorización del responsable de

la UO. El DISI realizará la evaluación del requerimiento y en caso de no afectar la seguridad del equipo de cómputo, la red o se encuentre en discordancia con la normatividad institucional, autorizará y ejecutará la instalación del software.

La actualización de software que no se realice automáticamente a través de las herramientas del DISI, deberán ser solicitadas como un requerimiento a través del Sistema de Solicitud de Trabajo.

El DISI es responsable de gestionar las actualizaciones de software en los equipos informáticos de forma automática y/o manual, por lo cual no se requiere la descarga de parches u otro software por parte de los colaboradores.

8.4.20 Seguridad de redes

El DISI debe:

a) Gestionar, proteger y conservar la seguridad de los datos en las redes de la CPMP.

b) Mantener actualizada la documentación técnica de la red, como los diagramas de red, el inventario de los equipos que conforman la infraestructura tecnológica y la información de su configuración.

c) Establecer controles y medidas especiales para salvaguardar la disponibilidad, confidencialidad e integrar los datos que se transfieren a través de redes públicas, incluyendo los sistemas de información, por ejemplo, implementando equipos como firewall, sistemas de detección y prevención de intrusiones, entre otros.

d) Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red.

e) Implementar sistemas de autenticación a la red que requieran más de un factor de autenticación de usuario.

f) Implementar procedimientos que permitan reducir las vulnerabilidades técnicas en las redes, como, deshabilitar los protocolos de red vulnerables y el endurecimiento (*hardening*) de red y servidores.

g) Registrar las acciones o vulnerabilidades que puedan afectar la seguridad de la información de las redes y realizar su atención.

El OSCD deberá verificar la atención a las vulnerabilidades de red identificadas y reportadas por el DRO.

8.4.21 Seguridad de servicios de red

El DISI debe:

a) Implementar procedimientos de autorización y controles de autenticación para acceder a las redes y servicios en red.

b) La conexión a la red de datos y servicios de red de la CPMP de manera remota se debe realizar a través de una Red Privada Virtual (VPN) u otro mecanismo que permita establecer una línea segura y cifrada entre la red de datos de la CPMP y el equipo de cómputo del usuario.

c) Monitorear, revisar y auditar regularmente todos los servicios de red incluyendo los provistos por terceros.

d) Analizar las vulnerabilidades y aplicar las correcciones de seguridad de manera oportuna.

e) Planificar y autorizar los cambios en los servicios de red, incluyendo los que proveen terceros, considerando los riesgos que podrían generar, en el marco de la normativa aplicable.

f) Identificar e incluir en los acuerdos de servicios de red y/o los términos de referencia (para los servicios tercerizados) los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red.

g) Verificar la implementación de los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red.

Los usuarios de la red deben:

a) Utilizar los recursos de red de manera responsable y ética, evitando acciones que puedan poner en riesgo la seguridad de las redes.

b) Reportar, a través de los procedimientos establecidos, cualquier incidente de seguridad, vulnerabilidad o sospecha de actividad maliciosa.

8.4.22 Segregación de redes

El DISI debe:

a) Segregar las redes en función de los niveles de confianza, criticidad y sensibilidad de la información, sistemas y servicios que contienen.

b) Configurar *firewalls*, *routers* y otros dispositivos para limitar el acceso entre las diferentes zonas de la red, por ejemplo, el acceso a los recursos y datos sensibles que permitan reducir el impacto potencial de un incidente de seguridad.

8.4.23 Filtrado de la web

El servicio de internet se encuentra disponible para los colaboradores como herramienta de apoyo para el cumplimiento de sus funciones y realización de actividades.

Los colaboradores son responsables de dar buen uso al servicio de internet, así como de adoptar las medidas de seguridad necesarias que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

El DISI es responsable de brindar el servicio de internet a través de mecanismos seguros para lo cual implementa controles y filtros de navegación lo cual puede implicar la restricción parcial o total de sitios web potencialmente peligrosos. De igual modo, establece las configuraciones necesarias en los navegadores web autorizados en los equipos de cómputo.

Las páginas de redes sociales, de archivos de transferencia masiva y de inteligencia artificial están restringidas y controladas para los usuarios. El uso de este tipo de recursos debe ser debidamente sustentado y aprobado por la jefatura y/o Gerencia correspondiente, así mismo, debe ser evaluado por el DRO y el OSCD.
Dentro de las instalaciones de la CPMP, no está permitido conectar los equipos informáticos de la CPMP a cualquier otro medio de conexión a internet de proveedores externos que no haya sido dispuesto por la CPMP.

La CPMP cuenta con la potestad de mantener los registros de navegación de su servicio de internet, así como de toda información entrante o saliente a través de su red, con la finalidad de monitoreo y/o revisión y sin previo aviso.

Las solicitudes de cambio en la configuración del acceso a internet son aprobadas por el DISI, y en caso sea necesario se elevará a evaluación por el Comité de Gobierno y Transformación Digital.

Está prohibido visitar sitios web con contenido inapropiado o que puedan ser fuente de archivos y programas maliciosos.

8.4.24 Uso de criptografía

El personal de la CPMP debe remitir de manera encriptada la información electrónica cuya clasificación no sea pública, en el caso de ser requerida; previa autorización de su propietario. Para ello puede solicitar el apoyo técnico del DISI.

El DISI establece los controles necesarios para protección durante la generación, almacenamiento y archivo de las claves criptográficas mediante protocolos *HTTPS*, *SFTP*, *IPSEC*, *SSH*, incluyendo los respaldos y accesos correspondientes.

El uso de certificados digitales se debe realizar cumpliendo las normas legales vigentes y las condiciones de uso establecidas por la Entidad de Certificación Digital.

El DISI debe:

a) Asegurar que los controles criptográficos cumplan con estándares nacionales e internacionales, evitando el uso de controles con algoritmos de encriptación considerados como débiles, obsoletos o inseguros.

b) Implementar métodos criptográficos que permitan la integridad y confidencialidad de la información desde su transmisión hasta su recepción, como la publicación de servicios y sistemas de información a través de un certificado digital SSL (*Secure Sockets Layer*).

c) Previa evaluación de riesgos, determinar la necesidad de encriptar la información que no sea de carácter público, incluyendo la referida a datos personales, almacenados en las bases de datos de la CPMP.

8.4.25 Ciclo de vida de desarrollo seguro

Las UUOO que requieran el desarrollo mantenimiento de sistemas de información deberán coordinarlos con el DDMSI.

El DDMSI cuenta con requisitos de seguridad de la información para el desarrollo (interno o tercerizado), la adquisición y mantenimiento de sistemas de información, los cuales forman parte de los términos de referencia o requisitos mínimos en sus proyectos, incluyendo principios de codificación.

El DDMSI es responsable de normar, solicitar e implementar los mecanismos técnicos que protejan los sistemas de información alojados en estos.

El DDMSI es responsable de gestionar las pruebas de seguridad y funcionales necesarias para los nuevos sistemas o mantenimientos.

El DDMSI establece un procedimiento para el control de cambios, el cual debe seguir principios de seguridad para los sistemas de información.

8.4.26 Requisitos de seguridad de la aplicación

El DDMSI, en coordinación con el OSCD, debe:

a) Incluir en los requisitos de los nuevos sistemas de información o en las propuestas de mejoras de los sistemas de información existente; aquellos relacionados con la seguridad de la información, desde las etapas iniciales del proyecto.

b) Proteger la información involucrada en los servicios de aplicaciones a través de redes públicas.

c) Proteger la información involucrada en las transacciones de servicios de las aplicaciones, para prevenir transmisión incompleta, ruteo incorrecto, alteración o divulgación no autorizada de mensajes, ya sea interna o externa a la CPMP.

d) Verificar que los cambios solicitados formalmente por los propietarios de la información no causen riesgos de seguridad y de ocurrir un incidente de seguridad en la implementación de un cambio, debe deshabilitarse para su posterior subsanación.

e) Determinar las pruebas de calidad y seguridad de software a aplicar de acuerdo con la criticidad del sistema y del cambio.

8.4.27 Arquitectura de sistemas seguros y principios de ingeniería

El DDMSI debe:

a) Establecer, documentar y aplicar principios de ingeniería segura en el desarrollo de los sistemas de información.

b) Diseñar la seguridad en todas las capas de la arquitectura de un sistema de información (negocios, datos, aplicaciones y tecnología).

c) En caso de uso de nueva tecnología, se deben analizar e identificar los riesgos de seguridad.

8.4.28 Codificación segura

El DDMSI, debe establecer pautas para la codificación segura. Dentro de estos deben incluir que:

a) Los desarrolladores y analistas sigan las mejores prácticas de codificación segura y estándares de seguridad reconocidos para el desarrollo y mantenimiento de software, por ejemplo, el uso de *frameworks* y librerías de seguridad reconocidas para mitigar las vulnerabilidades comunes como las difundidas por la *Open Web Application Security Project* - OWASP y su publicación de los diez riesgos de seguridad más importantes (Top 10).

b) Implementar controles de validación y sanitización de datos de entrada para prevenir ataques de inyección de código.

8.4.29 Pruebas de seguridad en desarrollo y aceptación

El DDMSI debe:

a) Validar los sistemas de información y aplicaciones durante todas las etapas del desarrollo de software.

b) Considerar pruebas unitarias, pruebas calidad funcional y no funcional (por ejemplo: validación de datos y rendimiento), pruebas de seguridad y pruebas de aceptación por el usuario.

c) En las pruebas de seguridad incluir pruebas de autenticación de usuario, restricción de acceso, codificación y configuración segura.

d) Determinar el alcance y los tipos de pruebas en la etapa de análisis en función a la importancia, la naturaleza del sistema y el impacto del cambio.

e) Implementar herramientas automatizadas para identificar vulnerabilidades.

f) Verificar la corrección de los defectos relacionados con la seguridad.

8.4.30 Desarrollo subcontratado

Los proveedores de desarrollo deben cumplir con las normas y requisitos de seguridad de la información establecidos por la CPMP, así como colaborar en la identificación y atención de riesgos de seguridad de la información durante el proceso de desarrollo.

La Gerencia de Informática debe:

a) Incluir en los términos de referencia de los sistemas desarrollados o modificados por terceras partes, que deben cumplir con lo establecido en esta política de seguridad y la normativa de la CPMP.

b) Establecer acuerdos previos con todos los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en los proyectos.

c) Implementar un proceso de supervisión, revisión y aprobación de los entregables para asegurar la calidad y seguridad de los sistemas y aplicaciones entregados.

El OSCD y el DRO, en coordinación con los propietarios del sistema y los desarrolladores, deben evaluar los riesgos asociados al desarrollo tercerizado para verificar que se cuentan con los controles de seguridad adecuados.

8.4.31 Separación de los entornos de desarrollo, prueba y producción

El DISI debe:

a) Mantener separados los ambientes de desarrollo, pruebas y producción.

b) Establecer las actividades a seguir para el despliegue del software desde el ambiente de desarrollo, prueba hasta el ambiente de producción.

c) No permitir la ejecución de pruebas en entornos de producción, salvo excepciones aprobadas por el Jefe de DISI y el propietario del sistema.

d) No utilizar en los ambientes de desarrollo y pruebas datos confidenciales o personales similares al ambiente de producción. De ser necesario se deben aplicar procedimientos de enmascaramiento o anonimización.

e) Implementar en los ambientes de desarrollo y pruebas las actualizaciones de seguridad del software utilizado y controlar el acceso solo a personal autorizado por el Jefe de DISI.

f) Proteger el acceso a la información de producción de acuerdo con su clasificación.

8.4.32 Gestión de cambios

El DISI es responsable de gestionar los cambios en la infraestructura tecnológica y/o sistemas de información, y normar los procesamientos necesarios para este fin, así como mantener información documentada sobre este proceso.

Los cambios deberán ser planificados e incluir la identificación de los posibles compromisos en seguridad de la información, los cuales, de ser el caso, serán comunicados al OSCD para su evaluación de acuerdo con las políticas y requisitos de seguridad de la información.
Los cambios de emergencia que requieren ser aplicados para resolver un incidente, deberán realizarse de forma rápida y controlada.

Los cambios realizados deben ser verificados para asegurar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información el sistema y que el propósito del cambio se cumplió satisfactoriamente.

Los cambios deben de incluir un plan de *roll-back* (volver al estado anterior), que incluyan las actividades a seguir para abortar los cambios que se ejecutaron sin éxito y/o eventos imprevistos.

8.4.33 Información de las pruebas

El DISI y el DDMSI deben:

a) Realizar las pruebas de los sistemas de información en un ambiente controlado y con los datos seleccionados para tal fin.

b) Implementar medidas de confidencialidad para proteger la información de prueba de acuerdo con su clasificación, como la encriptación de datos sensibles y la restricción de acceso solo a personal autorizado.

c) El personal que participa en la ejecución de las pruebas no debe ser el mismo que participó en su desarrollo.

d) Documentar los resultados de las pruebas realizadas.

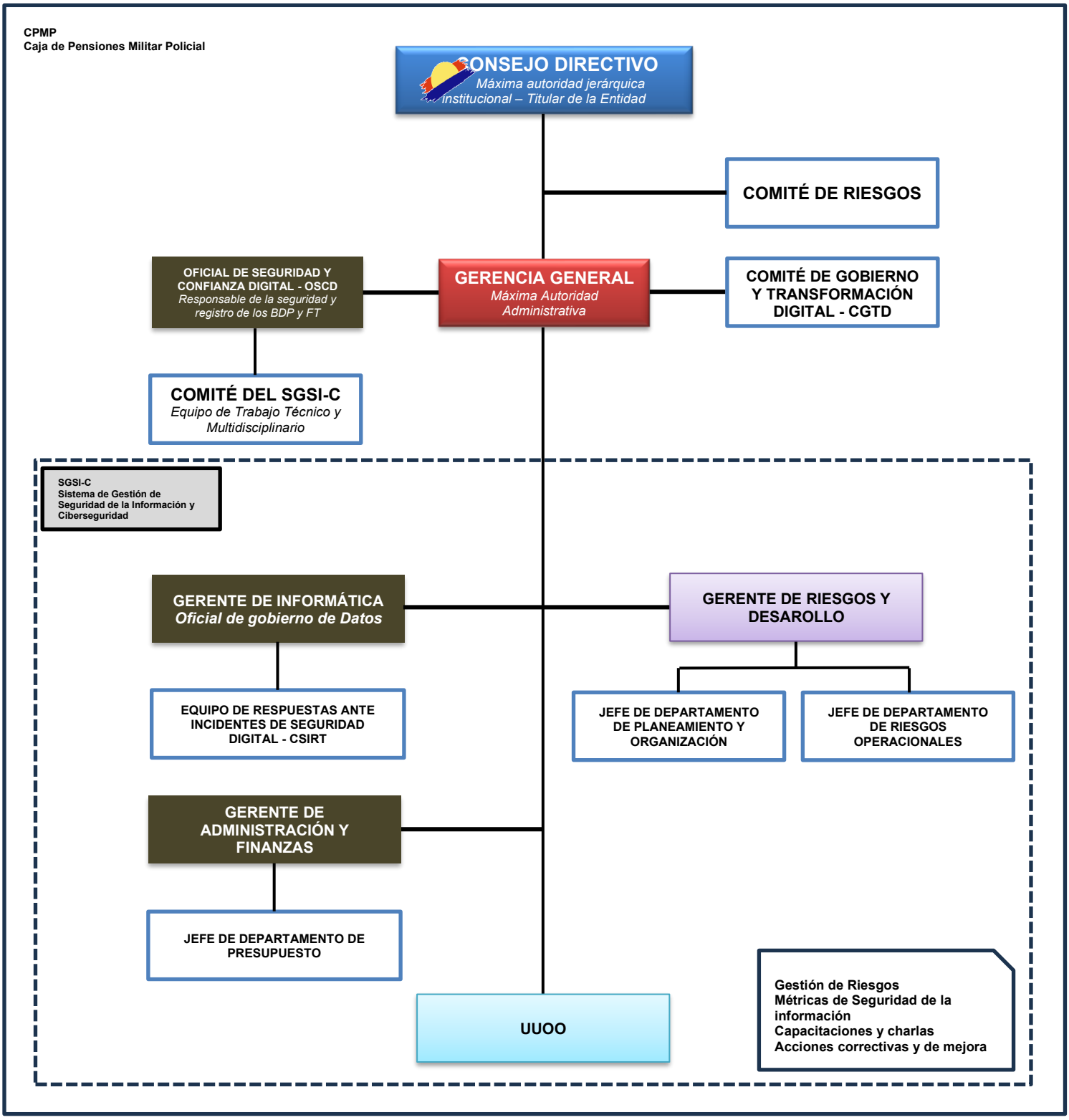
8.4.34 Protección de los sistemas de información durante las pruebas de auditoría

Se establecerá y mantendrá un programa de auditorías internas para verificar que el SGSI-C es conforme con los requisitos de la Norma ISO 27001:2022 y los requisitos de la propia organización para su SGSI-C. Los resultados de las auditorías se informarán a la dirección pertinente y se tomarán acciones correctivas oportunas para abordar las no conformidades.

Las pruebas de auditoría que afecten la disponibilidad de los sistemas deben ejecutarse fuera del horario de oficina previa coordinación entre el auditor, el OSCD, el DISI y los responsables de las UUOO cuya información se encuentre involucrada en la auditoría.

9. ESTRUCTURA ORGANIZACIONAL DEL SGSI-C

9.1 Estructura Organizativa – Sistema de Gestión de Seguridad de la Información y Ciberseguridad



9.1.1 Consejo Directivo

a) Aprobar el plan estratégico del SGSI-C.

b) Aprobar las políticas y objetivos para implementar, operar, mantener y mejorar el SGSI-C.

c) Asignar los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento.

d) Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados.

e) Tomar conocimiento del desempeño, de los resultados y de los acuerdos adoptados de la gestión integral de riesgos relacionados al SGSI-C.

9.1.2 Comité de Riesgos

a) Aprobar el plan de capacitación a fin de garantizar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades en el marco de la seguridad de la información.

b) Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.

c) Revisar y presentar semestralmente al Consejo Directivo el desempeño, los resultados y los acuerdos adoptados de la gestión integral de riesgos relacionados al SGSI-C.

d) Revisar y presentar semestralmente al Consejo Directivo, los resultados de las auditorías internas y/o externas, y los indicadores clave (KRIs) del SGSI-C.

9.1.3 Gerencia General

a) Revisar y elevar al Consejo Directivo el plan estratégico del SGSI-C.

b) Aprobar el plan de Implementación del SGSI-C.

c) Informar semestralmente al Consejo Directivo los avances y dificultades en la implementación y u operación del SGSI-C.

d) Velar por el cumplimiento de las políticas, objetivos planes, procedimientos y marco normativo en confianza y seguridad digital.

e) Adoptar las medidas necesarias para implementar y mantener adecuadamente el SGSI-C, de acuerdo a las disposiciones del Consejo Directivo y a lo dispuesto en la normativa vigente.

f) Brindar recursos, personal y/o asesorías a las UUOO para la implementación, mantenimiento y mejora continua del SGSI-C, previamente aprobados en el presupuesto institucional.

9.1.4 Comité de Gobierno y Transformación Digital - CGTD

El CGTD es responsable de dirigir, mantener y supervisar estratégicamente los planes, resultados y recursos del SGSI-C. A solicitud del Consejo Directivo o de la Gerencia General, puede emitir opiniones y recomendaciones sobre la gestión estratégica del SGSI-C. Además, la entidad podrá requerir la opinión de órganos consultivos relacionados con la gestión de riesgos. Sus funciones se encuentran establecidas en la Resolución de Gerencia General Nº 042-2023/CPMP-GG, o documento que lo reemplace.

Así mismo, el Comité de Gobierno y Transformación Digital está conformado por:

Rol en el CGTD	Cargo en la CPMP
Titular de la Entidad o su representante	Gerente General
Líder de Gobierno y Transformación Digital - secretario técnico del Comité	Gerente de Informática
Responsable del área de informática o quien haga sus veces	Jefe de Departamento de Desarrollo y Mantenimiento de Sistemas de Información
Responsable del área de recursos humanos o quien haga sus veces	Jefe de Departamento de Gestión de Personas
Responsable del área de atención al ciudadano o quien haga sus veces	Gerente de Pensiones
Oficial de Seguridad y Confianza Digital	Jefe de Departamento de Infraestructura y Seguridad Informática
Responsable del área legal o quien haga sus veces	Gerente Legal
Responsable del área de planificación o quien haga sus veces	Jefe de Departamento de Presupuesto

9.1.5 Comité del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C)

El Comité del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (Comité del SGSI-C) es un equipo de trabajo técnico y multidisciplinario para el SGSI encargado de realizar la implementación y mantenimiento del SGSI de la CPMP. Dicho equipo de trabajo es liderado por el OSCD. La organización del equipo de trabajo debe

considerar el contexto, tamaño, complejidad y estructura de la entidad. El Comité del SGSI-C está conformado por:

Titular	Suplente
Oficial de Seguridad y Confianza Digital	Especialista en Seguridad de Información
Jefe de Departamentos de Riesgos Operacionales	Analista de Riesgos Operacionales
Gerente de Informática	Jefe de Departamento de Desarrollo y Mantenimiento de Sistemas de Información
Gerente de Administración y Finanzas	Subgerente de Logística

Se podrá convocar a las reuniones del Comité a cualquier UO de la CPMP.

Las funciones del Comité del SGSI-C son:

a) Revisar y elevar a Gerencia General el plan estratégico del SGSI-C.

b) Revisar y elevar a la Gerencia General el plan de implementación del SGSI-C.

c) Revisar y elevar a la Gerencia General, las políticas, manuales y procedimientos, para implementar, operar, mantener y mejorar el SGSI-C.

d) Proponer la organización, roles y responsabilidades para el SGSI-C al Consejo Directivo.

e) Recomendar acciones a seguir al Comité de Riesgos.

f) Proponer al Comité de Riesgos el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el Consejo Directivo cuenten con competencias necesarias en seguridad de la información y ciberseguridad.

g) Revisar y elevar el plan de fomento de la cultura de riesgo al Comité de Riesgos.

h) Revisar y aprobar los planes, instructivos, guías, formatos y documentación en general relacionada con el SGSI-C.

i) Elaborar e informar semestralmente al Comité de Riesgos el desempeño, los resultados y los acuerdos adoptados de la gestión

integral de riesgos relacionados al SGSI-C, a través del Gerente de Riesgos y Desarrollo.

j) Elaborar e Informar semestralmente al Comité de Riesgos, los resultados de las auditorías internas y/o externas, y los indicadores clave (KRIs) del SGSI-C.

k) Elevar a la Gerencia General, las propuestas de solicitud de recursos, personal y/o asesorías, necesarios para el desarrollo del SGSI-C.

9.1.6 Oficial de Seguridad y Confianza Digital (OSCD)

Es la persona responsable de coordinar la implementación, operación, mantenimiento y mejora continua del (SGSI-C) en la CPMP, atendiendo políticas y normas en materia de seguridad digital, confianza digital y gobierno digital. Además, coordina y reporta al Comité de Gobierno y Transformación Digital institucional, la implementación, mantenimiento, y la aplicación de las normas relacionadas con la seguridad digital, confianza digital, transformación digital, y gobierno digital, cuyas responsabilidades son:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI-C de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

b) Coordinar con las UUOO de la entidad las acciones orientadas a implementar y/o mantener el SGSI-C, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

c) Formular y elevar al Comité del SGSI-C, el plan estratégico del SGSI-C.

d) Formular y elevar al Comité del SGSI, el plan de Implementación del SGSI-C y registrarlo en la Plataforma Facilita Perú.

e) Formular y elevar al Comité del SGSI las políticas, manuales, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.

f) Promover la conformación y adecuada operación del Equipo de respuestas ante incidentes de seguridad de la información.

g) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.

h) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.

i) Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.

j) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.

k) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la CPMP e informarlos a la Gerencia General.

l) Informar a la Gerencia General acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI-C, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la CPMP, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital. Formula y propone indicadores clave de desempeño del SGSI.

m) Coordinar con el CNSD y con el Comité del SGSI las acciones de sensibilización y capacitación para los funcionarios y colaboradores de la CPMP sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital, gobierno digital, uso de plataformas interoperables, ética en tecnología de información, protección de datos personales.

n) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la CPMP a fin de fortalecer la confianza en el entorno digital.

o) Coordinar con el CSIRT el registro y notificación obligatoria al CNSD de cualquier incidente de seguridad digital, e intercambio de información en materia de seguridad digital.

p) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.

q) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las UUOO de la CPMP su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.

r) Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la Gerencia de Informática cuando ésta adquiera, tercerice o desarrolle software o implemente otro tipo de soluciones tecnológicas.

s) Coordinar con la Gerencia de Informática, cuando corresponda, en los temas relativos a sus responsabilidades.

t) Otras responsabilidades afines que le sean asignadas por la Gerencia General.

9.1.7 Gerente de Riesgos y Desarrollo

a) Velar por una adecuada gestión de seguridad de la información y ciberseguridad, que promueva el alineamiento de la toma de decisiones de la entidad con el apetito de riesgo operacional.

b) Verificar periódicamente que las políticas, procedimientos, metodologías y demás normas internas relacionadas con la gestión de seguridad de la información y ciberseguridad sean consistentes con el tamaño, la complejidad de las operaciones y la estructura de la CPMP.

c) Informar a la Gerencia General y al Comité de Riesgos, los resultados de la gestión integral de riesgos relacionados al SGSI-C emitidos por el Comité del SGSI-C.

d) Comunicar, a la Gerencia General y al Comité de Riesgos, el desempeño y los acuerdos adoptados emitidos por el Comité del SGSI-C.

e) Comunicar a la Gerencia General y al Comité de Riesgos, los resultados de las auditorías internas y/o externas de seguridad de la información y los indicadores clave emitidos por el Comité del SGSI-C.

f) Enviar a través de la extranet de la SBS, el informe electrónico anual (a través del aplicativo IG-ROp) de la gestión de seguridad de la información y ciberseguridad dentro de los plazos establecidos según Resolución SBS Nº 2116-2009.

9.1.8 Jefe de Departamento de Planeamiento y Organización

a) Orientar al OSCD para asegurar una adecuada articulación con el plan estratégico y el plan operativo institucional orientada a implementar, operar, mantener y mejorar el SGSI-C.

9.1.9 Jefe de Departamento de Riesgos Operacionales

a) Participar en el diseño y permanente actualización de las Normas y Procedimientos del Sistema de Gestión de Seguridad de la Información, en coordinación con el OSCD.

b) Desarrollar la metodología para gestión de seguridad de la Información y ciberseguridad, en coordinación con el OSCD.

c) Identificar las necesidades de capacitación y difusión para una adecuada gestión de seguridad de la información y ciberseguridad en coordinación con el OSCD y presentarlas al Comité del SGSI.

d) Promover y coordinar con el OSCD, la ejecución de todas las actividades relacionadas con el proceso de implementación, operación, seguimiento y mejora continua del SGSI-C.

e) Realizar la supervisión, actualización y cumplimiento de la presente directiva, en coordinación con el OSCD.

f) Evaluar los riesgos del SGSI-C ante cambios significativos a nivel de procesos y tecnología en coordinación con el OSCD.

g) Elaborar el informe electrónico anual (a través del aplicativo IG-ROp) de la gestión de seguridad de la información y ciberseguridad dentro de los plazos establecidos (a más tardar el 31 de marzo del año siguiente al año del reporte, según Resolución SBS Nº 2116-2009).

9.1.10 Equipo de respuestas ante incidentes de seguridad digital (CSIRT)

El Equipo de respuestas ante incidentes de seguridad digital (CSIRT: *Computer Security Incident Response Team*): Es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza, su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros. Es un equipo técnico conformado principalmente por especialistas en seguridad de las tecnologías de la información o informática.

El Equipo de respuestas ante incidentes de seguridad digital está conformado por:

Rol	Titular	Suplente
Coordinador del CSIRT	Gerente de Informática	El/La colaborador(a) que asuma la encargatura
Gestor de Incidentes	Especialista en Seguridad de Información	Analista Funcional - DDMSI
Gestor de Redes y Comunicaciones/Gestor de Infraestructuras Digitales	Analista de Infraestructura - DISI	Asistente de Soporte Técnico I - DDMSI
Oficial de Seguridad y Confianza Digital	Jefe de Departamento de Infraestructura y Seguridad Informática	El/La colaborador(a) que asuma la encargatura
Gestor de Riesgos de Seguridad de la Información	Jefe de Departamento de Riesgos Operacionales	El/La colaborador(a) que asuma la encargatura

Es el encargado de gestionar la contención, respuesta y recuperación ante incidentes de seguridad digital para la protección de los activos de información frente a amenazas que atenten o comprometan la seguridad digital.

Sus funciones se encuentran establecidas en el artículo 2º de la Resolución de Gerencia General Nº 011-2024/CPMP-GG.

9.1.11 Gerente de Informática

a) Informar al OSCD todo incidente de seguridad digital crítico que afecte lo procesos misionales y servicios que brinda la CPMP de forma inmediata.

b) Articular con el OSCD la implementación de controles de seguridad de la información y coordina con el CSIRT la gestión de incidentes de seguridad digital.

c) Planificar, desarrollar, implantar y gestionar el sistema de información, infraestructura tecnológica, telecomunicaciones y estadísticas, que brinden el soporte de las funciones, desarrolladas por las diferentes UUOO estableciendo políticas, estándares y procedimientos.

d) Colaborar con el OSCD y con el Jefe de Departamento de Riesgos Operacionales integrar las mejores prácticas de seguridad en la gestión de Tecnología de la Información y Comunicaciones.

9.1.12 Gerente de Administración y Finanzas

a) Asegurar la disponibilidad de recursos financieros para implementar y mantener las políticas de seguridad de la información y ciberseguridad.

b) Gestionar el presupuesto y controlar los costos asociados a la gestión de seguridad de la información y ciberseguridad.

c) Asegurar el cumplimiento de las normativas financieras relacionadas con la seguridad digital.

d) Proveer el apoyo administrativo necesario para la implementación y mantenimiento asociados a la gestión de seguridad de la información y ciberseguridad.

9.1.13 Jefe de Departamento de Presupuesto

a) Responsable de conducir el proceso presupuestario de la CPMP, incluyendo las modificaciones orientadas para implementar, operar, mantener y mejorar el SGSI-C.

b) Orientar al OSCD para asegurar una adecuada articulación con el presupuesto de la CPMP.

9.1.14 Oficial de Gobierno de Datos

Las responsabilidades del Oficial de Gobierno de Datos de la CPMP se encuentran establecidas en la Directiva Nº 001-2022-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Gobierno de Datos aprobada con Resolución de Secretaría de Gobierno y Transformación Digital Nº 001-2022-PCM/SGTD y sus modificatorias. Sus funciones se encuentran establecidas en el artículo 3º de la Resolución de Gerencia General Nº 031-2024/CPMP-GG.

9.1.15 Oficial de Datos Personales

a) La designación, responsabilidades y perfil del ODP se establecen en la directiva RD 100-JUS/DGTAIPD.

b) Informar y asesorar al titular del banco de datos personales, al responsable del tratamiento y al personal que intervenga en dicho tratamiento, respecto de las obligaciones que le corresponden conforme a la normativa sobre protección de datos personales en la CPMP.

c) Vigilar y evaluar el cumplimiento de la normativa vigente y de las políticas internas del titular del banco de datos o del encargado del tratamiento, incluyendo la asignación de responsabilidades, la capacitación del personal involucrado y la realización de auditorías en materia de protección de datos personales.

d) Actuar como punto de contacto y cooperar, en lo que resulte pertinente, con la Autoridad Nacional de Protección de Datos Personales para el ejercicio de sus funciones y atribuciones.

9.1.16 Propietario de la Información o activos de información/Dueños de los procesos

a) Apoyar en la gestión de riegos e implementación de controles de seguridad de la información identificados en sus ámbitos de competencia, así como también coadyuvan en la gestión de incidentes según corresponda.

b) Clasificar la información de los procesos bajo su responsabilidad y establecer su nivel de criticidad y disposición final. A su vez deberá determinar cuando la información ya no es necesaria y el tiempo de retención en coordinación con su respectiva Gerencia.

c) Participar en la identificación y gestión de los riesgos de información asociados con los activos.

d) Ser responsable por la calidad, consistencia y disponibilidad de los datos, por lo que deberá tomar medidas para minimizar el riesgo por pérdida o exposición de la seguridad de la información bajo su responsabilidad.

e) Autorizar accesos a la información y ratificar periódicamente las decisiones sobre los mismos, así como dar cumplimiento las disposiciones sobre accesos a los sistemas de información.

f) Revisar la clasificación de la información y los accesos de los procesos bajo su responsabilidad periódicamente.

g) Apoyar en la gestión de los incidentes de seguridad de la información según corresponda.

9.1.17 Custodios de la Información

a) Preservar y proteger la información que le ha sido confiada en custodia.

b) Cumplir con las Políticas de Seguridad de la Información del CPMP y los especificados por el propietario de la información.

c) Realizar conjuntamente con los propietarios de la información, pruebas de contingencia y asegurar que todos los empleados y/o usuarios involucrados conozcan sus responsabilidades.

9.1.18 Personal de la CPMP

a) Cumplir las Políticas de Seguridad de la Información de la CPMP y documentos relacionados a la Seguridad de la Información de la CPMP.

b) Asegurar la protección de los activos de la información involucrados en las labores que realizan.

c) Informar a su inmediato superior, al OSCD y al Departamento de Riesgos Operacionales sobre la identificación de deficiencias e incidentes en materia de seguridad de la información.

10. ANÁLISIS DE RIESGOS

El análisis de riesgos permite determinar las vulnerabilidades de los activos de información de la CPMP y asimismo clasificarlos por su criticidad. También facilita la implementación de controles para tratar los riesgos asociados a los activos de información.

11. INFORMACIÓN A LA SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP (SBS)

11.1 Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por la SBS a través de su "Reglamento para la Gestión del Riesgo Operacional", la CPMP debe incluir información sobre la gestión de seguridad de la información y ciberseguridad.

11.2 La CPMP informa a la SBS la ocurrencia de un evento de interrupción significativa de las operaciones, en cuanto tome conocimiento y dentro de un plazo máximo de un (1) día hábil. Para tal efecto, se entiende como evento de interrupción significativa de las operaciones, a un evento que implique cualquiera de las siguientes situaciones:

11.2.1 La suspensión en la entrega de los productos y servicios priorizados por un tiempo mayor a los respectivos TOR.

11.2.2 La activación del plan de gestión de crisis (la función de activación (ejecución) del "Plan de Gestión de Crisis" le corresponde al Equipo de Gestión de Crisis, establecido en la directiva "Políticas y Objetivos de Continuidad del Negocio").

12. CUMPLIMIENTO Y CONFORMIDAD

El cumplimiento de la Política de Seguridad de la Información es obligatorio para las UUOO de la CPMP. En el caso de incumplimiento, la CPMP aplicará a los responsables las medidas necesarias según el Reglamento Interno de Trabajo de la CPMP.

13. VIGENCIA

La Política de Seguridad de la Información y Ciberseguridad de la CPMP entra en vigencia a partir de su aprobación y deberá ser revisada, y actualizada en caso corresponda, una vez al año o en caso de producirse modificaciones a las normas legales o cambios significativos en la organización o en los procesos que afecten la seguridad de la información.

14. MONITOREO, SEGUIMIENTO Y EVALUACIÓN

La Política de Seguridad de la Información y Ciberseguridad de la CPMP, será monitoreada en forma permanente con la revisión de los controles de seguridad, de acuerdo a lo establecido en el numeral 8. Políticas Específicas de Seguridad de la Información.

El seguimiento a la Política de Seguridad de la información y Ciberseguridad se realizará con la medición del cumplimiento de los objetivos de seguridad de la información a través de los indicadores y metas del SGSI.

La evaluación de la Política de Seguridad de la Información se realizará en forma anual, asimismo, se informará del progreso de la implementación del SGSI.

15. DISPOSICIONES COMPLEMENTARIAS

Quedan sin efecto la Directiva de Consejo Directivo DCD Nº 10-2021 y otras disposiciones que contravengan la presente directiva.

CAJA DE PENSIONES MILITAR POLICIAL

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
1. FINALIDAD	Establecer los lineamientos ~~de la política y objetivos de seguridad de la información y ciberseguridad~~ de la Caja de Pensiones Militar Policial (CPMP)~~, a fin de garantizar la~~ disponibilidad~~,~~ confidencialidad ~~e~~ integridad de la información.	Establecer los lineamientos **generales y compromisos** de la Caja de Pensiones Militar Policial (CPMP) **para el diseño, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de su Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C), garantizando la** confidencialidad, integridad**,** disponibilidad de la información **de acuerdo con los principios de la normativa de Gobierno Digital. Esta política proporciona un marco para el establecimiento de los objetivos de seguridad de la información y reafirma el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.**	Se actualizó la finalidad.
2. REFERENCIA LEGAL Y NORMATIVA	(…) • ~~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 • Decreto Supremo Nº 101-2021-EF – Normas Reglamentarias y Complementarias del Decreto Legislativo ~~Nº~~ 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~~ • ~~Decreto 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~~	(…) • 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 **Nº** 1133, Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial**, y sus modificatorias** • **Decreto Ley Nº 19846 – Ley de Pensiones Militar Policial** y sus modificatorias • **Decreto Supremo Nº 009-DE-CCFA – Reglamento de la Ley de Pensiones Militar Policial** y sus modificatorias • **Decreto Supremo Nº 126-2025-PCM – Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento** • **Decreto de Urgencia N° 007-2020 – Aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y sus modificatorias** • **Decreto Supremo N° 002-97-TR Texto Único Ordenado del D. Leg. Nº 728 – Ley de Formación y Promoción Laboral** • **Decreto Supremo Nº 021-2019-JUS - Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública**	Se actualizó la referencia legal y normativa.

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	• Decreto Supremo Nº ~~072-2003-PCM~~ – Reglamento de la Ley de Transparencia y Acceso a la Información Pública	• Decreto Supremo Nº **007-2024-JUS** - Reglamento de la Ley de Transparencia y Acceso a la Información Pública • **Resolución de Contraloría General Nº 320-2006-CG – Normas de Control Interno** • **Resolución Directoral N° 022-2022-INACAL/DN que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.**	
	• Resolución SBS Nº 2116-2009 – Reglamento para la Gestión del Riesgo Operacional	• Resolución SBS Nº 2116-2009 – Reglamento para la Gestión del Riesgo Operacional **y sus modificatorias**	
	• Resolución SBS Nº 272-2017 – Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos sus modificatorias	• Resolución SBS Nº 272-2017 – Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos **y** sus modificatorias	
	• Resolución SBS Nº 504-2021 – Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad	• Resolución SBS Nº 504-2021 – Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad **y sus modificatorias** • **Resolución Ministerial Nº 119-2018-PCM – Disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública y sus modificatorias** • **Resolución de Secretaría de Gobierno y Transformación Digital Nº 003-2023-PCM/SGTD - Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas** • **Resolución SBS Nº 877-2020 – Reglamento para la Gestión de la Continuidad del Negocio** • **Resolución Ministerial Nº 320-2021-PCM - Lineamientos para la gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de gobierno** • **Resolución Secretarial de Gobierno y Transformación Digital Nº 002-2023-PCM/SGTD que aprueban la Directiva Nº 001-2023-PCM/ SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital** • **Resolución Secretarial Nº 001-2018-PCM/SEGDI, que aprueba los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano** • **Resolución de Gerencia General Nº 042-2023-/CPMP-GG - Reconformación del Comité de Gobierno y Transformación Digital de la CPMP** • **Resolución de Gerencia General Nº 001-2024/CPMP-GG - Designación del Jefe de Infraestructura y Seguridad Informática de la Gerencia de Informática - Oficial de Seguridad y Confianza Digital de la CPMP** • **Resolución de Gerencia General Nº 011-2024/CPMP-GG - Reconformación del Equipo de respuestas ante incidentes de seguridad digital de la CPMP** • **Resolución de Gerencia General Nº 031-2024/CPMP-GG – Designación del Gerente de Informática como Oficial de Gobierno de Datos de la CPMP** • **Ley Nº 29733 - Ley de Protección de Datos Personales y sus modificatorias** • **Decreto Supremo Nº 016-2024-JUS –**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	(…) • Directiva de Consejo Directivo ~~Nº 12-2018~~ – Reglamento del Comité de Riesgos • ~~Directiva de Gerencia General Nº 02-GG-2018 – Normas y Procedimientos para la Atención de Solicitudes sobre Acceso a la Información Pública~~ • Directiva de Consejo Directivo Nº 15-2020 – Políticas y Objetivos de Continuidad del Negocio (…)	**Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales** • **Resolución Directoral N° 019-2013-JUS/DGPDP que aprueba la Directiva de seguridad para el tratamiento de datos personales** • **Resolución Directoral Nº 100-2025-JUS-DGTAIPD que aprueba la Directiva que establece las disposiciones para la designación, desempeño y funciones del Oficial de Datos Personales.** • **Ley Nº 30096 - Ley de Delitos Informáticos y sus modificatorias** • **Ley Nº 31572 - Ley del Teletrabajo y sus modificatorias** • **Decreto Supremo Nº 002-2023-TR - Reglamento de la Ley Nº 31572 – Ley del Teletrabajo** (…) • **Reglamento Interno de Trabajo de la Caja de Pensiones Militar Policial** • Directiva de Consejo Directivo DCD **Nº 14-2024** – Reglamento del Comité de Riesgos • Directiva de Consejo Directivo **DCD** Nº 15-2020 – Políticas y Objetivos de Continuidad del Negocio (…) • **Directiva de Gerencia General Nº 01-GI-2015 – Normas y Procedimientos para la Gestión de Incidentes en la Infraestructura Informática** • **Directiva de Gerencia General Nº 02-GI-2024 – Normas y Procedimientos para la Administración de Accesos a los Servicios Informáticos** • **Directiva de Gerencia General Nº 03-GI-2024 – Normas y Procedimientos para la Administración de Hardware, Software y Servicios Informáticos** • **Directiva de Gerencia General Nº 04-GI-2024 – Plan de Seguridad Informática Institucional** • **Directiva de Gerencia General Nº 02-GAF-2024 – Normas para la Entrega de Cargos del Personal** • **Directiva de Gerencia General Nº 05-GI-2021 – Plan de Continuidad de Servicios Informáticos**	
3. ALCANCE	~~Las disposiciones contenidas~~ en la presente directiva son de cumplimiento obligatorio por parte de todas las unidades orgánicas de la CPMP.	**Los lineamientos contenidos** en la presente directiva son de cumplimiento obligatorio por parte de todas las unidades orgánicas de la CPMP**, así como de las personas naturales o jurídicas que brindan servicios o prestaciones a la entidad y tengan acceso a la información que se genera, procesa, resguarda y/o administra**.	Se actualizó el alcance.

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
4. DEFINICIONES	~~GLOSARIO~~	**DEFINICIONES** **4.1. Acceso remoto: Acceso desde un equipo de cómputo hacia un recurso informático de la CPMP ubicado físicamente en otro lugar, puede darse a través de diferentes técnicas como VPN, escritorio virtual, u otro autorizado.** **4.2. Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.**	Se actualizó las definiciones.
	~~4.1.~~ Activo de información: ~~Es la información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la CPMP y tiene un ciclo de vida.~~	**4.3.** Activos de información**: Información y otros activos asociados de los que dependen la información como bienes, servicios tangibles o intangibles y personas, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos de negocio los cuales están alineados a sus objetivos planteados.** **4.4. Activos de TI: Está referido a los activos de Tecnologías de la Información, que son los recursos tecnológicos con los que cuenta una organización como el software, hardware y servicios.** **4.5. Anonimización: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.**	
	(…)	(…) **4.7. Banco de datos personales: Conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.** **4.8. Centro Nacional de Seguridad Digital (CNSD): El CNSD gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital en el país, a fin de fortalecer la confianza digital. El CNSD es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.**	
	4.9. Ciberseguridad: Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su confidencialidad ~~o~~ integridad en el ciberespacio, el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.	4.9. Ciberseguridad: Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su confidencialidad, integridad **o disponibilidad** en el ciberespacio, el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos. **4.10. Clasificación de la información: La clasificación de la información se realiza en función de acuerdo con lo establecido en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.** **4.11. Código fuente: El código fuente es el conjunto de instrucciones escritas en un lenguaje de programación que los desarrolladores crean para que un programa informático funcione.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	~~4.4.~~ Confidencialidad: La información sólo es disponible para la entidad o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria. (…) ~~4.6. Disponibilidad: Es asegurar acceso y uso oportuno a la información~~ ~~4.7. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la CPMP, originados por la misma causa, que ocurre durante el mismo periodo de tiempo.~~	**4.12.** Confidencialidad **de la información**: La información sólo es disponible para la entidad o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria. **4.13. Controles de seguridad de la información: En seguridad de la información, los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos: salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control.** (…) **4.15. Datos personales: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.** **4.16. Datos sensibles: Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.** **4.17. Disponibilidad de la información: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.** **4.18. Dispositivo móvil: Es una computadora lo suficientemente pequeña como para sostenerla y operarla en la mano, o que puede ser transportada fácilmente. Se caracteriza por su portabilidad y su capacidad de conectividad inalámbrica (Wi-Fi , Bluetooth, redes móviles, etc.).** **4.19. Enmascaramiento de datos: Es el proceso de ocultar datos personales modificando sus letras y números originales con la finalidad de proteger su confidencialidad.** **4.20. Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.** **4.21. Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	(…)	(…)	
	~~4.9.~~ Incidente~~: Es el evento que se ha determinado que tiene un impacto adverso sobre~~ la organización~~ y que requiere de acciones de respuesta y recuperación~~.	**4.23.** Incidente **de seguridad: Uno o varios eventos no deseados o inesperados que comprometan la confidencialidad, integridad o disponibilidad de la información o los sistemas tecnológicos de** la organización.	
	(…)	(…)	
		4.25. Información confidencial: Son excepciones al ejercicio de derecho de información, incluye datos personales, información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil.	
	~~4.11.~~ Integridad: Es asegurar el no repudio de la información y su autenticidad, y evitar su modificación o destrucción indebida.	**4.26.** Integridad **de la información:** Es asegurar el no repudio de la información y su autenticidad, y evitar su modificación o destrucción indebida.	
		4.27. IP - *Internet Protocol* o Protocolo de Internet. - La IP es una dirección única que identifica a un dispositivo en Internet o en una red local.	
	~~4.12. Propietario del activo de información: Es el responsable de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Asimismo, define y revisa periódicamente las restricciones y clasificaciones de acceso.~~	**4.28. Líder de Gobierno y Transformación Digital: Persona responsable de coordinar las políticas, objetivos, planes y acciones para desplegar la transformación digital y el desarrollo del Gobierno Digital en la entidad. El Líder de Gobierno y Transformación digital recae en el Gerente de Informática de la CPMP. En la conformación del Comité de Gobierno y Transformación Digital, el Líder de Gobierno y Transformación Digital actúa como Secretario Técnico de dicho Comité.**	
		4.29. Logueo: Acción de ingresar a un sistema de información o servicio informático.	
		4.30. Medios removibles de almacenamiento: Se refiere a un tipo de soporte de almacenamiento de datos que está diseñado para ser fácilmente insertado y retirado de un dispositivo (como una computadora, una cámara, un reproductor de música, etc.) sin la necesidad de apagar el equipo. Su principal característica es la portabilidad, permitiendo transportar información de un lugar a otro o entre diferentes dispositivos.	
		4.31. Mejora continua: Es la actividad recurrente para mejorar el desempeño de los procesos.	
		4.32. PIN: De las siglas en inglés, *Personal Identification Number*, es un número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema.	
	(…)	**4.33. Propietario del activo de información o sistemas de información: Individuo o entidad de forma responsable, que cuenta con la aprobación de la entidad, para el control de la producción, desarrollo, mantenimiento, utilización y seguridad de los activos. El término propietario no significa que la persona disponga de los derechos de propiedad reales del activo.**	
		4.34. Propietario del riesgo: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo, dentro del alcance de sus competencias.	
		4.35. Proveedor: Persona natural o jurídica que brinda un servicio o producto a la CPMP. En el	

<table>
<tr><th colspan="4">MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 “POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD”</th></tr>
<tr><th>SECCIÓN</th><th>DCD N° 10-2021</th><th>MODIFICACIÓN</th><th>COMENTARIOS</th></tr>
<tr><td></td><td></td><td>marco de la norma de contrataciones recibe la denominación de contratista.

4.36. Proyecto: Proceso único, que consiste en un conjunto de actividades coordinadas y controladas con fechas de inicio y finalización, llevadas a cabo para lograr un objetivo conforme con requisitos y requerimientos específicos, incluyendo las limitaciones de tiempo, coste y recursos.

4.37. Riesgo de seguridad de la información y ciberseguridad: Se refiere a la posibilidad de que una amenaza explote una vulnerabilidad en los activos de información, sistemas tecnológicos, procesos o personas de la organización, generando un impacto negativo sobre la confidencialidad, integridad y disponibilidad de la información.

(…)

4.39. Seguridad digital: Es la confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas y sistemas de información.

4.40. Siglas:

<table><tr><th>Abreviatura</th><th>Descripción</th></tr><tr><td>ANPD</td><td>Autoridad Nacional de Protección de Datos Personales</td></tr><tr><td>ODP</td><td>Oficial de Datos Personales</td></tr><tr><td>OSC</td><td>Oficial de Seguridad y Confianza Digital</td></tr><tr><td>CNSD</td><td>Centro Nacional de Seguridad Digital</td></tr><tr><td>CSIRT</td><td>Del término inglés Computer Security Incident Response Team, cuya correspondencia equivale a Equipo de respuestas ante incidentes de seguridad digital</td></tr><tr><td>GAF</td><td>Gerencia de Administración y Finanzas</td></tr><tr><td>DRO</td><td>Departamento de Riesgos Operacionales</td></tr><tr><td>SGL</td><td>Subgerencia de Logística</td></tr><tr><td>DISI</td><td>Departamento de Infraestructura y Seguridad Informática</td></tr><tr><td>DGP</td><td>Departamento de Gestión de Personas</td></tr><tr><td>DDMSI</td><td>Departamento de Desarrollo y Mantenimiento de Sistemas de Información</td></tr><tr><td>CPMP</td><td>Caja de Pensiones Militar Policial</td></tr><tr><td>PCM</td><td>Presidencia del Consejo de Ministros</td></tr><tr><td>UO / UUOO</td><td>Unidad Orgánica / Unidades Orgánicas</td></tr><tr><td>UPS</td><td>Del término inglés Uninterruptible Power Supply, Sistema de Alimentación Ininterrumpida.</td></tr><tr><td>SGSI-C</td><td>Sistema de Gestión de Seguridad de la Información y Ciberseguridad</td></tr><tr><td>TI</td><td>Tecnologías de Información</td></tr></table>
4.41. Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C): Es un marco estratégico que permite a una organización gestionar, proteger y mejorar de manera continua la seguridad de su información y activos tecnológicos frente a riesgos y amenazas. Este sistema integra políticas, procesos, roles, tecnologías y controles diseñados para garantizar que los objetivos de seguridad de la información se cumplan de manera eficaz.

4.42. Teletrabajo: Modalidad especial de prestación de labores, de condición regular o habitual. Se caracteriza por el desempeño subordinado de aquellas labores sin presencia física del trabajador o servidor civil en el centro de trabajo, con la que mantiene vínculo laboral.</td><td></td></tr>
<tr><td></td><td>~~4.14. Tiempo objetivo de recuperación (TOR): Tiempo establecido por la CPMP para reanudar operaciones, en caso de ocurrencia de una interrupción.~~

~~4.15. Usuario: Persona natural o jurídica que utiliza o puede utilizar los productos ofrecidos por la CPMP.~~

(…)</td><td></td><td></td></tr>
</table>

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		4.43. Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales. **4.44. Transformación digital: La transformación digital es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.** **4.45. Tercero: Toda persona que no cuentan con vínculo laboral con la CPMP, pero requiere hacer uso de sus activos de información ya sea para la prestación de un servicio (proveedores), en calidad de visitante o administrado (empresa operadora o usuario de servicio de telecomunicaciones).** **4.46. Unidades Orgánicas: Están compuestas por los gerentes, subgerentes, jefes, custodio del activo de información, propietario del activo de información, usuarios o dueños de proceso.** (…)	
	(…)	(…)	
5. PRINCIPIOS		**La Política de Seguridad de la Información de la CPMP se sustenta en los siguientes principios:** **5.1. Principio de confidencialidad: Garantizar que la información sea accesible solo para aquellas personas autorizadas a tener acceso a la misma.** **5.2. Principio de colaboración y cooperación: Se promueve el intercambio y transferencia de información, mejores prácticas, recursos y experiencias a nivel nacional e internacional, a fin de identificar, prevenir y mitigar riesgos en el entorno digital que afecten la continuidad de funciones u operaciones de las entidades públicas, organizaciones del sector privado, el bienestar de las personas y el desarrollo sostenible del país.** **5.3. Principio de gestión de riesgos: La gestión de riesgos se sustenta en la aplicación de estándares y mejores prácticas que permitan reducir los incidentes de seguridad. El diseño, implementación y mejora de las medidas y controles de seguridad digital se basan en la evaluación de riesgos.** **5.4. Principio de privacidad y seguridad desde el diseño: Se promueve la adopción de medidas preventivas de tipo tecnológico, organizacional, legal, humano y procedimental en todas las etapas del ciclo de vida de los servicios digitales, que preserven la disponibilidad, integridad, y confidencialidad de los datos personales e información y, cuando corresponda, la autenticidad de los datos y no repudio de la información proporcionada.** **5.5. Principio de Recuperación y resiliencia digital: Implica la capacidad por la que se adoptan medidas a fin de anticipar, responder, recuperarse y aprender ante incidentes de seguridad digital.** **5.6. Principio de respeto de los derechos humanos: El diseño, implementación y mantenimiento de**	Se incorporó los principios.

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		medidas y controles de seguridad digital en la prestación de servicios digitales, deben respetar los derechos humanos, garantizando que no existan efectos adversos a derechos como la vida, la libre expresión, la autodeterminación de la persona, la igualdad de trato, la protección de los datos personales y la no discriminación, entre otros, establecidos en los instrumentos internacionales sobre derechos humanos. **5.7. Principio de responsabilidad: Implica el compromiso a rendir cuenta sobre las medidas y controles para gestionar los riesgos de la seguridad digital en base a sus capacidades y contexto.** **5.8. Principio de transparencia: Se promueve que la provisión de datos o información a través del uso de tecnologías digitales en entornos digitales, independientemente de donde se encuentren almacenados, sea efectiva, clara, visible, confiable, comprensible, coherente para el ciudadano y personas en general; para lo cual se busca que toda información o datos que se gestionan en sistemas o plataformas digitales sean fidedignos, completos, íntegros, coherentes, consistentes y precisos, de conformidad con las normas legales vigentes.** **5.9. Principio de integridad: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento. En la interacción en el entorno digital o cualquier proceso de diseño, producción, despliegue y operación de plataformas, servicios digitales o uso de la tecnología digital, las personas deben tener una conducta proba, imparcial, honesta y ética en el uso de las tecnologías digitales, contribuyendo al fortalecimiento de la confianza digital, de conformidad con las disposiciones normativas vigentes.** **5.10. Principio de disponibilidad: Garantizar que los usuarios autorizados tengan accesos a la información y a los recursos necesarios con la misma, toda vez que lo requieran.** **5.11. Principio de no repudio: Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.** **5.12. Principio de auditabilidad: Asegurar que los eventos de un sistema deben poder ser registrados para su control posterior.** **5.13. Principio de legalidad: Garantizar el cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la institución.** **5.14. Principio de calidad: Salvaguardar la veracidad, exactitud y actualización de la información que administra.** **5.15. Principio de seguridad: Adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos y la información.**	
6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN		**La CPMP como entidad pública administradora de fondos de pensiones del personal militar y policial considera a la información como un activo valioso para el cumplimiento de sus funciones y alcance de sus objetivos estratégicos, por esta razón, gestiona la seguridad de la información física y digital bajo su responsabilidad y se compromete a:**	Se incorporó la Política General de Seguridad de la Información.

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		6.1. Preservar la confidencialidad, integridad y disponibilidad de la información y sus procesos de acuerdo con el marco normativo y regulatorio vigente. **6.2. Preservar la confidencialidad, integridad y disponibilidad de la información y sus procesos de acuerdo con el marco normativo y regulatorio vigente.** **6.3. Fortalecer la cultura de seguridad de la información a través de programas de concienciación y capacitación.** **6.4. Promover la gestión eficaz de sus riesgos, eventos e incidentes de seguridad de la información, con la finalidad de garantizar la disponibilidad de los servicios y recursos informáticos.** **6.5. Apoyar los objetivos y disposiciones de seguridad de la información designando los recursos necesarios para la ejecución de sus planes, así como el establecimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.**	
7. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	~~5.2. Objetivos~~ de seguridad de la información y ciberseguridad ~~5.2.1. Asegurar la disponibilidad de la información de manera oportuna para los diferentes usuarios internos y externos.~~ ~~5.2.2. Garantizar el acceso a la información de acuerdo a los niveles de la CPMP autorizados y criterios de seguridad que establezca la institución, la normativa aplicable y/o las partes interesadas.~~ ~~5.2.3. Fortalecer los mecanismos que aseguren la integridad de la información.~~	**7.1. Fortalecer la cultura** de seguridad de la información y ciberseguridad **en los funcionarios y colaboradores de la CPMP.** **7.2. Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información y ciberseguridad.** **7.3. Implementar controles para asegurar la confidencialidad, integridad y disponibilidad de la información de la CPMP, así como la continuidad de los servicios.** **7.4. Asegurar el cumplimiento de requerimientos legales y regulatorios en materia de seguridad y confianza digital** **7.5. Establecer, implementar, operar, evaluar y mejorar el Sistema de Gestión de Seguridad de la Información y Ciberseguridad de la CPMP.**	Se actualizó los Objetivos de Seguridad de la Información y Ciberseguridad
8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN		**En el contexto de la implementación del SGSI de la CPMP, siguiendo los requisitos y controles de la NTP ISO/IEC 27001:2022 "Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos", 3ª Edición, se definen las Políticas Específicas de Seguridad de la Información en este documento. En este sentido, la CPMP manifiesta su compromiso, a través del OSCD, de llevar a cabo lo siguiente:** **a) Difundir periódicamente las Políticas Específicas de Seguridad de la Información de la CPMP entre los colaboradores.** **b) Evaluar el cumplimiento de la implementación de los controles de seguridad de la información, como resultado de la aplicación de las Políticas Específicas de Seguridad de la Información.** **c) Revisar y actualizar, de ser necesario, las Políticas Específicas de Seguridad de la Información de la CPMP en un plazo de un año, contado a partir de la aprobación y publicación de este documento o antes, en caso de producirse cambios**	Se incorporó las Políticas Específicas de Seguridad de la Información

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		significativos que afecten la seguridad de la información. **Las siguientes políticas específicas se encuentran agrupadas en cuatro secciones de acuerdo con la categorización de controles de seguridad proporcionada en la NTP ISO /IEC 27002:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información", 3ª Edición.** **8.1. Controles organizacionales** **8.1.1. Roles y responsabilidades en seguridad de la información** **Se han establecido los siguientes roles para efectuar la implementación, mantenimiento del SGSI y la operación de los controles de seguridad de la información.** **• Consejo Directivo** **• Comité de Riesgos** **• Gerencia General** **• Comité del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C)** **• Oficial de Seguridad y Confianza Digital (OSCD)** **• Gerente de Riesgos y Desarrollo** **• Jefe de Departamento de Riesgos Operacionales** **• Jefe de Departamento de Planeamiento y Organización** **• Comité de Gobierno y Transformación Digital (CGTD)** **• Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT)** **• Gerente de Informática** **• Gerente de Administración y Finanzas** **• Jefe de Departamento de Presupuesto** **• Oficial de Gobierno de Datos** **• Oficial de Datos Personales** **• Propietario de la Información** **• Custodios de la Información** **Las responsabilidades de cada rol se encuentran en el numeral 9, así mismo, las actividades específicas de cada rol se encontrarán en los documentos normativos que designan el rol, directivas y procedimientos.** **8.1.2. Segregación de funciones** **Los propietarios de los procesos deben evaluar las actividades y responsabilidades de cada rol de los colaboradores para asegurar que se encuentran separadas las funciones conflictivas entre diferentes individuos para reducir el riesgo de modificación no autorizada, error, evasión de controles o mal uso de los activos de información de la CPMP.** **8.1.3. Responsabilidades de la dirección** **La Alta Dirección de la CPMP demuestra su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C). Así mismo, establece los mecanismos para respaldar la difusión y actualización, tanto de la presente política como de los demás componentes del SGSI-C.** **8.1.4. Contacto con autoridades**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		El CSIRT y el OSCD son los encargados de la gestión de la "Lista de contactos con autoridades". Esta lista debe ser actualizada de manera periódica con el fin de reportar oportunamente los eventos e incidentes de seguridad de la información. **8.1.5. Contacto con grupos especiales de interés** **El OSCD en coordinación con el DISI, el CSIRT, y los propietarios de los procesos, en caso corresponda es responsable de crear y mantener actualizada una "Lista de contactos con grupos especiales de interés" en los que participan a fin de realizar consultas o recibir alertas tempranas sobre vulnerabilidades relacionadas a seguridad de la información.** **8.1.6. Inteligencia de amenazas** **El CSIRT de la CPMP recopila información de las amenazas provenientes de los eventos de seguridad sobre los activos críticos de la entidad, reportes externos de amenazas y/o comunicaciones del CNSD. El DISI analiza la información recopilada y ejecuta actividades para prevenir que las amenazas reportadas puedan afectar la seguridad de la información de la CPMP.** **El OSCD utiliza la información de amenazas reportadas para mejorar y ajustar el proceso de gestión de riesgos de seguridad de la información, incluyendo la identificación y mitigación de riesgos emergentes.** **8.1.7. Seguridad de la información en la gestión de proyectos** **Las UUOO que tenga bajo su responsabilidad la ejecución de un proyecto, independientemente de su naturaleza (informático o no), deben incluir en la gestión de proyectos la identificación de los requisitos y riesgos de seguridad de la información para que sean tratados.** **Los responsables de los proyectos deben comunicar al OSCD sobre el alcance del proyecto de forma que se cuente con su acompañamiento y en conjunto se definan los requisitos necesarios para preservar la seguridad de la información de los activos de información involucrados.** **8.1.8. Inventario de información y otros activos asociados** **Los responsables de las UUOO, que son propietarios de activos de información, deben mantener el inventario de sus activos de información actualizado de acuerdo con la directiva "Normas y Procedimientos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad".** **8.1.9. Uso aceptable de la información y activos asociados** **a) Todo colaborador y/o tercero debe proteger la información y otros activos asociados asegurándose de evitar la exposición, alteración, eliminación y/o transferencia no autorizada de la información.** **b) Los colaboradores que tengan asignado información y/o activos de TI deben hacer uso de**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		estos en estricto cumplimiento a sus funciones y/o actividades asignadas. **c) Los colaboradores cuentan con carpetas compartidas en red donde deben almacenar sólo información institucional evitando la duplicidad de datos por ser un uso incorrecto del almacenamiento.** **d) Los colaboradores deben proteger los activos de TI y la información albergada o procesada en estos, contra el acceso (físico y lógico) no autorizado, robo, daño, saturación de recursos, consumo excesivo del ancho de banda, exposición de datos personales, u otras situaciones que puedan exponer su confidencialidad, integridad o disponibilidad.** **e) El DISI es responsable de implementar mecanismos técnicos para brindar seguridad a los activos de TI por ello norma su uso a través de la directiva "Normas y Procedimientos para la Administración de Hardware, Software y Servicios Informáticos".** **f) Los activos de TI son parte de patrimonio de la CPMP, por tanto, el DISI en coordinación con la SGL realizan el proceso de asignación formal.** **g) El servicio de correo electrónico se encuentra disponible para los colaboradores como herramienta de apoyo para el cumplimiento de sus funciones y realización de actividades.** **h) El DISI es responsable de brindar el servicio de correo a través de mecanismos seguros y confiables para lo cual implementa controles y filtros que pueden implicar la restricción parcial o total de cuentas de correo que remiten información potencialmente peligrosa. Así mismo, a través de la directiva "Normas y Procedimientos para la Administración de Hardware, Software y Servicios Informáticos", entre otras normas, establece las pautas para su adecuada gestión.** **i) El software cliente de correo electrónico autorizado es el Gmail de Google Workspace. El acceso a cuentas de correo personal debe ser restringido.** **j) Los colaboradores no deben divulgar o publicar información confidencial en sitios web o en servicios de almacenamiento en la nube (Dropbox, Google Drive, etc.) o aplicaciones de mensajería instantánea gratuita (Whatsapp, Telegram u otros). El canal oficial para la comunicación de la información (no considerando información confidencial) es el aplicativo Chat del Google Suite de la CPMP.** **k) Los colaboradores no deben enviar información confidencial de la CPMP por correo electrónico hacia cuentas de terceros y/o gratuitos. Está prohibido el envío de publicidad, correos masivos, suplantación de identidad, correos cadenas, virus, código malicioso, contenido inapropiado u ofensivo, entre otros) y/o que ponga en peligro la información almacenada o transmitida por el servicio de correo, así como su infraestructura, está prohibida y será considerada como un ataque.** **l) Los colaboradores que remitan información a cuentas grupales o listas de correo deben**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		asegurarse de que los destinatarios tienen necesidad de conocer la información a remitir, entendiéndose que esta información es estrictamente laboral. **m) Los colaboradores no deben remitir información de su entorno privado a través de cuentas de correo electrónico de la CPMP, tampoco deben usar su cuenta de correo institucional para suscribirse a boletines, revistas, programas u otros medios de notificaciones de carácter personal.** **n) Los colaboradores y/o UUOO que requieran enviar comunicaciones a todo el personal de la CPMP deberán coordinarlo con el DISI.** **o) Los colaboradores deben hacer uso de firmas (resumen de datos) estandarizadas que lo identifiquen en el intercambio de correos electrónicos. La estructura de la firma seguirá lo normado por la administración.** **p) Los colaboradores son responsables controlar el espacio de almacenamiento en su correo de forma que garantice su disponibilidad contando con opciones de eliminación, copia a carpetas del equipo local, entre otras.** **8.1.10. Devolución de activos** **El personal, al término de su relación laboral con la CPMP, debe:** **a) Poner a disposición de su jefe inmediato (o a quien este designe formalmente), todos los documentos físicos o en formato digital que le fueron entregados o hayan sido generados, como parte del cumplimiento de sus actividades.** **b) En el caso de los equipos informáticos como computadoras, laptop, teléfonos celulares, entre otros que utilizaba para el desempeño de sus funciones, deberá ser gestionado con la Subgerencia de Logística de acuerdo con el procedimiento establecido para tal fin.** **c) Otros activos relacionados con el tratamiento de la información que le fueron entregados, de acuerdo con las disposiciones establecidas.** **También corresponde a los jefes de cada UO tomar las acciones necesarias para asegurar la transferencia del conocimiento del personal que ya no labora.** **8.1.11. Clasificación de la información** **Los propietarios de activos de la información (dueños del proceso) son los responsables de:** **a) Clasificar su información de acuerdo con lo establecido en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública: confidencial y/o pública.** **b) Clasificar toda información producida, transferida o recibida o bajo su control dentro del ámbito de sus responsabilidades, ya sea lógica (información que se genera y que se encuentra almacenada en Internet o medio electrónico como disco duro, USB, CD, DVD, entre otros) o física (información contenida en papel).**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		El DRO debe definir los mecanismos de clasificación de la información e informar el inventario de activos de información a los dueños del proceso. **El OSCD debe verificar los controles, supervisar su correcta implementación y recomendar mejoras de los controles requeridos en concordancia con su clasificación.** **Los responsables de las UUOO deben asegurar que la información sea tratada y protegida a nivel físico y lógico en concordancia con su clasificación.** **Para Información clasificada como Confidencial:** **a) Se debe ubicar en un ambiente que cuente con acceso restringido, registrándose los accesos a estos ambientes.** **b) Su almacenamiento debe ser mínimamente bajo llave (o algún otro mecanismo de seguridad similar) y ser cifrado (con la última versión tecnológica compatible con los sistemas institucionales), según corresponda.** **c) Se debe controlar las copias físicas o electrónicas registrándose, como mínimo, la fecha de la copia y de la persona que lo recibe.** **d) Su comunicación digital se debe dar por canales seguros de transmisión, cifrados con la última tecnología vigente y a direcciones de correos electrónicos institucionales autorizados por el propietario del activo de información.** **Para la difusión o divulgación de la información clasificada como "Confidencial" se requiere el consentimiento previo, informado, expreso e inequívoco del Propietario del activo de información.** **8.1.12. Etiquetado de la información** **Los propietarios de activos de la información son los responsables de etiquetar la información ya sea almacenada en papel o medio electrónico.** **Los responsables de las UUOO deben:** **a) Asegurar que la información sea etiquetada en concordancia con su clasificación.** **b) Para el etiquetado se puede utilizar sellos, etiquetas físicas, encabezados y pies de página, metadatos, marca de agua, entre otros.** **c) Toda información física o digital que es considerada como confidencial, debe ser etiquetada (marcada), siempre y cuando los activos sean de propiedad del CPMP.** **d) La información, documentos o activos que no tienen la clasificación de confidencial o reservado o secreto, no amerita etiquetado.** **e) Se excluye de etiquetar la salida de información de los sistemas de información.** **8.1.13. Transferencia de la información**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		Corresponde al propietario de la información analizar, evaluar y definir el alcance de la transferencia de la información que realizarán con otras entidades para darle los controles de seguridad, al transferir información que no sea de carácter público. Así mismo, asegurar el uso de un acuerdo o cláusula de confidencialidad y no divulgación previa a la transferencia de información que no sea de carácter público ya sea dentro del CPMP o con otra entidad externa. **El DISI debe proteger el intercambio de información por medio electrónico, en concordancia con su clasificación.** **a) Las solicitudes de información por parte de organismos externos deben ser autorizadas por los propietarios de los activos de información y cuando corresponda debe ponerse en conocimiento de la Gerencia General. Los listados de los activos de información son identificados y clasificados por el DRO en conjunto con los propietarios de los activos de información.** **b) Los colaboradores deben evitar tener conversaciones verbales confidenciales en lugares públicos o por medios de comunicación inseguros (mensajes de voz, contestadoras), ya que pueden ser escuchados por personas no autorizados.** **c) La información confidencial contenida en documentos físicos no debe ser transferida fuera de las instalaciones de la CPMP y debe ser almacenada en lugares seguros y/o gabinetes con llave, evitando accesos no autorizados.** **d) La información confidencial contenida en documentos digitales, que requiera ser transferida a entidades externas debe seguir los siguientes lineamientos bajo la supervisión del OSCD:** **• Uso de medios de transmisión seguros haciendo uso de cifrado (por ejemplo: SFTP, HTTPS, entre otros).** **• Mecanismos de autenticación o contraseña.** **• El almacenamiento debe contar con controles de acceso lógico y mecanismos de autenticación o contraseña** **• Checksum para validación de archivos enviados.** **•Temporalidad de la información remitida a través de enlaces temporales.** **• Identificación de receptores de la información.** **e) La transferencia de información por medios informáticos desde o hacia organismos externos se deberá realizar usando mecanismos seguros (SFTP, IPSEC, etc.), bajo el control y supervisión del OSCD.** **f) La publicación de documentos en el portal web institucional (.docx, .xlsx, .pdf, etc.) se realizarán previa eliminación de los metadatos que puedan contener, a cargo del DDMSI.** **g) Toda publicación web que haga referencia a información autorizada de la CPMP debe utilizar los dominios y subdominios de lacaja.com.pe, no se acepta publicaciones que usen direcciones IP directamente.** **h) La UO que cuente con autorización para realizar transferencia de información confidencial y/o datos personales deberá con el DISI que se mantienen**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		registros (logs de auditoría) sobre las operaciones realizadas en los repositorios de información con un periodo de retención de noventa (90) días. **8.1.14. Control de acceso** **Todo acceso otorgado a los sistemas de información, servicios informáticos debe considerar la premisa de mínimo privilegio ("Todo está prohibido a menos que esté expresamente permitido"), los principios de necesidad de saber ("sólo acceso a la información necesaria para sus actividades") y necesidad de uso ("sólo acceso a la infraestructura que requiere para sus actividades").** **a) El acceso a la información, a los recursos y servicios de TI debe ser controlado con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad.** **b) Los propietarios de los activos de información son los responsables de definir las reglas de acceso y restricciones que son requeridas, así como la revisión periódica de los derechos de acceso a los mismos.** **c) El DISI es responsable de normar e implementar los mecanismos técnicos para controlar el acceso lógico a los recursos y servicios de TI, por tanto, no debe existir equipamiento informático y/o software que no cumpla con las condiciones de seguridad exigidos por este.** **d) La GAF debe comunicar al DISI la relación de personal de los entes de supervisión / control que requieren acceso a los sistemas de información con la debida autorización para la auditoría, así también comunicar la culminación de la auditoría para las bajas correspondientes en los accesos.** **e) El acceso a los activos de TI se realiza a través de una cuenta de acceso a red, la misma que es habilitada por el DISI.** **8.1.15. Gestión de identidades** **El DISI, debe considerar en los directivas y procedimientos referido al acceso a los sistemas de información y servicios informáticos lo siguiente:** **a) Solo una identidad específica se pueda asignar a una persona.** **b) En el caso se requiera asignar una identidad a más de una persona (identidades compartidas), esta debe ser justificada y autorizada por el jefe de la UO propietaria del proceso.** **c) De requerirse asignar identidades a entidades no humanas, estás deben ser aprobadas por el Jefe del DISI.** **d) Guardar todos los eventos relacionados al uso y gestión de identidades de usuario.** **El OSCD debe supervisar identidades a entidades humanas y no humanas de manera periódica.** **8.1.16. Información de autenticación**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		El DISI, debe asegurar que el procedimiento, los sistemas de información y servicios informáticos consideren lo siguiente: **a) Todo acceso a recursos y servicios de TI se realiza con una cuenta de usuario que es un identificador único compuesto por un usuarios y contraseña.** **b) El uso de cuentas genéricas solo está permitido para el uso de servicios específicos, previa autorización de la UO responsable y en coordinación con el DISI.** **c) La contraseña está clasificada como información confidencial por lo cual no se debe compartir o mantener anotaciones de esta, ya sea en papeles o archivos digitales.** **d) Los colaboradores o terceros tienen prohibido usar una cuenta de usuario de otra persona o suplantar su identidad.** **e) Las cuentas de usuario serán bloqueadas ante tres (3) intentos de autenticación fallida.** **f) Las contraseñas deben ser robustas para mitigar riesgos de acceso no autorizado, por lo cual debe ser de una longitud mínima de catorce (14) caracteres cumpliendo una combinación de números, símbolos, letras mayúsculas y minúsculas.** **g) Las contraseñas almacenadas deben hacer uso de cifrados robustos. Si la tecnología lo permite, se debe implementar la Autenticación de doble factor (MFA).** **h) Las cuentas de usuario deben permitir que los colaboradores realicen cambio de contraseña con una frecuencia máxima de cuarenta y cinco (45) días, no se podrán reutilizar contraseñas anteriores. El usuario de una nueva cuenta de acceso debe cambiar su contraseña la primera vez que inicie sesión.** **i) El colaborador es responsable de que su contraseña cumpla con la fortaleza o robustez establecida en la presente política.** **j) El DISI, dentro de las características técnicas de las herramientas involucradas, establecerá los mecanismos para el cumplimiento de la fortaleza o robustez de la contraseña, bloqueo de intentos de autenticación fallida, cifrado robusto, tiempo de vigencia, reutilización y cambio de contraseña por defecto.** **k) El restablecimiento de contraseña por olvido debe ser solicitada al DISI que es responsable de realizar la validación de la identificación del solicitante bajo los mecanismos que establezca y asignando una contraseña temporal que cumpla con las características de fortaleza ya definidas.** **l) La entrega de la primera contraseña o clave temporal deben ser brindadas en cumplimiento del procedimiento establecido por el DISI.** **m) Todos los equipos y/o dispositivos conectados a la red de la CPMP (*routers, firewalls, switches*, etc.) deben contar con contraseñas u otro mecanismo superior de control de acceso. El DISI es responsable de la seguridad de la red de la CPMP**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		por tanto norma los procedimientos adecuados para su cumplimiento. **n) Ningún equipo o dispositivo conectado a la red de la CPMP debe mantener contraseñas por defecto u omisión, incluyendo aquellas provistas por fabricantes o proveedores de equipamiento o software.** **8.1.17. Derechos de acceso** **El DISI es responsable, de crear, actualizar y dar de baja a las cuentas de usuario y sus accesos a los sistemas de información y servicios informáticos, previa autorización del responsable de la UO en el que labora el usuario, cualquiera que sea la modalidad de contractual (incluido proveedores y terceros); y del responsable de la UO propietaria del sistema de información y servicio informático.** **Los responsables de las UUOO propietaria de un sistema de información y servicio informático, debe coordinar que el DISI mantenga un inventario actualizado de las identidades y accesos a los sistemas de información y servicios informáticos del cual son propietarios, así como se guarde el registro de la autorización de acceso de los usuarios (activación, modificación o bajas de cuentas de acceso).** **El Departamento de Gestión de Personas o quien haga sus veces, debe comunicar al DISI, la relación de los colaboradores que finalizan su relación laboral, tienen una licencia mayor o igual a tres (3) meses o un desplazamiento de personal, en un plazo máximo de un (01) día hábil de acontecido el evento, a través del procedimiento establecido.** **Para el caso de la baja de las cuentas de acceso a los sistemas de información que utilizaban los colaboradores y/o proveedores o terceros que laboraron o prestaron servicios o tienen una licencia mayor o igual a tres (3) meses, corresponde al jefe de la UO en el que trabajaron, solicitar la baja de las cuentas a la Unidad Orgánica propietaria del sistema de información en un plazo máximo de un (01) día hábil.** **El DISI, debe atender la solicitud de inactivación de las cuentas de acceso a la red de datos y a los servicios tecnológicos de la CPMP que administra en un plazo de un (1) día hábil a partir de la comunicación.** **Así mismo, las cuentas de red, sistemas y correo electrónico deben ser eliminadas hasta cinco (5) días como máximo, posterior al cese del colaborador.** **También, corresponde al responsable de la UO en el que laboró el personal, remover los accesos físicos, por ejemplo: llaves de puertas o de armarios, accesos con lectores biométricos.** **El responsable del sistema de información o quien este designe, debe revisar trimestralmente la gestión de las cuentas de acceso de los usuarios de los sistemas de información. En caso de que haya observaciones, puede realizarlas directamente en los sistemas usados.** **El OSCD debe revisar trimestralmente, a nivel de muestra, las cuentas de acceso a los sistemas de información y servicios informáticos.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		8.1.18. Seguridad de la información en las relaciones con los proveedores **a) Todo contrato de servicio especialmente relacionado a un servicio crítico deberá incluir acuerdos de confidencialidad de la información.** **b) Todo proveedor o contratista se asegurará que su personal designado para formar parte o brindar el servicio conozca y cumpla la presente política.** **c) Todo personal del proveedor o contratista que en prestación de su contrato esté involucrado o en contacto con información, recursos o servicios tecnológicos de la CPMP, debe protegerlos del acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o robo, cumpliendo con los lineamientos de la presente política y con toda aquella normativa que sea aplicable a estos. Asimismo, se deberá aplicar el principio de mínimo privilegio, otorgando solo el acceso necesario y asegurando la revocatoria cuando finalice la relación contractual.** **d) Toda información albergada en la red corporativa, de forma estática o circulando a través de ella mediante elementos de comunicación o transmisión, es propiedad de la CPMP y debe ser tratada como confidencial por todo proveedor o contratista.** **e) Todo personal del proveedor o contratista de servicio con responsabilidades en áreas de operación o administración de sistemas y redes debe:** **• Asegurar que la integridad, autenticación, control de acceso, auditoría y registro se contemplan e incorporan al diseñar, implantar y operar los Sistemas de Información y Redes de Comunicaciones.** **• Asegurar la confidencialidad de la información almacenada, tanto en formato electrónico como físico.** **f) Todo personal del proveedor o contratista que tenga contacto o haya obtenido conocimiento de información de la CPMP debe guardar absoluta confidencialidad, esta obligación permanece vigente aún posterior a la extinción del contrato y por tiempo indefinido.** **g) Toda información (física o digital) que haya sido puesta a disposición del personal del proveedor o contratista es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.** **h) Todo personal del proveedor debe notificar inmediatamente a la CPMP cualquier evento o incidente de seguridad o violación de datos que involucre información de la CPMP a través del correo electrónico, y colaborar en la mitigación y resolución del incidente, en caso sea necesario.** **i) Todo proveedor o contratista que tenga acceso a las instalaciones de la CPMP deberá cumplir con lo especificado en el numeral 8.3.6 "Trabajo en áreas seguras" de la presente directiva. Así mismo,**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		deberán cumplir con otros numerales, según la naturaleza del producto o servicio que brinden a la CPMP, y que sean relevantes y esenciales para asegurar la seguridad de la información de la CPMP. **j) Se deberá efectuar auditorías periódicas para verificar el cumplimiento de los controles de seguridad.** **8.1.19. Abordar la seguridad de la información dentro de los acuerdos de proveedores** **a) El acceso a los activos de información por parte del personal del proveedor o contratista debe ser autorizado por el propietario del activo de información de la CPMP.** **b) Las UUOO solicitantes de servicios o productos suministrados por proveedores o contratistas deben de coordinar con la SGL para que se garantice la inclusión de cláusulas de seguridad de la información en los contratos.** **c) La SGL brinda a los proveedores o contratistas la documentación necesaria relacionada al SGSI-C.** **Se pueden considerar como parte de los requisitos de seguridad en los términos de referencia del servicio lo siguiente:** **a) La incorporación de requerimientos de seguridad de la información (organizativos, legales y técnicos) en las especificaciones técnicas y/o términos de referencia; para ello podrá solicitar el apoyo de la Gerencia de Informática y/o del OSCD de la CPMP.** **b) Establecer en los acuerdos contractuales cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, cláusulas respecto a las leyes de derecho de autor o protección de datos personales; según corresponda. Dichos acuerdos contractuales deben estar vigentes hasta la finalización del contrato; según sea necesario.** **c) Derecho a auditar los procesos y controles del proveedor relacionados con la seguridad de la información dentro del marco del contrato.** **d) Procedimientos para la autorización y revocación de accesos y uso de información de la CPMP y otros activos asociados.** **e) Procedimientos para la notificación y gestión de incidentes de seguridad de la información.** **f) Cumplimiento de las políticas y normas referidas a seguridad de la información de la CPMP por parte del proveedor.** **De haber algún cambio en la provisión de servicios por parte de los proveedores se debe realizar una reevaluación de los riesgos de seguridad de la información con apoyo del DRO, tomando en cuenta la criticidad de la información, sistemas y procesos involucrados.** **8.1.20. Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		El DISI, cuando requieran la contratación de bienes y servicios TIC, debe: **a) Incorporar requerimientos o requisitos de seguridad de la información en los Términos de referencia del bien o servicio.** **b) Solicitar que los proveedores de servicios de tecnología de la información y comunicaciones, que requieran subcontratar a otros proveedores, cumplan los requisitos de seguridad.** **c) Validar que los productos y servicios TIC cumplan con los requisitos de seguridad establecidos, así como la funcionalidad solicitada.** **d) Implementar medidas para garantizar que los componentes de los productos o servicios no son alterados o modificados sin autorización del DISI, por ejemplo: etiquetas anti-manipulación, verificaciones hash criptográficas o firmas digitales.** **e) Gestionar el ciclo de vida de los componentes TIC, incluyendo riesgos de seguridad como la obsolescencia.** **8.1.21. Seguimiento, revisión y gestión del cambio de los servicios de proveedores** **a) La UO usuaria en calidad de supervisor de la ejecución contractual deberá asegurarse que aquellos proveedores o contratistas y/o su personal que brindan servicio dentro de las instalaciones de la CPMP y/o realizan actividades donde se involucre el manejo de información y servicios informáticos, participen en una actividad de sensibilización en seguridad de la información.** **b) La UO usuaria en su calidad de supervisor de la ejecución contractual deberá revisar de forma trimestral la relación de sus proveedores o contratistas con acceso remoto y con acceso a los sistemas de información de la CPMP y validar su correspondencia ante el DISI.** **c) La UO usuaria en su calidad de supervisor de la ejecución contractual será la encargada de monitorear y revisar el cumplimiento de los servicios o productos brindados por el proveedor o contratista, en coordinación con la SGL.** **8.1.22. Seguridad de la información en el uso de servicios en la nube** **a) Todo colaborador y tercero que requiera el uso de servicios en la nube en el ámbito del cumplimiento de sus funciones o actividades debe contar con la autorización del responsable de la UO a la que pertenece o brinda servicio.** **b) El responsable de la UO que autoriza el uso de servicios en la nube lo realiza en base a los servicios en la nube autorizados por el DISI.** **c) El DISI establece los requisitos para los servicios en la nube contratados por la CPMP y las responsabilidades del proveedor de servicios en la nube, garantizando que cumplan con los controles de seguridad y la normativa establecida por la Secretaria de Gobierno y Transformación Digital[1] (SGTD) u otro ente rector para el sector público.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		d) Todo colaborador o tercero que cuente con autorización para gestionar el acceso a información institucional en un servicio en la nube es responsable de aplicar el principio de menor privilegio, otorgando solo los permisos necesarios a cada usuario para desempeñar sus funciones o actividades. **e) La CPMP se reserva el derecho de realizar auditorías (con auditores internos o externos) o revisiones a sus proveedores de servicios en la nube para verificar el cumplimiento continuo y garantizar que los estándares de seguridad se mantengan alineados con las últimas regulaciones y mejores prácticas, la eficacia de los procesos de gestión de riesgos y la preparación para incidentes de segundad.** **f) Los proveedores de servicio en la nube son responsables como mínimo de:** **• Implementar mecanismos de autenticación como múltiple factor de autenticación (MFA) o alternativas robustas de seguridad para asegurar que solo usuarios autorizados accedan a los recursos en la nube.** **• Utilizar algoritmos de cifrado fuertes como (*Advanced Encryption Standard*), o superiores, para garantizar la seguridad de los datos almacenados y transmitidos.** **• Implementar técnicas de borrado seguro de información garantizando la eliminación completa y segura de los datos de la CPMP de sus sistemas en la nube al finalizar el contrato de servicio o en caso de una solicitud específica.** **• Implementar políticas de respaldo y recuperación robustas considerando los lineamientos brindados por el DISI con la finalidad de garantizar la disponibilidad y la integridad de los datos y utilizando métodos de cifrado para proteger la información confidencial durante el proceso de respaldo.** **• Cumplir la Política de Seguridad de la Información de la CPMP y demás documentos normativos de la institución que les aplique. La CPMP deberá solicitar al proveedor una declaración de aplicabilidad de las medidas, certificaciones o acreditaciones en materia de seguridad de la información.** **• Cumplir con las medidas de seguridad aplicables para las entidades del Estado, como la NTP ISO/IEC 27001 (en su versión vigente) y las disposiciones señaladas en la Directiva de Seguridad emitida por la ANPDP del Ministerio de Justicia (cuando corresponda).** **8.1.23. Planificación y preparación de la gestión de incidentes de seguridad de la información** **Se deben establecer los procedimientos y responsabilidades para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. Este procedimiento debe considerar:** **a) El monitoreo y reporte de los eventos de seguridad de la información para decidir si son**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		clasificados como incidentes de seguridad de la información en conjunto con el DRO. **b) Clasificar, priorizar y analizar los incidentes de seguridad de la información, determinando mínimamente su causa raíz, impacto, probabilidad de ocurrencia, la solución a la causa raíz, responsable de la atención y el periodo de implementación de la solución.** **c) Seguimiento de la atención de los incidentes hasta su conclusión, incluyendo el escalamiento requerido y la comunicación a las partes interesadas.** **d) Informar al OSCD todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata.** **e) Informar al OSCD las debilidades y eventos de seguridad de la información que podrían comprometer la continuidad de los servicios informáticos de la CPMP.** **f) Identificación y registro de las lecciones aprendidas y mejoras a los controles de seguridad de la información.** **8.1.24. Evaluación y decisión sobre eventos de seguridad de la información** **Los trabajadores deben reportar los eventos y/o debilidades de seguridad de la información relacionada a los servicios informáticos al DRO, de acuerdo con los procedimientos establecidos.** **Dicho Departamento debe dar tratamiento a los eventos y/o debilidades de seguridad de la información reportadas, asimismo, evaluar, clasificar, priorizar el evento y determinar si es un incidente; en caso afirmativo deberá comunicar al OSCD y/o al CSIRT de acuerdo a los procedimientos establecidos.** **8.1.25. Respuesta a incidentes de seguridad de la información** **El DRO, debe comunicar los procedimientos establecidos para el reporte y la atención de los incidentes de seguridad de la información en forma rápida, efectiva y ordenada. Las UUOO en el marco de su competencia, deben dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos elaborados y establecidos por el DRO.** **8.1.26. Aprendizaje de los incidentes de seguridad de la información** **Corresponde al DRO, en coordinación con el OSCD, considerar en el procedimiento de gestión de incidentes de seguridad de la información la cuantificación de los tipos, volúmenes y costos de los incidentes de seguridad de la información que permita:** **a) Mejorar los protocolos de atención de los incidentes.** **b) Identificar incidentes recurrentes o graves y sus causas para analizarlos e incluirlos en la evaluación de riesgos de seguridad de la información y así**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		reducir la probabilidad o las consecuencias de futuros incidentes similares. **c) Mejorar los programas o planes de concienciación en seguridad de la información del usuario.** **El OSCD, debe:** **a) Comunicar al CSIRT los incidentes de seguridad digital que le fueron reportados.** **b) Comunicar al Responsable del Tratamiento los incidentes de seguridad de la información relacionados a bancos de datos personales a fin de que, de considerarlo, pueda comunicarlo a la ANPDP.** **c) Revisar trimestralmente el proceso de gestión de incidentes del DRO.** **El OSCD en calidad de coordinador del CSIRT, debe comunicar al CNSD los incidentes identificados a través de los medios que indique la Secretaría de Gobierno y Transformación Digital y la ANPD.** **8.1.27. Recolección de evidencia** **El DISI deberá definir un procedimiento para la identificación, recolección y conservación de la información que puede servir como evidencia para propósitos de acción disciplinaria y legal. La evidencia corresponde a logs de auditoría de accesos a los sistemas y recursos tecnológicos de la CPMP. En general, las evidencias deben recopilarse de una manera que sea admisible.** **8.1.28. Seguridad de la información durante la interrupción** **En situaciones adversas, la CPMP establece los siguientes lineamientos de seguridad de la información y de continuidad para la gestión de seguridad de la información:** **a) Mantener el uso de credenciales de acceso a los sistemas de información de acuerdo con los lineamientos establecidos en el numeral 8.1.16 "Información de autenticación" de la presente política.** **b) Mantener activados los logs de auditoría, en cumplimiento de lo establecido en el numeral 8.4.15 "Registro" de la presente política.** **c) El acceso a las copias de respaldo solo está permitido al DISI.** **d) Mantener la configuración de copias de respaldo de archivos y bases de datos.** **e) Verificar que la documentación (física o digital) con clasificación confidencialidad esté protegida durante los traslados o restauración, incluyendo copias de respaldo.** **f) Mantener la misma configuración de los perfiles y usuarios de las aplicaciones en el ambiente de contingencia.** **g) En caso de verse afectados equipos de usuario final y estos requieran ser reemplazados, se debe mantener la configuración base.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		h) Los planes de continuidad del negocio deben reflejar los principios y directrices definidos en la directiva "Políticas y Objetivos de Continuidad del Negocio" y en la directiva "Normas y Procedimientos del Sistema de Gestión de Continuidad del Negocio (SGCN)", tales como: Priorización de procesos críticos, Tiempos máximos aceptables de interrupción, Niveles de pérdida de datos tolerables, Cumplimiento de requisitos legales, regulatorios y contractuales. **8.1.29. Preparación para las TICs para la continuidad del negocio** **a) El DISI establece un Plan de Contingencia Informático detallado en el Plan de Continuidad de Servicios Informáticos, que describe las acciones a realizar ante escenarios adversos definidos.** **b) La CPMP cuenta con un CSIRT ante incidentes de seguridad digital y es responsable de la gestión de incidentes de seguridad digital que afectan los activos de información.** **c) La CPMP cuenta con un Grupo de Comando que es el órgano técnico interdisciplinario responsable de la planificación, coordinación y ejecución de las acciones operativas orientadas a garantizar la continuidad operativa y la resiliencia institucional.** **8.1.30. Requisitos legales, estatutarios, regulatorios y contractuales** **Las UUOO de la CPMP deben:** **a) Identificar todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes.** **b) Implementar procedimientos para asegurar el cumplimiento de lo señalado en las normas legales, estatutarias, regulatorias o documentos contractuales relacionados con el tratamiento de la información, derechos de propiedad intelectual y uso de producto de software propietario.** **Corresponde al DISI implementar los controles de seguridad respecto al de enmascaramiento o criptográficos o de enmascaramiento criptografía, en cumplimiento con todos los acuerdos, legislación y regulación vigente.** **El OSCD, debe verificar la implementación de los controles para recomendar mejoras. Para el caso de los controles de seguridad en los bancos de datos personales de la CPMP debe coordinar con el ODP y Responsable del Tratamiento.** **8.1.31. Derechos de propiedad intelectual** **a) La CPMP es titular legítima de los activos de propiedad intelectual utilizados, y su uso está restringido a fines autorizados.** **b) La CPMP establecerá a través de acuerdos de confidencialidad la protección de los derechos de propiedad intelectual.** **c) La CPMP reconoce como activo de propiedad intelectual al software y código fuente desarrollado internamente, patentes, diseños industriales,**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		documentación técnica, manuales y materiales formativos, know-how corporativo, en tal sentido, el DISI deberá: **• Catalogar los recursos sujetos a derecho de propiedad intelectual (código fuente, patentes, marcas, secretos comerciales, etc.).** **• Implementar mecanismos de autenticación y autorización para limitar el acceso a la propiedad intelectual.** **d) La Gerencia de Informática es la unidad responsable de asumir las siguientes funciones vinculadas al software empleado por la CPMP:** **• Mantener un registro actualizado de todas las licencias de software utilizadas en la entidad, junto con la documentación que acredite su correcta adquisición.** **• Ejecutar revisiones periódicas para confirmar que únicamente se haya instalado software autorizado y debidamente licenciado.** **• Gestionar la inscripción y/o registro, ante Indecopi y a nombre de la CPMP, del software desarrollado incluyendo aquel creado por terceros para la institución en el registro de propiedad intelectual correspondiente.** **8.1.32. Protección de registros** **Las UUOO de la CPMP deben proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, por lo tanto, deben incorporar en los lineamientos y procedimientos de operativos o de tratamiento de información, las normas a seguir para el almacenamiento, custodia y eliminación de los registros de acuerdo con el esquema de clasificación.** **8.1.33. Privacidad y protección de la información de identificación personal (IIP)** **En estricto cumplimiento del marco normativo de protección de datos personales, la CPMP gestiona la información bajo los principios de confidencialidad, integridad y disponibilidad. Dicho tratamiento se limita estrictamente a las finalidades declaradas en la "Política de Privacidad y Protección de Datos Personales", asegurando la máxima protección de los derechos de sus titulares.** **En tal sentido, las unidades orgánicas de la CPMP deben:** **a) Designar a un responsable por cada banco de datos personales, así como un responsable del tratamiento de estos.** **b) Garantizar el ejercicio de los derechos ARCO de los datos personales, a través del enlace en su página web – https://www.lacaja.com.pe/arco.** **c) Promover la toma de conciencia del personal responsable sobre la protección de los datos personales.** **d) Cumplir con los requisitos legales, normativos y regulatorios aplicables.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		e) Fomentar la mejora continua sobre las medidas adoptadas en protección de los datos personales a fin de minimizar los riesgos e incidentes de seguridad relacionados a los datos personales. **f) Establecer la necesidad de evaluaciones de impacto de privacidad (DPIA/PIA) para nuevos tratamientos de datos personales o cambios significativos en los existentes.** **g) Identificar y documentar los bancos de datos personales que existan dentro de su ámbito de responsabilidad, y proceder a registrarlos ante la ANPD conforme a la normativa vigente.** **h) Establecer mediante cláusulas contractuales u otros instrumentos jurídicos aplicables, la obligación de que los terceros cumplan con las disposiciones legales y regulatorias sobre el tratamiento de datos personales a los que pudieran acceder durante la prestación de sus servicios.** **El DISI debe implementar los controles de seguridad de la información para la protección de los bancos de datos localizados en el Centro de Datos. El OSCD, en coordinación con el ODP y el Responsable del Tratamiento, debe verificar los controles, supervisar la correcta implementación, recomendar mejoras de los controles requeridos para la seguridad y gestión de los bancos de datos de la CPMP.** **8.1.34. Revisión independiente de la seguridad de la información** **El OSCD, debe:** **a) Elaborar y proponer al Comité de Gobierno y Transformación Digital para su aprobación, el programa de auditoría interna o externa al menos una vez por año, de los procesos que forman parte del alcance del SGSI.** **b) Coordinar la ejecución de las auditorías internas o externas por personas independientes a los procesos o UUOO a revisar.** **c) Realizar revisiones de la seguridad de la información al menos una vez al año, a los controles de seguridad de la información implementadas en el DISI.** **d) La revisión incluye los procesos relacionados con el procesamiento de la información, como son desarrollo de software, base de datos, redes, entre otros y debe realizarse tomando como criterios los controles del Anexo A de la NTP ISO/IEC 27001:2022 NTP Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.** **e) Informar al Comité de Gobierno y Transformación Digital los resultados de las revisiones y auditorías.** **El Comité de Gobierno y Transformación Digital, debe revisar los informes de los resultados de la auditoría interna, externa o de las revisiones realizadas o coordinadas por el OSCD.** **8.1.35. Cumplimiento con políticas, reglas y normas de seguridad de la información**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		Los jefes de las UUOO de la CPMP deben asegurar que el personal y los terceros dentro de la UO que lideran, cumplen la política de la seguridad de la información. De existir incumplimientos, deben reportarlo, analizar las causas, implementar las acciones correctivas y verificar la efectividad de las acciones tomadas. **El OSCD debe:** **a) Revisar las políticas, directivas y procedimientos de seguridad de la información al menos una vez al año o cuando existan cambios en las normas o procesos de la institución.** **b) Revisar, a nivel de muestra, que el personal y los terceros cumplan la política de la seguridad de la información al menos una vez al año.** **8.1.36. Procedimientos operativos documentados** **El DISI debe elaborar procedimientos documentados como mínimo para las actividades operativas que represente un riesgo de no realizarse de manera correcta. Estos procedimientos deben:** **a) Establecer las actividades y responsabilidades para la gestión y operación de los medios de procesamiento y almacenamiento de la información, por ejemplo: monitoreo de la capacidad y desempeño de los recursos informáticos, instalación y configuración de los sistemas, entre otros.** **b) Asegurar la segregación de funciones en la operación para reducir el riesgo de un mal uso.** **Corresponde al DISI, registrar, controlar e identificar el impacto de los cambios que se realicen en los procesos de tecnología de la información y comunicaciones y las instalaciones de procesamiento de la información que afecten la seguridad de la información.** **8.2. Controles de Personal** **8.2.1. Selección** **El Departamento de Gestión de Personas, debe comprobar los antecedentes del personal que ingresa a laborar en la CPMP, de acuerdo con las leyes y regulaciones vigentes, independientemente de su modalidad de contratación.** **8.2.2. Términos y condiciones del empleo** **El Departamento de Gestión de Personas, debe:** **a) Establecer en los acuerdos contractuales de empleo, cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, cumplimiento a la política de seguridad de la información y documentos normativos institucionales, cláusulas respecto a las leyes de derecho de autor o protección de datos personales; según corresponda. Dichos acuerdos contractuales deben estar vigentes hasta la finalización del contrato; según sea necesario.** **b) Comunicar que el incumplimiento de la Política de Seguridad de la información podrá ser objeto de**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		sanción administrativa disciplinaria, previo procedimiento administrativo disciplinario. **El personal debe:** **a) Cumplir con lo dispuesto en las Políticas de Seguridad de la Información; así como con toda normativa relacionada con la seguridad de la información emitida por la CPMP.** **b) Informar las vulnerabilidades detectadas y violaciones de seguridad de la información al OSCD de la CPMP.** **8.2.3. Toma de conciencia, educación y entrenamiento sobre la seguridad de la información** **a) El nuevo colaborador de la CPMP participa del proceso de inducción organizado por el Departamento de Recursos Humanos, con la participación del OSCD o quién él delegue.** **b) Todos los colaboradores deben asistir a las charlas, entrenamientos o capacitaciones en Seguridad de la Información, así como cumplir con las políticas de seguridad de la información y ciberseguridad.** **c) Todos los colaboradores deben atender las recomendaciones de seguridad de la información que son remitidas a través de los medios de comunicación institucionales.** **8.2.4. Proceso disciplinario** **a) La CPMP cuenta con un Reglamento Interno de Trabajo (RIT) que norma las relaciones y condiciones laborales de los servidores de la CPMP, durante el desempeño de sus funciones, conforme a las normas legales.** **b) Todo colaborador debe aplicar el RIT, teniendo en cuenta, que, para el SGSI-C, es fundamental el cumplimiento del art. 42º del RIT referidas a la seguridad de la información.** **c) El Departamento de Recursos Humanos debe difundir que el incumplimiento de la Política del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, podrá ser objeto de sanción administrativa disciplinaria, previo procedimiento administrativo disciplinario; como también los medios de presentación de la denuncia para reportar tal incumplimiento.** **8.2.5. Responsabilidades después del cese o cambio de empleo** **a) Todos los colaboradores antes de su desvinculación realizan la entrega de cargo incluyendo la información contenida en la cuenta de correo electrónico institucional, ello conforme a lo dispuesto en la directiva "Normas para la entrega de cargos del personal".** **b) El Departamento de Recursos Humanos debe comunicar al DISI y la GAF sobre las rotaciones, licencias mayores o iguales a tres (3) meses, y ceses que se produzcan en la CPMP, hasta con tres (3) días de anticipación, de forma que el DISI y la GAF tomen las medidas de control sobre la revocación de accesos a las instalaciones físicas, recursos y**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		servicios informáticos. Los procedimientos relacionados se encuentran normados en la directiva "Normas y Procedimientos para la Administración de Accesos a los Servicios Informáticos". **c) Las cuentas de usuario de colaboradores con licencia mayor o igual a tres (3) meses serán deshabilitadas salvo autorización expresa del responsable de la UO. En los casos de cese, las cuentas serán inicialmente deshabilitadas por quince (15) días, posterior a ello el buzón del correo será eliminado de los servidores. El DISI mantiene el respaldo de la información histórica de acuerdo con la directiva "Plan de Seguridad Informática Institucional".** **d) Todos los colaboradores están sujetos a cláusulas de confidencialidad, las cuales se mantienen vigentes aun cuando haya finalizado el vínculo laboral con la CPMP.** **8.2.6. Acuerdos de confidencialidad o no divulgación** **Corresponde a los jefes de las UUOO identificar a los colaboradores que acceden a información confidencial, reservada o secreta para supervisar la aplicación de los controles de seguridad en el tratamiento de la información a la que acceden, entre ellos, la firma de un acuerdo de confidencialidad.** **8.2.7. Teletrabajo** **El colaborador que preste labores de teletrabajo o requiera acceso remoto debe cumplir con la presente política, la Directiva de Gerencia General "Normas y procedimientos para la aplicación del Teletrabajo", y cualquier otra normativa interna relacionada a seguridad de la información, protección de datos personales y confidencialidad de la información.** **El colaborador que cuente con acceso remoto ya sea por teletrabajo o porque ha sido autorizado para su uso, debe proteger la información a la que tiene acceso de amenazas como el acceso no autorizado, alteración indebida o software malicioso cumpliendo con lo siguiente:** **a) Asegurarse que en el sitio donde realizarán el teletrabajo sea un ambiente en donde se reduzca la probabilidad de accesos no autorizados a información o recursos.** **b) Utilizar redes privadas para el acceso a internet.** **c) Verificar que el Sistema Operativo y el antivirus o antimalware del equipo con el que trabaja, cuente con las últimas actualizaciones.** **d) Verificar que los equipos asignados cuenten con bloqueo automático por inactividad. No utilizar otra herramienta de comunicación o de videoconferencia a la establecida por la CPMP.** **e) Guardar confidencialidad de la información proporcionada por la CPMP para la prestación de las labores.** **El DISI es el responsable de habilitar el acceso remoto a la red de datos de la CPMP a través de un**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		software VPN previa autorización del jefe de la UO y del jefe de Recursos Humanos. También debe implementar las medidas necesarias para: **a) Capacitar y concientizar a los usuarios sobre las medidas de seguridad y confianza digital que deben tener para la protección de la información a la que acceden, como la protección de sus credenciales de acceso a los recursos de información y los cuidados en los equipos de cómputo asignados.** **b) Verificar que los equipos de teletrabajo tengan instalado el software VPN, el software antivirus o antimalware, el firewall activado y el sistema operativo actualizado.** **Se encuentra prohibido cualquier otro mecanismo técnico de acceso remoto no autorizado que permita el acceso desde redes externas a la red de la CPMP o viceversa.** **8.2.8. Reporte de eventos de seguridad de la información** **a) Todos los colaboradores tienen la responsabilidad de reportar incidentes, eventos y/o debilidades de seguridad de la información que se identifican o se genere duda al respecto.** **b) Los colaboradores que reciban un correo electrónico con contenido malicioso, fraudulento o donde se alerte situaciones que comprometan la seguridad de la información deberá remitir el mensaje a través de un correo electrónico al DISI con la finalidad de que se brinde el tratamiento adecuado, así como evitar su difusión o reenvío a otros destinatarios.** **8.3. Controles físicos** **8.3.1. Perímetros de seguridad física** **El Departamento de Servicios Inmobiliarios debe supervisar que el servicio de vigilancia privada brinde la seguridad de forma permanente, al interior y en el sector perimétrico de las sedes de la CPMP a fin de prevenir actos ilícitos o incidentes que puedan generar riesgos contra la integridad de los colaboradores, usuarios y patrimonio de la CPMP.** **8.3.2. Ingreso Físico** **a) Toda persona que ingrese a las instalaciones de la CPMP debe identificarse y ser registrado tanto en el ingreso como en la salida. Los colaboradores y los terceros deben usar en todo momento su *fotocheck* o el identificador que se les haya sido asignado, portándolo en un lugar visible.** **b) El DISI es el responsable de normar e implementar los mecanismos técnicos para asegurar el control del acceso físico a las instalaciones y a través de su Especialista en Seguridad de Información, o quien haga sus veces, establece los procedimientos necesarios para cumplir con tal fin.** **c) El personal de seguridad debe asegurarse que se registre los dispositivos del tipo *tablet* o *laptop* y los dispositivos de almacenamiento externo como discos duros portátiles que ingresen o salgan de las instalaciones de la CPMP.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		d) El acceso al Centro de Datos está permitido sólo al personal técnico autorizado del DISI. El ingreso y salida es previa identificación biométrica. **e) Los terceros que requieran ingresar al Centro de Datos deben contar con autorización del responsable del Centro de Datos.** **8.3.3. Asegurar oficinas, salas e instalaciones** **El Departamento de Servicios Inmobiliarios debe dar cumplimiento a la Directiva de Normas Internas y Procedimientos de Seguridad de la CPMP vigente con la finalidad de garantizar la seguridad de los colaboradores, usuarios y los bienes patrimoniales de la CPMP. El personal de la CPMP, proveedores y el personal de terceros autorizados, deben portar siempre su identificación (*fotocheck* o pase especial) en un lugar visible al permanecer en las instalaciones de la CPMP, incluyendo en el Centro de Datos. Corresponde a los responsables de las UUOO verificar que las personas dentro de las instalaciones bajo su responsabilidad cumplan con portar su identificación.** **8.3.4. Supervisión de la seguridad física** **El Departamento de Servicios Inmobiliarios es responsable del monitoreo de la segundad seguridad física de las instalaciones de la CPMP. Para este fin, cuenta con personal de vigilancia, sistemas de videovigilancia, panel de control de alarmas, entre otros.** **Las directrices de monitorización de seguridad física se establecen en la Directiva Nº 01-2020-JUS/DGTAIPD - Tratamiento de Datos Personales mediante sistemas de videovigilancia.** **8.3.5. Protección contra amenazas físicas y ambientales** **Las instalaciones de la CPMP cuentan con extintores operativos y cargados, sistema de alarma contra incendios y rutas de salida y zonas seguras señalizadas.** **El Departamento de Servicios Inmobiliarios, así como las UUOO responsables de las instalaciones de procesamiento y/o almacenamiento de información, deben tomar las acciones para:** **a) Realizar evaluaciones de riesgo a las instalaciones de procesamiento y/o almacenamiento de información que permita identificar las amenazas físicas y ambientales a las que están expuestas, por ejemplo, incendio, inundación, disturbios civiles, entre otras, según lo establecido en el Plan de Continuidad Operativa de la CPMP.** **b) Implementar los controles adecuados para el tratamiento de los riesgos identificados e informar al DRO para la actualización del Plan de Continuidad Operativa o situaciones no contempladas en el mismo.** **c) Realizar pruebas periódicas y/o revisiones a los controles ambientales implementados como**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		sensores de humedad, detectores de humo, entre otros. **8.3.6. Trabajo en áreas seguras** **a) Las oficinas o instalaciones donde se almacene o procese información confidencial (Centro de Datos, Archivo, entre otras) son instalaciones críticas por lo cual deben contar con acceso restringido y deben ser monitoreadas con cámaras de videovigilancia. El ingreso y salida de los colaboradores autorizados debe ser registrado por las UUOO responsables de dichos ambientes y, de ser el caso, emplear mecanismos biométricos.** **b) Todo tercero que ingrese al Centro de Datos debe estar acompañado por un personal técnico autorizado del DISI quién supervisará los trabajos o actividades a realizar.** **c) Todo equipamiento que sea instalado debe ser inspeccionado antes de la entrega a fin de determinar si su contenido representa un peligro para la seguridad del Centro de Datos, de igual manera, esta tarea será supervisada por un personal técnico autorizado del DISI.** **d) No se encuentra permitido tomar fotografías o filmar dentro de los ambientes donde se almacene o procese información confidencial, como los archivos de las UUOO, el Archivo Central y el Centro de Datos.** **e) Las oficinas o instalaciones que contengan equipos de comunicaciones (*switches,* PBX*, routers, firewalls*) y consolas de administración, deben contar con acceso restringido y monitoreado con cámaras de videovigilancia.** **8.3.7. Escritorio y pantalla limpios** **a) Los colaboradores deben bloquear su equipo de cómputo cuando se ausenten de su puesto de trabajo, así como guardar en un sitio seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial. Si los colaboradores están ubicados cerca de zonas de atención al público, deben guardar también los documentos y medios que contengan información de uso interno.** **b) AI finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.** **c) Los colaboradores que usen las impresoras deberán retirar los documentos inmediatamente después de su impresión.** **d) El colaborador debe mantener su escritorio virtual con la menor cantidad de archivos o accesos directos debido a que estos generan degradación del performance de los equipos de usuario.** **8.3.8. Ubicación y protección de los equipos** **El DISI, debe implementar controles que permitan:** **a) Evitar la apertura de los equipos informáticos. Solo el personal de soporte técnico del DISI podría hacerlo en caso corresponda.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		b) La apertura de equipos debe estar controlada con etiquetas o algún tipo de hardware de seguridad. **Para el caso de los equipos ubicados en el Centro de Datos de la CPMP, corresponde al DISI monitorear las condiciones ambientales como la temperatura y humedad que puedan afectar el funcionamiento de los equipos.** **8.3.9. Seguridad de los activos fuera de las instalaciones** **a) Los colaboradores que requieran retirar activos de TI de las instalaciones de la CPMP deberán solicitarlo a la SGL (Control Patrimonial), según los formatos establecidos y contar con la autorización previa del responsable de la UO correspondiente.** **b) El colaborador que haya sido autorizado para retirar los activos de TI debe hacer sellar el formato patrimonial por personal de vigilancia cada vez que se retire y/o ingrese.** **c) El personal de vigilancia debe verificar el activo de TI antes de su retiro y/o ingreso a las instalaciones de la CPMP.** **d) La SGL coordinará con el DISI para garantizar que los equipos de cómputo que serán entregados a los colaboradores en calidad de préstamo y retirados de las instalaciones de la CPMP, tengan los puertos bloqueados para el uso de medios removibles. Estos puertos sólo se habilitarán cuando exista la necesidad y se cuente con la autorización del responsable de la UO.** **e) Todo colaborador que tenga asignado un equipo de cómputo para su uso fuera de las instalaciones es responsable de su resguardo, evitando dejarlo sin vigilancia y exponerlo a ambientes con condiciones extremas (temperatura, humedad, polvo).** **8.3.10. Medios de almacenamiento** **a) El DISI es responsable de establecer los requisitos técnicos y de seguridad para la adquisición de medios removibles.** **b) Todo colaborador que, para el cumplimiento de sus funciones, requiera conectar un medio removible a un equipo de cómputo de la CPMP deberá asegurarse que sea analizado previamente por el software antimalware/antivirus.** **c) El colaborador que tenga asignado un medio removible debe resguardarlo y evitar el acceso no autorizado o uso indebido.** **d) El colaborador que haga uso de un medio removible debe evitar dejarlo conectado a equipos desatendidos.** **e) La movilización y salida de medios removibles que contengan información confidencial, fuera de las oficinas de la CPMP se encuentra prohibida, salvo con autorización expresa del Gerente de Informática o en su defecto del DISI. Esta prohibición no incluye el traslado de las cintas de respaldo hacia su lugar de custodia gestionado por el DISI.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		f) Los medios removibles que requieran ser dados de baja, deberán pasar por un proceso de borrado seguro. **g) El DISI es responsable de implementar el procedimiento de borrado seguro y destrucción de los medios removibles (en caso corresponda), antes que se realice la baja o reutilización de este.** **8.3.11. Servicios de suministro de apoyo** **El Departamento de Servicios Inmobiliarios, dentro del marco de sus competencias y en coordinación con el DISI, debe:** **a) Programar los mantenimientos de los equipos de respaldo de energía eléctrica (como grupo electrógeno y UPS) para asegurar el funcionamiento de los componentes del centro de datos, ante la pérdida del servicio de suministro eléctrico.** **b) Asegurarse que los equipos de respaldo de energía eléctrica se inspeccionen y prueben periódicamente para garantizar su correcto funcionamiento.** **El DISI debe solicitar disponer de un servicio de conexión a Internet de contingencia que permita la operatividad de los servicios informáticos de la CPMP ante la interrupción del servicio de conexión principal.** **8.3.12. Seguridad del cableado** **El DISI debe implementar controles que permitan asegurar que los cables que transportan datos se encuentren debidamente protegidos contra la interceptación interferencia o posibles daños.** **8.3.13. Mantenimiento de equipos** **El DISI debe:** **a) Programar y realizar en forma periódica mantenimientos preventivos de los equipos informáticos de los colaboradores de la institución de acuerdo con las recomendaciones del fabricante.** **b) Asegurar que se efectúe el mantenimiento de los equipos informáticos que conforman la infraestructura de tecnología del Centro de Datos de la CPMP como son equipos de servidores, UPS, sistema de aire acondicionado de precisión, entre otros.** **8.3.14. Eliminación segura o reutilización de equipos** **El DISI debe:** **a) Asegurar que, la información clasificada como no pública, almacenada en los medios de almacenamiento que van a ser reutilizados, reemplazados o puestos a disposición (baja), sea borrada de manera segura; así como también en el caso que contengan software propietario.** **b) De acuerdo a una evaluación de riesgos de acceso a información no pública, determinar si los medios de almacenamiento deberían destruirse físicamente.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		Corresponde a la Subgerencia de Logística, retirar las etiquetas y marcas que identifican a la CPMP de los equipos o medios de almacenamiento antes de ser puestos a disposición para donación o eliminación. **Corresponde los responsables de las UUOO que, en el caso que se requiera eliminar documentos físicos que ya no se utilicen, estos deben ser destruidos, por ejemplo, triturados, para evitar que puedan ser reconstruidos. Para la eliminación de grandes volúmenes de información física, se debe utilizar proveedores certificados y aprobados de servicios de eliminación segura.** **8.4. Controles Tecnológicos** **8.4.1 Dispositivos terminales del usuario** **a) Todo colaborador o tercero que ingrese o retire dispositivos móviles del tipo Tablet o laptop y los dispositivos de almacenamiento externo como discos duros portátiles, de las instalaciones de la CPMP, debe coordinar su registro con el personal de seguridad de la entidad.** **b) Todo colaborador o tercero debe configurar mecanismos de autenticación como PIN, clave, patrón, etc. En los dispositivos móviles bajo su responsabilidad, asignados por la CPMP o de su propiedad, que almacenen o guarden información de la CPMP.** **c) Los colaboradores que hagan uso de dispositivos móviles de propiedad de la CPMP podrán conectarlos a internet a través de medios autorizados como plan de datos, red cableada, modem inalámbrico o la red inalámbrica privada del colaborador, quedando prohibido el acceso a traces de redes inalámbricas públicas como parques, cafeterías, aeropuertos, etc.** **d) EL colaborador que tenga asignado un dispositivo móvil de la CPMP debe evitar dejarlo en cajones sin seguro, lugares de reunión, autos o ambientes sin supervisión, manteniéndolo en lugares que ofrezcan seguridad.** **e) El colaborador que tenga asignado un dispositivo móvil de la CPMP debe ser responsable de su cuidado general, debiendo reportar al DSI cualquier tipo de siniestro.** **f) Se encuentra prohibido descargar, guardar o almacenar información clasificadas como confidencial en dispositivos móviles personales.** **Corresponde al OSCD:** **a) Dar a conocer las políticas y procedimientos de seguridad establecidos en la CPMP, así como las responsabilidades de los usuarios en seguridad de la información.** **b) Concientizar a los usuarios sobre las amenazas más comunes a la seguridad de la información.** **8.4.2. Derechos de acceso privilegiados** **a) Las cuentas de usuarios del tipo administrador, súper administrador y/o administradores del**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		dominio son de uso exclusivo del DISI y deben ser usados solo para labores de mantenimiento, configuración y/o soporte de la plataforma tecnológica institucional. **b) Las cuentas de administración local deberán ser desactivadas por defecto para los equipos de cómputo de usuario final.** **c) Los colaboradores o terceros que gestionen bases de datos con información confidencial y/o datos personales deben contar con controles que prevengan la pérdida de confidencialidad de la información como una adecuada gestión de accesos, controles en el equipo de usuario, controles de red, entre otros.** **d) El OSCD debe supervisar el cumplimiento de asignación de acceso privilegiados, así como realizar una revisión trimestral de las cuentas con privilegios administrativos en los sistemas de información.** **8.4.3. Restricción de acceso a la información** **El DISI debe asegurar que se implementen los controles de acceso a la información como:** **a) Accesos a los sistemas de información y servicios informáticos de la CPMP mediante mecanismos de autenticación.** **b) No permitir el acceso a información sensible mediante los sistemas de información o servicios a identidades de usuario desconocidas o de forma anónima.** **c) Permitir la restricción de accesos a los datos o información, así como a las acciones que puede realizar sobre ellos.** **d) Mecanismos para proteger la información contra cambios, copias y distribución no autorizada, como uso de credenciales fuertes, restringir accesos por periodos de tiempo o ubicación, uso del cifrado para información confidencial y registro de quien accede a la información.** **8.4.4. Acceso al código fuente** **El DDMSI debe incluir en las directivas de desarrollo de software lo siguiente:** **a) Restringir de acceso al código fuente, así como a la documentación del proyecto solo al personal y/o terceros involucrados en la construcción del sistema de información o aplicativo, previa autorización del Jefe de DDMSI.** **b) Se debe almacenar el código fuente en una herramienta centralizada que permita:** **• Controlar los accesos a modo de lectura o escritura y mantener registros de auditoría de todos los accesos y de todos los cambios realizados al código fuente.** **• Controlar las versiones del código fuente y de sus componentes asociados como manuales técnicos y documentos del proyecto.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		c) Mantener copias de seguridad del código fuente de acuerdo con la programación aprobada por el DISI. **8.4.5. Autenticación segura** **El DISI debe asegurar la implementación de tecnologías o controles de autenticación a los sistemas de información que considere:** **a) El uso de un mecanismo de autenticación fuerte, si la tecnología lo permite, para verificar la identidad del usuario con métodos de autenticación adicionales a la contraseña (autenticación multifactor) como el uso de certificados digitales de autenticación, tarjetas inteligentes, tokens o medios biométricos, sobre todo para el acceso a los sistemas críticos de la CPMP o aquellos que permiten el acceso a datos personales.** **b) De utilizar autenticación biométrica incluir alguna técnica de autenticación alternativa que permita la disponibilidad del acceso en caso de falla.** **c) Para los sistemas críticos o que contienen información confidencial, verificar que cuenten con controles para la restricción de acceso a los sistemas de información y servicios.** **d) En el inicio de sesión a los aplicativos y/o sistemas de información de la CPMP no se debe:** **• Brindar mensajes que permitan identificar el dato incorrecto.** **•Mostrar información confidencial o del sistema antes de la autenticación exitosa para evitar exponer información a un usuario no autorizado.** **•Mostrar el texto de la contraseña sin enmascarar mientras esté siendo ingresada por el usuario.** **e) Implementar medidas de seguridad para proteger los aplicativos y/o sistemas de información de intentos de inicio de sesión por fuerza bruta, como el uso de captcha, o aplicando el bloqueo al usuario después de tres (3) errores.** **f) Almacenar la información de autenticación, tanto de los intentos exitosos como de los fallidos.** **g) Configurar el envío de alertas de seguridad al usuario y administradores ante algún incumplimiento de los controles de inicio de sesión.** **h) Transmitir las contraseñas cifradas por la red para evitar que esta sea capturada por ciberdelincuentes.** **En el caso de los servicios tecnológicos se deben configurar el uso de mecanismos de autenticación fuertes y otros controles dependiendo de la herramienta y la información que contiene.** **8.4.6. Gestión de capacidad** **El DISI debe analizar y aplicar controles para la supervisión de la demanda de capacidad de sus recursos administrados, por ejemplo, monitorear el consumo de recursos de procesadores, memorias, servicios de almacenamiento, servicios de**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		impresión, anchos de banda, servicio de internet, servicios externos requeridos a otras instituciones, tráfico de las redes de datos, entre otros, y realizar proyecciones de crecimiento de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. **8.4.7. Protección contra programas maliciosos (*malware*)** **El DISI debe implementar reglas y controles que detecten el uso de software no autorizado, el acceso a sitios web maliciosos y detección de *malware*. Estos controles deben considerar:** **a) Asegurar que los equipos informáticos cuenten con herramientas de seguridad contra códigos maliciosos y se actualicen periódicamente.** **b) Realizar charlas de concientización apropiada a los usuarios y colaboradores, sobre los riesgos a los que estamos expuestos en Internet y cómo afrontar un evento u ocurrencia de infección de virus o *malware*.** **c) Todo equipo que se encuentre operativo y que no cuente con una herramienta de protección contra software malicioso no podrá ser conectado a la red de datos de la CPMP.** **d) Todo contrato de arrendamiento de equipos informáticos debe incluir el requisito de una herramienta de protección contra software malicioso. Mantener los sistemas operativos y software, con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).** **e) La plataforma de comunicaciones debe contar con equipamiento de seguridad que otorgue la protección necesaria ante amenazas y controle el tráfico de entrada y de salida para la red de datos de la CPMP.** **No está permitido por el personal de la CPMP:** **a) La desinstalación y/o desactivación de software y herramientas de seguridad implementadas por el DISI.** **b) Instalar y ejecutar programas ya sean propios u obtenidos a través de internet, correo u otro medio, en los equipos de la institución sin la debida autorización del DISI.** **8.4.8. Gestión de vulnerabilidades técnicas** **El DISI incluye dentro de los requisitos de adquisición o mantenimiento de software pruebas o análisis de vulnerabilidades.** **El DRO realiza periódicamente pruebas de vulnerabilidades sobre los servicios e infraestructura tecnológica y comunicará los resultados a las UO encargadas de la remediación para que planifiquen las acciones necesarias.** **El DISI como responsable de la seguridad de los recursos y servicios informáticos, realiza tareas de actualización periódica sobre el software de los**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		servidores, equipos de cómputo, comunicaciones o seguridad perimetral. **Los colaboradores o terceros que detecten vulnerabilidades o debilidades que puedan poner en peligro la información, recursos o servicios de TI, debe comunicarlo al OSCD siguiendo las disposiciones y actividades establecidas en la directiva "Normas y Procedimientos para la Gestión de Incidentes en la Infraestructura Informática".** **Los colaboradores o terceros que detecten vulnerabilidades no deben aprovecharse de estas para acceder o difundir información no autorizada, así como producir alguna interrupción o daño en los recursos y servicios de TI.** **8.4.9. Gestión de la configuración** **El DISI establece controles para documentar, implementar, monitorear y revisar las configuraciones de seguridad de sus activos críticos (hardware, software, servicios y redes). Así mismo, es el encargado de revisar periódicamente y actualizar la configuración del hardware, software, servicios y redes de acuerdo con las buenas prácticas de seguridad definida por los proveedores o las organizaciones de seguridad como el CNSD de la PCM. En la revisión y actualización se debe considerar las nuevas amenazas, debilidades, así como su viabilidad y aplicabilidad de la actualización de las versiones de acuerdo a contexto de la CPMP.** **Solo los administradores del hardware, software, servicios y redes del DISI, son los responsables de realizar una actualización en la configuración siguiendo el procedimiento de gestión de cambio.** **8.4.10. Eliminación de información** **Los responsables de cada UO, en coordinación con el DISI, deben asegurar que la eliminación de la información clasificada como confidencial se realice de manera segura guardando evidencia de la actividad y resultados de la eliminación: información del lugar, fecha, hora, personas que intervinieron, método y herramienta utilizada.** **Corresponde al DISI:** **a) Identificar el método de eliminación de información (digital) apropiada para cada tipo de medio de almacenamiento, por ejemplo, uso de un software de eliminación segura, desmagnetizado de unidades de disco duro o de disco de almacenamiento externo, trituradoras de papel.** **b) Registrar los resultados de la eliminación como evidencia.** **c) Asegurarse que la información confidencial almacenada en la nube se elimine de forma segura cuando no se requiera.** **Las UUOO que requieran Para la eliminación de grandes volúmenes de información física, se debe utilizar proveedores certificados y aprobados de servicios de eliminación segura.** **8.4.11. Enmascaramiento de datos** **No está permitido el uso de data de producción para desarrollos, pruebas, salvo que esta sea**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		previamente enmascarada para evitar la pérdida de confidencialidad de la información. **Los responsables de las UUOO deben proteger la información, incluyendo datos personales y sensibles, a la que acceden de acuerdo con su clasificación, considerando mecanismos de enmascaramiento, anonimización o disociación.** **El DISI implementa técnicas adicionales para el enmascaramiento de datos en los sistemas de información (anular, eliminar o sustituir caracteres) con la finalidad de limitar la exposición de datos confidenciales.** **8.4.12. Prevención de fuga de datos** **Los responsables de las UUOO deben identificar, clasificar y registrar en el inventario de activos la información contenida en los procesos y sistemas de información del cual son propietarios.** **El DISI debe implementar herramientas que permitan monitorear y/o prevenir la fuga de datos en servicios como el correo electrónico, transferencia de archivos a través servicios de almacenamiento en la nube, discos de almacenamiento externo, entre otros.** **8.4.13 Copia de seguridad de la información** **El respaldo de la información debe almacenarse en lugares distantes de la sede principal para evita cualquier daño en caso de desastre en las instalaciones de la CPMP.** **El DISI establece los requisitos necesarios para la protección ambiental y física de las copias de respaldo.** **Se realiza copias de respaldo de la información de los servicios de ambiente de producción, desarrollo y pruebas de la CPMP, los cuales incluyen bases de datos y unidades de red y se encuentran administrados por el DISI.** **El DISI revisará periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.** **El DISI realizará pruebas periódicas (mínimo anual) de recuperación del respaldo, para asegurar que son confiables, para lo cual seleccionará una muestra de información coordinará la verificación con la correspondiente UO propietaria.** **Adicionalmente, en caso un área usuaria requiera la restauración de una copia de respaldo, esta será considerada como una prueba de recuperación de respaldo.** **8.4.14 Redundancia de las instalaciones de procesamiento de información** **Los propietarios de los sistemas de información y procesos, en coordinación con el DISI, deben establecer los requisitos de disponibilidad de la información y servicios informáticos y sistemas de información, en el caso de la materialización de situaciones adversas.** **El DISI debe:**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		a) Asegurar la redundancia de los principales componentes tecnológicos (servidores, base de datos y otros), que permitan la continuidad de los sistemas de información que se considere crítico para la institución. **b) Determinar la infraestructura alterna de tecnología de información, la cual debe localizarse geográficamente en un lugar diferente a la sede principal, asegurando que presente seguridad en los siguientes aspectos: calidad de suelos y del entorno, riesgo de inundación, calidad de la construcción, disponibilidad de servicios básicos, entre otros.** **c) Elaborar un plan de contingencia informático que permita definir las actividades a seguir para la activación de los componentes tecnológicos redundantes, incluyendo las instalaciones de procesamiento alterno.** **d) Contar con dos proveedores diferentes de los servicios críticos para la continuidad de los sistemas de información, por ejemplo, el servicio de Internet.** **El DRO es el encargado de probar de manera anual y documentar los resultados del plan de contingencia informático.** **8.4.15. Registro** **Se deben contar con registros (logs de auditoría) de acceso a las bases de datos que contengan datos personales, así como registro de las acciones relevantes sobre estas.** **El DISI es responsable de la custodia de los registros y de implementar sistemas de monitoreo continuo y detección de amenazas para identificar y responder rápidamente a posibles incidentes de seguridad sobre los componentes informáticos, así mismo, deberá analizar los registros para validar la integridad y disponibilidad de estos.** **El OSCD es responsable de validar y/o recomendar el análisis de los registros.** **8.4.16. Actividades de monitoreo** **El DISI debe:** **a) Identificar los recursos informáticos críticos que deben ser monitoreados, estableciendo una línea base de comportamiento del recurso, la frecuencia de monitoreo y el periodo de retención de las evidencias.** **b) Se debe implementar una herramienta que permita monitorear y enviar alertas automáticas de:** **• El tráfico de la red y los sistemas de información, entrante y saliente.** **• El acceso a los sistemas de información, equipos de la red de datos y demás servicios críticos.** **•Uso de recursos como CPU, disco duro, memoria y ancho de banda, incluyendo su rendimiento.** **• Así como almacenar y revisar los registros del monitoreo para realizar proyecciones de futuros requisitos de capacidad, que aseguren el**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		desempeño requerido por los servicios informáticos y sistemas de información. **8.4.17. Sincronización de reloj** **El DISI, debe sincronizar los relojes de todos los sistemas de procesamiento de información y servicios informáticos tomando como referencia una única fuente confiable de transmisión del tiempo, basándose en protocolos estándares de sincronización reconocidos cómo el Protocolo de Tiempo de Red (PTR o NTP *Network Time Protocol*) o el Protocolo de Tiempo de Precisión (PTP).** **8.4.18. Uso de programas de utilidad privilegiados** **Toda instalación de programas de utilidad privilegiados en los equipos informáticos de la red de datos de la CPMP debe contar con la autorización del jefe de la UO en la que labora el usuario y del jefe del DISI.** **DISI debe:** **a) Mantener un inventario actualizado de los programas privilegiados instalados en el CPMP.** **b) Establecer controles de acceso en los equipos y servicios informáticos para limitar la instalación y uso de programas privilegiados solo a los usuarios autorizados.** **Corresponde a los usuarios que cuenta con la autorización de uso de programas de utilidad privilegiados:** **a) Utilizar los programas solo para las actividades autorizadas.** **b) Mantener la confidencialidad de la información a la que puedan acceder con dichos programas privilegiados.** **8.4.19. Instalación de software en sistemas operativos** **Los colaboradores o terceros no deben ejecutar o instalar software en los equipos informáticos, esta actividad es exclusiva del personal técnico del DISI.** **El colaborador que requiera la instalación de software adicional a lo instalado en su equipo de cómputo deberá solicitarlo a través del Sistema de Solicitud de Trabajo previa autorización del responsable de la UO. El DISI realizará la evaluación del requerimiento y en caso de no afectar la seguridad del equipo de cómputo, la red o se encuentre en discordancia con la normatividad institucional, autorizará y ejecutará la instalación del software.** **La actualización de software que no se realice automáticamente a través de las herramientas del DISI, deberán ser solicitadas como un requerimiento a través del Sistema de Solicitud de Trabajo.** **El DISI es responsable de gestionar las actualizaciones de software en los equipos informáticos de forma automática y/o manual, por lo cual no se requiere la descarga de parches u otro software por parte de los colaboradores.** **8.4.20. Seguridad de redes**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		El DISI debe: **a) Gestionar, proteger y conservar la seguridad de los datos en las redes de la CPMP.** **b) Mantener actualizada la documentación técnica de la red, como los diagramas de red, el inventario de los equipos que conforman la infraestructura tecnológica y la información de su configuración.** **c) Establecer controles y medidas especiales para salvaguardar la disponibilidad, confidencialidad e integrar los datos que se transfieren a través de redes públicas, incluyendo los sistemas de información, por ejemplo, implementando equipos como firewall, sistemas de detección y prevención de intrusiones, entre otros.** **d) Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red.** **e) Implementar sistemas de autenticación a la red que requieran más de un factor de autenticación de usuario.** **f) Implementar procedimientos que permitan reducir las vulnerabilidades técnicas en las redes, como, deshabilitar los protocolos de red vulnerables y el endurecimiento (*hardening*) de red y servidores.** **g) Registrar las acciones o vulnerabilidades que puedan afectar la seguridad de la información de las redes y realizar su atención.** **El OSCD deberá verificar la atención a las vulnerabilidades de red identificadas y reportadas por el DRO.** **8.4.21. Seguridad de servicios de red** **El DISI debe:** **a) Implementar procedimientos de autorización y controles de autenticación para acceder a las redes y servicios en red.** **b) La conexión a la red de datos y servicios de red de la CPMP de manera remota se debe realizar a través de una Red Privada Virtual (VPN) u otro mecanismo que permita establecer una línea segura y cifrada entre la red de datos de la CPMP y el equipo de cómputo del usuario.** **c) Monitorear, revisar y auditar regularmente todos los servicios de red incluyendo los provistos por terceros.** **d) Analizar las vulnerabilidades y aplicar las correcciones de seguridad de manera oportuna.** **e) Planificar y autorizar los cambios en los servicios de red, incluyendo los que proveen terceros, considerando los riesgos que podrían generar, en el marco de la normativa aplicable.** **f) Identificar e incluir en los acuerdos de servicios de red y/o los términos de referencia (para los servicios tercerizados) los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red.**	

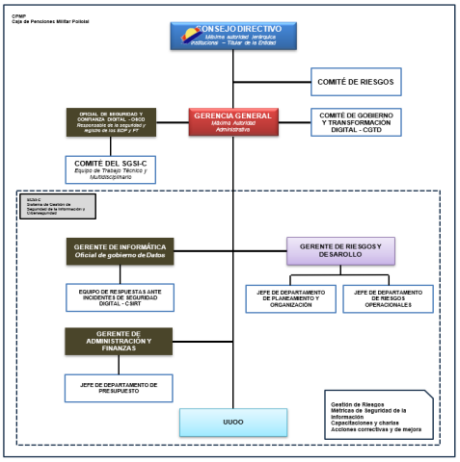
MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		g) Verificar la implementación de los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red. **Los usuarios de la red deben:** **a) Utilizar los recursos de red de manera responsable y ética, evitando acciones que puedan poner en riesgo la seguridad de las redes.** **b) Reportar, a través de los procedimientos establecidos, cualquier incidente de seguridad, vulnerabilidad o sospecha de actividad maliciosa.** **8.4.22. Segregación de redes** **El DISI debe:** **a) Segregar las redes en función de los niveles de confianza, criticidad y sensibilidad de la información, sistemas y servicios que contienen.** **b) Configurar *firewalls, routers* y otros dispositivos para limitar el acceso entre las diferentes zonas de la red, por ejemplo, el acceso a los recursos y datos sensibles que permitan reducir el impacto potencial de un incidente de seguridad.** **8.4.23. Filtrado de la web** **El servicio de internet se encuentra disponible para los colaboradores como herramienta de apoyo para el cumplimiento de sus funciones y realización de actividades.** **Los colaboradores son responsables de dar buen uso al servicio de internet, así como de adoptar las medidas de seguridad necesarias que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.** **El DISI es responsable de brindar el servicio de internet a través de mecanismos seguros para lo cual implementa controles y filtros de navegación lo cual puede implicar la restricción parcial o total de sitios web potencialmente peligrosos. De igual modo, establece las configuraciones necesarias en los navegadores web autorizados en los equipos de cómputo.** **Las páginas de redes sociales, de archivos de transferencia masiva y de inteligencia artificial están restringidas y controladas para los usuarios. El uso de este tipo de recursos debe ser debidamente sustentado y aprobado por la jefatura y/o Gerencia correspondiente, así mismo, debe ser evaluado por el DRO y el OSCD.** **Dentro de las instalaciones de la CPMP, no está permitido conectar los equipos informáticos de la CPMP a cualquier otro medio de conexión a internet de proveedores externos que no haya sido dispuesto por la CPMP.** **La CPMP cuenta con la potestad de mantener los registros de navegación de su servicio de internet, así como de toda información entrante o saliente a través de su red, con la finalidad de monitoreo y/o revisión y sin previo aviso.** **Las solicitudes de cambio en la configuración del acceso a internet son aprobadas por el DISI, y en**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		caso sea necesario se elevará a evaluación por el Comité de Gobierno y Transformación Digital. **Está prohibido visitar sitios web con contenido inapropiado o que puedan ser fuente de archivos y programas maliciosos.** **8.4.24. Uso de criptografía** **El personal de la CPMP debe remitir de manera encriptada la información electrónica cuya clasificación no sea pública, en el caso de ser requerida; previa autorización de su propietario. Para ello puede solicitar el apoyo técnico del DISI.** **El DISI establece los controles necesarios para protección durante la generación, almacenamiento y archivo de las claves criptográficas mediante protocolos *HTTPS, SFTP, IPSEC, SSH*, incluyendo los respaldos y accesos correspondientes.** **El uso de certificados digitales se debe realizar cumpliendo las normas legales vigentes y las condiciones de uso establecidas por la Entidad de Certificación Digital.** **El DISI debe:** **a) Asegurar que los controles criptográficos cumplan con estándares nacionales e internacionales, evitando el uso de controles con algoritmos de encriptación considerados como débiles, obsoletos o inseguros.** **b) Implementar métodos criptográficos que permitan la integridad y confidencialidad de la información desde su transmisión hasta su recepción, como la publicación de servicios y sistemas de información a través de un certificado digital SSL *(Secure Sockets Layer*).** **c) Previa evaluación de riesgos, determinar la necesidad de encriptar la información que no sea de carácter público, incluyendo la referida a datos personales, almacenados en las bases de datos de la CPMP.** **8.4.25. Ciclo de vida de desarrollo seguro** **Las UUOO que requieran el desarrollo mantenimiento de sistemas de información deberán coordinarlos con el DDMSI.** **El DDMSI cuenta con requisitos de seguridad de la información para el desarrollo (interno o tercerizado), la adquisición y mantenimiento de sistemas de información, los cuales forman parte de los términos de referencia o requisitos mínimos en sus proyectos, incluyendo principios de codificación.** **El DDMSI es responsable de normar, solicitar e implementar los mecanismos técnicos que protejan los sistemas de información alojados en estos.** **El DDMSI es responsable de gestionar las pruebas de seguridad y funcionales necesarias para los nuevos sistemas o mantenimientos.** **El DDMSI establece un procedimiento para el control de cambios, el cual debe seguir principios de seguridad para los sistemas de información.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		8.4.26. Requisitos de seguridad de la aplicación **El DDMSI, en coordinación con el OSCD, debe:** **a) Incluir en los requisitos de los nuevos sistemas de información o en las propuestas de mejoras de los sistemas de información existente; aquellos relacionados con la seguridad de la información, desde las etapas iniciales del proyecto.** **b) Proteger la información involucrada en los servicios de aplicaciones a través de redes públicas.** **c) Proteger la información involucrada en las transacciones de servicios de las aplicaciones, para prevenir transmisión incompleta, ruteo incorrecto, alteración o divulgación no autorizada de mensajes, ya sea interna o externa a la CPMP.** **d) Verificar que los cambios solicitados formalmente por los propietarios de la información no causen riesgos de seguridad y de ocurrir un incidente de seguridad en la implementación de un cambio, debe deshabilitarse para su posterior subsanación.** **e) Determinar las pruebas de calidad y seguridad de software a aplicar de acuerdo con la criticidad del sistema y del cambio.** **8.4.27. Arquitectura de sistemas seguros y principios de ingeniería** **El DDMSI debe:** **a) Establecer, documentar y aplicar principios de ingeniería segura en el desarrollo de los sistemas de información.** **b) Diseñar la seguridad en todas las capas de la arquitectura de un sistema de información (negocios, datos, aplicaciones y tecnología).** **c) En caso de uso de nueva tecnología, se deben analizar e identificar los riesgos de seguridad.** **8.4.28. Codificación segura** **El DDMSI, debe establecer pautas para la codificación segura. Dentro de estos deben incluir que:** **a) Los desarrolladores y analistas sigan las mejores prácticas de codificación segura y estándares de seguridad reconocidos para el desarrollo y mantenimiento de software, por ejemplo, el uso de *frameworks* y librerías de seguridad reconocidas para mitigar las vulnerabilidades comunes como las difundidas por la *Open Web Application Security Project* - OWASP y su publicación de los diez riesgos de seguridad más importantes (Top 10).** **b) Implementar controles de validación y sanitización de datos de entrada para prevenir ataques de inyección de código.** **8.4.29. Pruebas de seguridad en desarrollo y aceptación** **El DDMSI debe:** **a) Validar los sistemas de información y aplicaciones durante todas las etapas del desarrollo de software.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		b) Considerar pruebas unitarias, pruebas calidad funcional y no funcional (por ejemplo: validación de datos y rendimiento), pruebas de seguridad y pruebas de aceptación por el usuario. **c) En las pruebas de seguridad incluir pruebas de autenticación de usuario, restricción de acceso, codificación y configuración segura.** **d) Determinar el alcance y los tipos de pruebas en la etapa de análisis en función a la importancia, la naturaleza del sistema y el impacto del cambio.** **e) Implementar herramientas automatizadas para identificar vulnerabilidades.** **f) Verificar la corrección de los defectos relacionados con la seguridad.** **8.4.30. Desarrollo subcontratado** **Los proveedores de desarrollo deben cumplir con las normas y requisitos de seguridad de la información establecidos por la CPMP, así como colaborar en la identificación y atención de riesgos de seguridad de la información durante el proceso de desarrollo.** **La Gerencia de Informática debe:** **a) Incluir en los términos de referencia de los sistemas desarrollados o modificados por terceras partes, que deben cumplir con lo establecido en esta política de seguridad y la normativa de la CPMP.** **b) Establecer acuerdos previos con todos los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en los proyectos.** **c) Implementar un proceso de supervisión, revisión y aprobación de los entregables para asegurar la calidad y seguridad de los sistemas y aplicaciones entregados.** **El OSCD y el DRO, en coordinación con los propietarios del sistema y los desarrolladores, deben evaluar los riesgos asociados al desarrollo tercerizado para verificar que se cuentan con los controles de seguridad adecuados.** **8.4.31. Separación de los entornos de desarrollo, prueba y producción** **El DISI debe:** **a) Mantener separados los ambientes de desarrollo, pruebas y producción.** **b) Establecer las actividades a seguir para el despliegue del software desde el ambiente de desarrollo, prueba hasta el ambiente de producción.** **c) No permitir la ejecución de pruebas en entornos de producción, salvo excepciones aprobadas por el jefe de DISI y el propietario del sistema.** **d) No utilizar en los ambientes de desarrollo y pruebas datos confidenciales o personales similares al ambiente de producción. De ser necesario se**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		deben aplicar procedimientos de enmascaramiento o anonimización. **e) Implementar en los ambientes de desarrollo y pruebas las actualizaciones de seguridad del software utilizado y controlar el acceso solo a personal autorizado por el Jefe del DISI.** **f) Proteger el acceso a la información de producción de acuerdo con su clasificación.** **8.4.32. Gestión de cambios** **El DISI es responsable de gestionar los cambios en la infraestructura tecnológica y/o sistemas de información, y normar los procesamientos necesarios para este fin, así como mantener información documentada sobre este proceso.** **Los cambios deberán ser planificados e incluir la identificación de los posibles compromisos en seguridad de la información, los cuales, de ser el caso, serán comunicados al OSCD para su evaluación de acuerdo con las políticas y requisitos de seguridad de la información.** **Los cambios de emergencia que requieren ser aplicados para resolver un incidente, deberán realizarse de forma rápida y controlada.** **Los cambios realizados deben ser verificados para asegurar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información el sistema y que el propósito del cambio se cumplió satisfactoriamente.** **Los cambios deben de incluir un plan de roll-back (volver al estado anterior), que incluyan las actividades a seguir para abortar los cambios que se ejecutaron sin éxito y/o eventos imprevistos.** **8.4.33. Información de las pruebas** **El DISI y el DDMSI deben:** **a) Realizar las pruebas de los sistemas de información en un ambiente controlado y con los datos seleccionados para tal fin.** **b) Implementar medidas de confidencialidad para proteger la información de prueba de acuerdo con su clasificación, como la encriptación de datos sensibles y la restricción de acceso solo a personal autorizado.** **c) El personal que participa en la ejecución de las pruebas no debe ser el mismo que participó en su desarrollo.** **d) Documentar los resultados de las pruebas realizadas.** **8.4.34. Protección de los sistemas de información durante las pruebas de auditoría** **Se establecerá y mantendrá un programa de auditorías internas para verificar que el SGSI-C es conforme con los requisitos de la Norma ISO 27001:2022 y los requisitos de la propia organización para su SGSI-C. Los resultados de las auditorías se informarán a la dirección pertinente y**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		se tomarán acciones correctivas oportunas para abordar las no conformidades. **Las pruebas de auditoría que afecten la disponibilidad de los sistemas deben ejecutarse fuera del horario de oficina previa coordinación entre el auditor, el OSCD, el DISI y los responsables de las UUOO cuya información se encuentre involucrada en la auditoría.**	
9. ESTRUCTURA ORGANIZACIONAL DEL SGSI-C	~~5.3 Estructura organizacional del SGSI-C~~ ~~5.3.1~~ Consejo Directivo ~~a)~~ Aprobar políticas y lineamientos para la implementación del SGSI-C y su mejora continua. ~~b) Aprobar el presupuesto para la disposición de~~ los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento. ~~c)~~ Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados. ~~d) Aprobar el plan estratégico del SGSI-C y recomendar acciones a seguir.~~ ~~f) Aprobar el plan de fomento de la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.~~ ~~5.3.2~~ Comité de Riesgos ~~a) Proponer al Consejo Directivo el plan estratégico del SGSI-C y recomendar acciones a seguir.~~ ~~b) Proponer al Consejo Directivo el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y Ciberseguridad.~~ ~~c) Proponer al Consejo Directivo el plan de fomento~~	**9.1 Estructura Organizativa – Sistema de Gestión de Seguridad de la Información y Ciberseguridad**  **9.1.1.** Consejo Directivo **a) Aprobar el plan estratégico del SGSI-C de la CPMP.** **b)** Aprobar las políticas y lineamientos para la implementación del SGSI-C y su mejora continua. **c) Asignar** los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento. **d)** Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados. **e) Tomar conocimiento del desempeño, de los resultados y de los acuerdos adoptados de la gestión integral de riesgos relacionados al SGSI-C.** **9.1.2.** Comité de Riesgos **a) Aprobar el plan de capacitación a fin de garantizar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades en el marco de la seguridad de la información.** **b) Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.** **c) Revisar y presentar semestralmente al Consejo Directivo el desempeño, los resultados y los acuerdos adoptados de la gestión integral de riesgos relacionados al SGSI-C.**	Se incorporó y actualizó la Estructura Organizacional del SGSI-C. Se estableció la estructura de Gobierno de Seguridad de la Información y Ciberseguridad.

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	~~d) Proponer al Consejo Directivo las políticas y la organización para la gestión de riesgos de seguridad de la información y ciberseguridad.~~ ~~c) Presentar trimestralmente al Consejo Directivo, un reporte de eventos inesperados, registrados durante el periodo y las acciones~~ ~~f) Proponer al Consejo Directivo los recursos necesarios para la gestión de los riesgos de la seguridad de la información y ciberseguridad.~~ ~~g) Velar por el cumplimiento de las referidas políticas.~~ ~~5.3.3 Unidad de Auditoría Interna~~ ~~a) Evaluar el cumplimiento de los requisitos de seguridad de la información y ciberseguridad de la CPMP.~~ ~~5.3.4~~ Gerencia General ~~b)~~ Velar por el cumplimiento de las políticas ~~de seguridad de la información y ciberseguridad~~. ~~a) La Gerencia General es responsable de tomar las medidas necesarias para implementar~~ el SGSI-C de acuerdo a las disposiciones del Consejo Directivo y lo dispuesto en la normativa vigente ~~sobre el sistema de seguridad de la información y ciberseguridad.~~ ~~c) Aprobar los procedimientos de seguridad de la información y ciberseguridad.~~ ~~5.3.5. Comité Especializado en Seguridad de la Información y Ciberseguridad~~	**d) Revisar y presentar semestralmente al Consejo Directivo, los resultados de las auditorías internas y/o externas, y los indicadores clave (KRIs) del SGSI-C.** **9.1.3.** Gerencia General **a) Revisar y elevar al Consejo Directivo el plan estratégico del SGSI-C.** **b) Aprobar el plan de Implementación del SGSI-C.** **c) Informar semestralmente al Consejo Directivo los avances y dificultades en la implementación y/u operación del SGSI-C.** **d)** Velar por el cumplimiento de las políticas, **objetivos planes, procedimientos y marco normativo en confianza y seguridad digital**. **e) Adoptar las medidas necesarias para implementar y mantener adecuadamente** el SGSI-C, de acuerdo a las disposiciones del Consejo Directivo y a lo dispuesto en la normativa vigente**.** **f) Brindar recursos, personal y/o asesorías a las UUOO para la f) implementación, mantenimiento y mejora continua del SGSI-C, previamente aprobados en el presupuesto institucional.** **9.1.4. Comité de Gobierno y Transformación Digital - CGTD** **El CGTD es responsable de dirigir, mantener y supervisar estratégicamente los planes, resultados y recursos del SGSI-C. A solicitud del Consejo Directivo o de la Gerencia General, puede emitir opiniones y recomendaciones sobre la gestión estratégica del SGSI-C. Además, la entidad podrá requerir la opinión de órganos consultivos relacionados con la gestión de riesgos. Sus funciones se encuentran establecidas en la Resolución de Gerencia General Nº 042-2023/CPMP-GG, o documento que lo reemplace.** **Así mismo, el Comité de Gobierno y Transformación Digital está conformado por:** **Rol en el CGTD** / **Cargo en la CPMP** **Titular de la Entidad o su representante** / **Gerente General** **Líder de Gobierno y Transformación Digital - secretario técnico del Comité** / **Gerente de Informática**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		Responsable del área de informática o quien haga sus veces → **Jefe de Departamento de Desarrollo y Mantenimiento de Sistemas de Información** **Responsable del área de recursos humanos o quien haga sus veces** → **Jefe de Departamento de Gestión de Personas** **Responsable del área de atención al ciudadano o quien haga sus veces** → **Gerente de Pensiones** **Oficial de Seguridad y Confianza Digital** → **Jefe de Departamento de Infraestructura y Seguridad Informática** **Responsable del área legal o quien haga sus veces** → **Gerente Legal** **Responsable del área de planificación o quien haga sus veces** → **Jefe de Departamento de Presupuesto** **9.1.5. Comité del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C)** **El Comité del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (Comité del SGSI-C) es un equipo de trabajo técnico y multidisciplinario para el SGSI encargado de realizar la implementación y mantenimiento del SGSI de la CPMP. Dicho equipo de trabajo es liderado por el OSCD. La organización del equipo de trabajo debe considerar el contexto, tamaño, complejidad y estructura de la entidad. El Comité del SGSI-C está conformado por:** **Titular** → **Suplente** **Oficial de Seguridad y Confianza Digital** → **Especialista en Seguridad de Información** **Jefe de Departamentos de Riesgos Operacionales** → **Analista de Riesgos Operacionales** **Gerente de Informática** → **Jefe de Departamento de Desarrollo y Mantenimiento de Sistemas de Información** **Gerente de Administración y Finanzas** → **Subgerente de Logística** **Se podrá convocar a las reuniones del Comité a cualquier UO de la CPMP.** **Las funciones del Comité del SGSI-C son:**	
	a) Revisar y elevar ~~el plan estratégico~~ del SGSI-C ~~y recomendar acciones a seguir al Comité de Riesgos~~.	a) Revisar y elevar **las propuestas de políticas y lineamientos** del SGSI-C.	
	~~c)~~ Revisar y elevar~~ el plan de fomento de la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención al Comité de Riesgos.~~	**b)** Revisar y elevar **a la Gerencia General el plan de implementación del SGSI-C.**	
	~~d~~) Revisar y elevar~~ las políticas y la organización para la gestión de riesgos de seguridad de la información al Comité de Riesgos para su revisión y aprobación.~~	**c)** Revisar y elevar **a la Gerencia General, las políticas, manuales y procedimientos, para implementar, operar, mantener y mejorar el SGSI-C.**	
	~~e) Informar los resultados de la operación del SGSI-C a la Gerencia General y Comité de Riesgos.~~	**d) Proponer la organización, roles y responsabilidades para el SGSI-C al Consejo Directivo.**	
	~~f) Revisar y aprobar los planes, instructivos, guías, formatos y documentación general del SGSI-C.~~	**e) Recomendar acciones a seguir al Comité de Riesgos.**	
	~~g) Solicitar los recursos necesarios para la gestión de los riesgos de la seguridad de la información y ciberseguridad.~~		
	~~5.3.1.~~ ~~e) Aprobar~~ el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el	**f) Proponer al Comité de Riesgos** el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el Consejo Directivo cuenten con	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	~~directorio~~ cuenten con competencias necesarias en seguridad de la información y ciberseguridad. ~~5.3.5~~ ~~b)~~ Revisar y elevar el plan de ~~capacitación en seguridad de la información y ciberseguridad,~~ al Comité de Riesgos. ~~5.3.6 Oficial de Seguridad de la Información y Ciberseguridad~~ ~~El Oficial de Seguridad de la Información y Ciberseguridad es el responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información; dichas funciones son realizadas por el Jefe de Departamento de Riesgos Operacionales.~~ ~~a) Elaborar y proponer las políticas, planes, instructivos, guías, formatos y documentación en general del SGSI-C para revisión del Comité Especializado en Seguridad de la Información y Ciberseguridad.~~ ~~b) Elaborar y proponer los procedimientos de seguridad de la información y ciberseguridad para aprobación de la Gerencia General.~~ ~~c) Informar sobre los incidentes de seguridad de la información al Comité Especializado en Seguridad de la Información y Ciberseguridad, según los lineamientos que este establezca, y al ente regulador.~~ ~~d) Evaluar las amenazas de seguridad y ciberseguridad en las estrategias de continuidad del negocio que la CPMP defina y proponer medidas de mitigación de riesgos, así como informar al Comité Especializado en Seguridad de la Información y Ciberseguridad.~~ ~~e) Promover y coordinar la ejecución de todas las actividades relacionadas con el proceso de implementación, operación y mejora continua del SGSI-C.~~ ~~f) Realizar la supervisión y cumplimiento de la presente directiva. Asimismo, que el SGSI-C se implemente conforme a los requisitos de seguridad de la información y ciberseguridad.~~ ~~g) Guiar al personal del proceso con la correcta aplicación de la metodología del SGSI-C.~~	competencias necesarias en seguridad de la información y ciberseguridad. **g)** Revisar y elevar el plan de **fomento de la cultura de riesgo** al Comité de Riesgos. **h) Revisar y aprobar los planes, instructivos, guías, formatos y documentación en general relacionada con el SGSI-C.** **i) Elaborar e informar semestralmente al Comité de Riesgos el desempeño, los resultados y los acuerdos adoptados de la gestión integral de riesgos relacionados al SGSI-C, a través del Gerente de Riesgos y Desarrollo.** **j) Elaborar e Informar semestralmente al Comité de Riesgos, los resultados de las auditorías internas y/o externas, y los indicadores clave (KRIs) del SGSI-C.** **k) Elevar a la Gerencia General, las propuestas de solicitud de recursos, personal y/o asesorías, necesarios para el desarrollo del SGSI-C.** **9.1.6 Oficial de Seguridad y Confianza Digital (OSCD)** **Es la persona responsable de coordinar la implementación, operación, mantenimiento y mejora continua del (SGSI-C) en la CPMP, atendiendo políticas y normas en materia de seguridad digital, confianza digital y gobierno digital. Además, coordina y reporta al Comité de Gobierno y Transformación Digital institucional, la implementación, mantenimiento, y la aplicación de las normas relacionadas con la seguridad digital, confianza digital, transformación digital, y gobierno digital, cuyas responsabilidades son:** **a) Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI-C de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.** **b) Coordinar con las UUOO de la entidad las acciones orientadas a implementar y/o mantener el SGSI-C, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.** **c) Formular y elevar al Comité del SGSI-C, el plan estratégico del SGSI-C.** **d) Formular y elevar al Comité del SGSI, el plan de Implementación del SGSI-C y registrarlo en la Plataforma Facilita Perú.** **e) Formular y elevar al Comité del SGSI las políticas, manuales, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
	~~h) Evaluar, coordinar y monitorear la implementación de controles y mejoras en seguridad de la información relacionadas al SGSI-C.~~ ~~i) Evaluar los riesgos de seguridad de información y ciberseguridad ante cambios significativos a nivel de procesos y tecnología en la CPMP.~~ ~~j) Realizar las charlas establecidas en el Plan de Capacitación y Sensibilización.~~ ~~k) Informar los resultados de seguridad de la información y ciberseguridad al Comité Especializado en Seguridad de la Información y Ciberseguridad.~~ ~~l) En general realizar lo necesario para dar debido cumplimiento a lo dispuesto en la presente directiva.~~ ~~5.3.7 Unidades orgánicas~~ ~~Las unidades orgánicas están compuestas por los gerentes, jefes de departamentos, custodio del activo de información, propietario del activo de información, y el usuario.~~ ~~a) Apoyar el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y ciberseguridad en el marco de sus funciones.~~ ~~b) Cumplir con las políticas, procedimiento y metodologías de seguridad de la información y ciberseguridad.~~ ~~c) Utilizar los activos de información únicamente para los fines autorizados.~~ ~~d) Identificar, analizar, evaluar y tratar los riesgos de seguridad de la información y ciberseguridad.~~ ~~e) Participar en la implementación de los controles y mejoras de seguridad de la información y ciberseguridad que estén relacionados a sus funciones.~~ ~~f) Gestionar y liderar la implementación de planes de tratamiento para el aseguramiento de activos de información.~~ ~~g) Gestionar y comunicar la ejecución de las acciones correctivas o de mejora bajo su responsabilidad.~~ ~~h) Reportar y gestionar oportunamente incidentes de seguridad de información y ciberseguridad.~~ ~~i) Administrar toda documentación relacionada a la gestión de seguridad de la información y ciberseguridad de su competencia.~~ ~~j) Facilitar información de la unidad orgánica bajo su competencia para la medición de indicadores, auditorías o revisiones del SGSI-C.~~	**f) Promover la conformación y adecuada operación del Equipo de respuestas ante incidentes de seguridad de la información.** **g) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.** **h) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.** **i) Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.** **j) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.** **k) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la CPMP e informarlos a la Gerencia General.** **l) Informar a la Gerencia General acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI-C, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la CPMP, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital. Formula y propone indicadores clave de desempeño del SGSI.** **m) Coordinar con el CNSD y con el Comité del SGSI las acciones de sensibilización y capacitación para los funcionarios y colaboradores de la CPMP sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital, gobierno digital, uso de plataformas interoperables, ética en tecnología de información, protección de datos personales.** **n) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la CPMP a fin de fortalecer la confianza en el entorno digital.** **o) Coordinar con el CSIRT el registro y notificación obligatoria al CNSD de cualquier incidente de seguridad digital, e intercambio de información en materia de seguridad digital.** **p) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.** **q) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las UUOO de la CPMP su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información. **r) Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la Gerencia de Informática cuando ésta adquiera, tercerice o desarrolle software o implemente otro tipo de soluciones tecnológicas.** **s) Coordinar con la Gerencia de Informática, cuando corresponda, en los temas relativos a sus responsabilidades.** **t) Otras responsabilidades afines que le sean asignadas por la Gerencia General.** **9.1.7 Gerente de Riesgos y Desarrollo** **a) Velar por una adecuada gestión de seguridad de la información y ciberseguridad, que promueva el alineamiento de la toma de decisiones de la entidad con el apetito de riesgo operacional.** **b) Verificar periódicamente que las políticas, procedimientos, metodologías y demás normas internas relacionadas con la gestión de seguridad de la información y ciberseguridad sean consistentes con el tamaño, la complejidad de las operaciones y la estructura de la CPMP.** **c) Informar a la Gerencia General y al Comité de Riesgos, los resultados de la gestión integral de riesgos relacionados al SGSI-C emitidos por el Comité del SGSI-C.** **d) Comunicar, a la Gerencia General y al Comité de Riesgos, el desempeño y los acuerdos adoptados emitidos por el Comité del SGSI-C.** **e) Comunicar a la Gerencia General y al Comité de Riesgos, los resultados de las auditorías internas y/o externas de seguridad de la información y los indicadores clave emitidos por el Comité del SGSI-C.** **f) Enviar a través de la extranet de la SBS, el informe electrónico anual (a través del aplicativo IG-ROp) de la gestión de seguridad de la información y ciberseguridad dentro de los plazos establecidos según Resolución SBS Nº 2116-2009.** **9.1.8 Jefe de Departamento de Planeamiento y Organización** **a) Orientar al OSCD para asegurar una adecuada articulación con el plan estratégico y el plan operativo institucional orientada a implementar, operar, mantener y mejorar el SGSI-C.** **9.1.9 Jefe de Departamento de Riesgos Operacionales** **a) Participar en el diseño y permanente actualización de las Normas y Procedimientos del Sistema de Gestión de Seguridad de la Información, en coordinación con el OSCD.** **b) Desarrollar la metodología para gestión de seguridad de la Información y ciberseguridad, en coordinación con el OSCD.**	

<table>
<tr><th colspan="4">MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 “POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD”</th></tr>
<tr><th>SECCIÓN</th><th>DCD N° 10-2021</th><th>MODIFICACIÓN</th><th>COMENTARIOS</th></tr>
<tr><td></td><td>~~5.4. Conformación del Comité Especializado en Seguridad de la Información y Ciberseguridad~~

~~El Comité Especializado en Seguridad de la Información y Ciberseguridad está presidido por el Gerente de Riesgos y Desarrollo y está conformado por:~~

<table><tr><th>~~Titular~~</th><th>~~Alterno~~</th></tr><tr><td>~~Gerente de Riesgos y Desarrollo~~</td><td>~~Jefe de Departamento de Riesgos Financieros~~</td></tr><tr><td>~~Oficial de Seguridad de la Información y Ciberseguridad (Jefe de Departamento de Riesgos Operacionales)~~</td><td>~~Analista de Riesgos Operacionales~~</td></tr><tr><td>~~Gerente de Informática~~</td><td>~~Jefe de Departamento de Desarrollo y Mantenimiento de Sistemas de Información~~</td></tr><tr><td>~~Gerente de Administración y Finanzas~~</td><td>~~Jefe de Departamento de Logística~~</td></tr><tr><td>~~Jefe de Departamento de Infraestructura y Seguridad Informática~~</td><td>~~Jefe de Departamento de Desarrollo y Mantenimiento de Sistemas de Información~~</td></tr></table>
~~Nota: Se convocará la participación de la Gerencia Legal y Cumplimiento, para el apoyo legal en el manejo de incidentes de ciberseguridad.~~</td><td>c) Identificar las necesidades de capacitación y difusión para una adecuada gestión de seguridad de la información y ciberseguridad en coordinación con el OSCD y presentarlas al Comité del SGSI.

d) Promover y coordinar con el OSCD, la ejecución de todas las actividades relacionadas con el proceso de implementación, operación, seguimiento y mejora continua del SGSI-C.
e) Realizar la supervisión, actualización y cumplimiento de la presente directiva, en coordinación con el OSCD.

f) Evaluar los riesgos del SGSI-C ante cambios significativos a nivel de procesos y tecnología en coordinación con el OSCD.

g) Elaborar el informe electrónico anual (a través del aplicativo IG-ROp) de la gestión de seguridad de la información y ciberseguridad dentro de los plazos establecidos (a más tardar el 31 de marzo del año siguiente al año del reporte, según Resolución SBS Nº 2116-2009).

9.1.10 Equipo de respuestas ante incidentes de seguridad digital (CSIRT)

El Equipo de respuestas ante incidentes de seguridad digital (CSIRT: Computer Security Incident Response Team): Es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza, su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros. Es un equipo técnico conformado principalmente por especialistas en seguridad de las tecnologías de la información o informática.

El Equipo de respuestas ante incidentes de seguridad digital está conformado por:

<table><tr><th>Rol</th><th>Titular</th><th>Suplente</th></tr><tr><td>Coordinador del CSIRT</td><td>Gerente de Informática</td><td>El/La colaborador(a) que asuma la encargatura</td></tr><tr><td>Gestor de Incidentes</td><td>Especialista en Seguridad de Información</td><td>Analista Funcional - DDMSI</td></tr><tr><td>Gestor de Redes y Comunicaciones/Gestor de Infraestructuras Digitales</td><td>Analista de Infraestructura - DISI</td><td>Asistente de Soporte Técnico I - DDMSI</td></tr><tr><td>Oficial de Seguridad y Confianza Digital</td><td>Jefe de Departamento de Infraestructura y Seguridad Informática</td><td>El/La colaborador(a) que asuma la encargatura</td></tr><tr><td>Gestor de Riesgos de Seguridad de la Información</td><td>Jefe de Departamento de Riesgos Operacionales</td><td>El/La colaborador(a) que asuma la encargatura</td></tr></table>
Es el encargado de gestionar la contención, respuesta y recuperación ante incidentes de seguridad digital para la protección de los activos de información frente a amenazas que atenten o comprometan la seguridad digital.

Sus funciones se encuentran establecidas en el artículo 2º de la Resolución de Gerencia General Nº 011-2024/CPMP-GG.

9.1.11 Gerente de Informática

a) Informar al OSCD todo incidente de seguridad digital crítico que afecte lo procesos misionales y servicios que brinda la CPMP de forma inmediata.</td><td></td></tr>
</table>

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		b) Articular con el OSCD la implementación de controles de seguridad de la información y coordina con el CSIRT la gestión de incidentes de seguridad digital. **c) Planificar, desarrollar, implantar y gestionar el sistema de información, infraestructura tecnológica, telecomunicaciones y estadísticas, que brinden el soporte de las funciones, desarrolladas por las diferentes UUOO estableciendo políticas, estándares y procedimientos.** **d) Colaborar con el OSCD y con el Jefe de Departamento de Riesgos Operacionales integrar las mejores prácticas de seguridad en la gestión de Tecnología de la Información y Comunicaciones.** **9.1.12 Gerente de Administración y Finanzas** **a) Asegurar la disponibilidad de recursos financieros para implementar y mantener las políticas de seguridad de la información y ciberseguridad.** **b) Gestionar el presupuesto y controlar los costos asociados a la gestión de seguridad de la información y ciberseguridad.** **c) Asegurar el cumplimiento de las normativas financieras relacionadas con la seguridad digital.** **d) Proveer el apoyo administrativo necesario para la implementación y mantenimiento asociados a la gestión de seguridad de la información y ciberseguridad.** **9.1.13 Jefe de Departamento de Presupuesto** **a) Responsable de conducir el proceso presupuestario de la CPMP, incluyendo las modificaciones orientadas para implementar, operar, mantener y mejorar el SGSI-C.** **b) Orientar al OSCD para asegurar una adecuada articulación con el presupuesto de la CPMP.** **9.1.14 Oficial de Gobierno de Datos** **Las responsabilidades del Oficial de Gobierno de Datos de la CPMP se encuentran establecidas en la Directiva Nº 001-2022-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Gobierno de Datos aprobada con Resolución de Secretaría de Gobierno y Transformación Digital Nº 001-2022-PCM/SGTD y sus modificatorias. Sus funciones se encuentran establecidas en el artículo 3º de la Resolución de Gerencia General Nº 031-2024/CPMP-GG.** **9.1.15 Oficial de Datos Personales** **a) La designación, responsabilidades y perfil del ODP se establecen en la directiva RD 100-JUS/DGTAIPD.** **b) Informar y asesorar al titular del banco de datos personales, al responsable del tratamiento y al personal que intervenga en dicho tratamiento, respecto de las obligaciones que le corresponden conforme a la normativa sobre protección de datos personales en la CPMP.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		c) Vigilar y evaluar el cumplimiento de la normativa vigente y de las políticas internas del titular del banco de datos o del encargado del tratamiento, incluyendo la asignación de responsabilidades, la capacitación del personal involucrado y la realización de auditorías en materia de protección de datos personales. **d) Actuar como punto de contacto y cooperar, en lo que resulte pertinente, con la Autoridad Nacional de Protección de Datos Personales para el ejercicio de sus funciones y atribuciones.** **9.1.16 Propietario de la Información o activos de información/Dueños de los procesos** **a) Apoyar en la gestión de riegos e implementación de controles de seguridad de la información identificados en sus ámbitos de competencia, así como también coadyuvan en la gestión de incidentes según corresponda.** **b) Clasificar la información de los procesos bajo su responsabilidad y establecer su nivel de criticidad y disposición final. A su vez deberá determinar cuando la información ya no es necesaria y el tiempo de retención en coordinación con su respectiva Gerencia.** **c) Participar en la identificación y gestión de los riesgos de información asociados con los activos.** **d) Ser responsable por la calidad, consistencia y disponibilidad de los datos, por lo que deberá tomar medidas para minimizar el riesgo por pérdida o exposición de la seguridad de la información bajo su responsabilidad.** **e) Autorizar accesos a la información y ratificar periódicamente las decisiones sobre los mismos, así como dar cumplimiento las disposiciones sobre accesos a los sistemas de información.** **f) Revisar la clasificación de la información y los accesos de los procesos bajo su responsabilidad periódicamente.** **g) Apoyar en la gestión de los incidentes de seguridad de la información según corresponda.** **9.1.17 Custodios de la Información** **a) Preservar y proteger la información que le ha sido confiada en custodia.** **b) Cumplir con las Políticas de Seguridad de la Información del CPMP y los especificados por el propietario de la información.** **c) Realizar conjuntamente con los propietarios de la información, pruebas de contingencia y asegurar que todos los empleados y/o usuarios involucrados conozcan sus responsabilidades.** **9.1.18 Personal de la CPMP** **a) Cumplir las Políticas de Seguridad de la Información de la CPMP y documentos relacionados a la Seguridad de la Información de la CPMP.**	

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		b) Asegurar la protección de los activos de la información involucrados en las labores que realizan. **c) Informar a su inmediato superior, al OSCD y al Departamento de Riesgos Operacionales sobre la identificación de deficiencias e incidentes en materia de seguridad de la información.**	
10. ANALISIS DE RIESGOS		**El análisis de riesgos permite determinar las vulnerabilidades de los activos de información de la CPMP y asimismo clasificarlos por su criticidad. También facilita la implementación de controles para tratar los riesgos asociados a los activos de información.**	Se incorporó el Análisis de Riesgos.
11. INFORMACION A LA SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP (SBS)	~~5.5 Información a la Superintendencia de Banca, Seguros y AFP (SBS)~~ ~~5.5.1.~~ Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por ~~el~~ Reglamento para la Gestión del Riesgo Operacional, la CPMP ~~deberá~~ incluir información sobre la gestión de la seguridad de la información y ciberseguridad. ~~5.5.2.~~ La CPMP informa a la SBS la ocurrencia de un evento de interrupción significativa de operaciones, en cuanto tome conocimiento y dentro de un plazo máximo de un (1) día hábil. Para tal efecto, se entiende como evento de interrupción significativa de operaciones un evento que implique cualquiera de las siguientes situaciones: ~~a)~~ La suspensión en la entrega de los productos y servicios priorizados por un tiempo mayor a los respectivos TOR~~; o~~ ~~b)~~ La activación del plan de gestión de crisis (la función de activación (ejecución) del "Plan de Gestión de Crisis" le corresponde al Equipo de Gestión de Crisis, establecido en ~~el numeral 4.4.3. de~~ la ~~D~~irectiva de Consejo Directivo "Políticas y Objetivos de Continuidad del Negocio").	**11.1.** Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por **la SBS a través de su** "Reglamento para la Gestión del Riesgo Operacional", la CPMP **debe** incluir información sobre la gestión de seguridad de la información y ciberseguridad. **11.2.** La CPMP informa a la SBS la ocurrencia de un evento de interrupción significativa de **las** operaciones, en cuanto tome conocimiento y dentro de un plazo máximo de un (1) día hábil. Para tal efecto, se entiende como evento de interrupción significativa de **las** operaciones**, a** un evento que implique cualquiera de las siguientes situaciones: **11.2.1.** La suspensión en la entrega de los productos y servicios priorizados por un tiempo mayor a los respectivos TOR**.** **11.2.2.** La activación del plan de gestión de crisis (la función de activación (ejecución) del "Plan de Gestión de Crisis" le corresponde al Equipo de Gestión de Crisis, establecido en la **d**irectiva "Políticas y Objetivos de Continuidad del Negocio").	Se actualizó la Información a la Superintendencia de Banca, Seguros y AFP (SBS).
12. CUMPLIMIENTO Y CONFORMIDAD		**El cumplimiento de la Política de Seguridad de la Información es obligatorio para las UUOO de la CPMP. En el caso de incumplimiento, la CPMP aplicará a los responsables las medidas necesarias según el Reglamento Interno de Trabajo de la CPMP.**	Se incorporó el Cumplimiento y Conformidad.
13. VIGENCIA		**La Política de Seguridad de la Información y Ciberseguridad de la CPMP entra en vigencia a partir de su aprobación y deberá ser revisada, y actualizada en caso corresponda, una vez al año o en caso de producirse modificaciones a las normas legales o cambios significativos en la organización o en los procesos que afecten la seguridad de la información.**	Se incorporó la Vigencia.
14. MONITOREO, SEGUIMIENTO Y EVALUACION		**La Política de Seguridad de la Información y Ciberseguridad de la CPMP, será monitoreada en forma permanente con la revisión de los controles de seguridad, de acuerdo a lo establecido en el numeral 8. Políticas Específicas de Seguridad de la Información.** **El seguimiento a la Política de Seguridad de la información y Ciberseguridad se realizará con la medición del cumplimiento de los objetivos de seguridad de la información a través de los indicadores y metas del SGSI.** **La evaluación de la Política de Seguridad de la Información se realizará en forma anual, asimismo,**	Se incorporó el Monitoreo, Seguimiento y Evaluación.

MODIFICACIONES EFECTUADAS A LA DIRECTIVA DE CONSEJO DIRECTIVO DCD N° 10-2021 "POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD"			
SECCIÓN	**DCD N° 10-2021**	**MODIFICACIÓN**	**COMENTARIOS**
		se informará del progreso de la implementación del SGSI.	
15. DISPOSICIONES COMPLEMENTARIAS	Quedan sin efecto la Directiva de Consejo ~~Directivo DCD Nº 12-2019~~ y otras disposiciones que contravengan la presente directiva.	Quedan sin efecto la Directiva de Consejo Directivo **DCD Nº 10-2021** y otras disposiciones que contravengan la presente directiva.	Se actualizó las Disposiciones Complementarias.

Nota: Para la elaboración del cuadro comparativo, se ha considerado lo siguiente:
- El orden de la comparación es con base en la nueva propuesta.
- Negrita: Lo que se ha agregado en la nueva propuesta.
- Tachado: Lo que se ha retirado en la nueva propuesta.