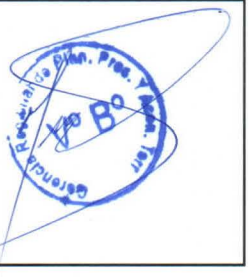
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

GOBIERNO REGIONAL DE MADRE DE DIOS

Código:	
Versión:	V 1.0
Fecha de versión:	30/06/2020
Elaborado por:	Ing. Edwin Joel Holgado Canal
Aprobado por:	Líder y Comité de Gobierno Digital del GOREMAD
NOMBRE DEL ARCHIVO:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE MADRE DE DIOS
Nivel de confidencialidad:	Media

REVISIONES SEGÚN RESOLUCION EJECUTIVA REGIONAL N°106-2020-GOREMAD/GR

Fecha	Versión	Miembro del Comité de Gobierno Digital	V° B°
	V 1.0	**GOBERNADOR REGIONAL**	
	V 1.0	**LÍDER DE GOBIERNO DIGITAL**	
	V 1.0	**RESPONSABLE DEL ÁREA DE INFORMÁTICA**	
	V 1.0	**RESPONSABLE DE LA OFICINA DE RECURSOS HUMANOS**	

	V 1.0	**RESPONSABLE DE OFICINA REGIONAL DE ASESORÍA JURÍDICA**	
	V 1.0	**OFICIAL DE SEGURIDAD DE INFORMACIÓN**	
	V 1.0	**RESPONSABLE DE LA GERENCIA REGIONAL DE PLANEAMIENTO, PRESUPUESTO Y ACONDICIONAMIENTO TERRITORIAL**	

GOBIERNO REGIONAL
MADRE DE DIOS
Caminemos Juntos

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

DEL GOBIERNO REGIONAL DE MADRE DE DIOS

OFICINA DE UNIDAD DE INFORMÁTICA
SUB GERENCIA DE DESARROLLO INSTITUCIONAL E INFORMÁTICA

INDICE

1. ANTECEDENTES

En la nueva era digital que nos encontramos, la información se ha convertido en el activo más valioso para las empresas y entidades, en la actualidad los datos se constituyen como un elemento esencial para generar competitividad. La seguridad de la información protege a esta, de un amplio rango de amenazas para asegurar la continuidad de las actividades de la Entidad y minimizar daños, y esto se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, normas, procedimientos, estructuras organizativas, herramientas informáticas, entre otros.

La Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros a dispuesto a través de la Resolución Ministerial N.º 004-2016-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001 :2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

2. OBJETIVO

El presente documento define y establece los principios que conforman la Política de Seguridad de la información del Gobierno Regional de Madre de Dios, para garantizar en la mayor medida de posible la confidencialidad, disponibilidad de sus sistemas informáticos, de la comunicación y de los servicios que proporciona al ciudadano y los propios usuarios del Gobierno Regional de Madre de Dios.

Asimismo, debe constituirse en parte de la cultura organizacional de la institución, establecer el compromiso del Gobierno Regional de Madre de Dios con la Seguridad de la información, definiendo los objetivos y criterios básicos para el tratamiento de la misma, sentando los pilares del marco normativo de la seguridad de esta institución y la estructura organizativa y de gestión que velara por su cumplimiento.

3. ALCANCE

La presente política es aplicable a toda la información y activos de la información del Gobierno Regional de Madre de Dios que la soportan, incluyendo todas las personas y terceras empresas o instituciones que de una forma u otra acceden a ellos, independientemente de su situación física, dentro o fuera de las instituciones de la institución. Afecta por lo tanto y son de aplicación directa a todo el sistemas, aplicaciones, servicios, información y ubicaciones del Gobierno Regional de Madre de Dios, incluyendo el personal implicado en su tratamiento.

Las Políticas de Seguridad expuestas en el presente documento sirve de referencia, en ningún momento pretenden ser una política absoluta, pudiendo estar sometida a cambios realizables en cualquier momento, siempre y cuando se tenga presentes los objetivos de seguridad marcados por el Gobierno Peruano.

El presente documento comprende las siguientes políticas específicas:

Política de Seguridad de la Información.
Política de Organización de la Seguridad de la Información.
Política de Seguridad Relativa a los Recursos Humanos.
Política de Gestión de Seguridad de Activos de Información.
Política de Control de Accesos.
Política de Seguridad Física y del Entorno.
Política de Seguridad de las Operaciones.
Política de Seguridad de las Comunicaciones.
Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.
Política de Relación con Proveedores.
Política de Gestión de Incidentes de Seguridad de la Información.
Política de Continuidad de Seguridad de la Información.
Política de Cumplimiento.

4. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27815, Ley del Código de Ética de la Función Pública.
- Ley Nº 29733, Ley de Protección de Datos Personales.
- Decreto Supremo Nº 109-2012-PCM, que aprueba la Estrategia para la Modernización de la Gestión Pública.
- Resolución Ministerial Nº 092-2012-PCM, que aprueba el Código de Ética del Ministerio de Desarrollo e Inclusión Social.
- Resolución N° 129-2014/CNB-INDECOPI, que aprueba 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"
- Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso Obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

5. LINEAMIENTOS

5.1. Responsabilidades Generales

Los Lineamientos de Seguridad de la Información son de cumplimiento obligatorio para todos los servidores designados o asignados bajo cualquier régimen laboral o modalidad contractual, considerando a los proveedores de servicio bajo contrato que tengan acceso o que desarrollen, adquieran o usen sistemas de información.

5.2. Sanciones por Incumplimiento

El GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados se reservan el derecho de tomar medidas administrativas disciplinarias de los servidores que incumplan con lo dispuesto en los Lineamientos de Seguridad de la Información conforme a las disposiciones señaladas en los documentos normativos de la Entidad, sin perjuicio de las acciones civiles y/o penales que pudieran corresponder.

5.3. Objetivos de Seguridad de la Información

En el Gobierno Regional de Madre de Dios define los siguientes Objetivos de Seguridad:

- Proteger los recursos de información y las tecnologías para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de los mismos.

- Minimizar la probabilidad de ocurrencia de incidentes, así como reducir su frecuencia y duración de los mismos, en especial los incidentes a través de internet y de los sistemas de información de la entidad.

- Mantener la disponibilidad de la información y los sistemas de información que soportan los procesos del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados que garantiza que las Entidades o personas debidamente autorizadas tengan acceso a la información cuando lo requieran.

- Establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados.

5.4. Política de Seguridad de la Información

5.4.1. Objetivos

Proporcionar orientación y apoyo a la gestión para la seguridad de la información en concordancia con los requisitos de la entidad y las leyes y regulaciones relevantes.

5.4.2. Política

a) Políticas de Seguridad de la Información:

i. EL GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados deben elaborar documentos normativos de Seguridad de la Información a fin proteger la información de la Entidad, de considerarlo pertinente.

ii. Los documentos normativos de Seguridad de la Información deben estar alineados a la estrategia de la institución, las regulaciones, leyes, normas y amenazas a que estén sujetos como Entidad.

iii. El Comité de Gestión de Seguridad de la Información del GOBIERNO REGIONAL MADRE DE DIOS y sus órganos desconcentrados debe monitorear el cumplimiento de la presente política, periódicamente.

b) Revisión de Políticas de Seguridad de la Información:

El GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados debe revisar por lo menos una vez al año, cuando la Entidad lo determina o cuando se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia, en un contexto de mejora continua.

5.5. Política de Organización de la Seguridad de la Información

5.5.1. Objetivos

Instaurar un marco de referencia de la gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de cada unidad orgánica y órgano desconcentrado.

5.5.2. Política

a) Roles y Responsabilidades:

El GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados debe definir roles y responsabilidades de Seguridad de la Información para la protección de los activos de información, la gestión de riesgos de Seguridad de la Información y la aceptación de los riesgos residuales.

b) Segregación de Funciones:

El GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados debe segregar funciones para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.

c) Seguridad de la Información en la gestión de proyectos:

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DIOS o la que haga de sus veces en sus órganos desconcentrados debe integrar la seguridad de la información en el proceso de gestión de proyectos de la Entidad, para garantizar que

los riesgos de seguridad de la información sean identificados y tratados pertinentemente.

d) Equipos Portátiles:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DIOS, o la que haga sus veces en los órganos desconcentrados, debe elaborar y mantener vigente un proceso de instalación y configuración de las aplicaciones y sistemas en los equipos portátiles, el cual define todas las actividades y responsabilidades que desempeña el personal de la Oficina de Unidad de Informática, así como el personal usuario y proveedores de servicio bajo contrato respecto del uso correcto, administración, configuración de seguridad, respaldo y soporte de los equipos portátiles de la Entidad.

ii El proceso de instalación y configuración de las aplicaciones y sistemas en los equipos portátiles, debe ser responsabilidad de la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DIOS, o la que haga sus veces en los órganos desconcentrados.

iii. El servidor del GOBIERNO REGIONAL DE MADRE DIOS y sus órganos desconcentrados deben proteger sus equipos portátiles donde se haya instalado o configurado la aplicación o sistema institucional, no debiendo entregarlos a otra persona, en particular.

iv. El GOBIERNO REGIONAL DE MADRE DIOS a través de la Oficina de Unidad de Informática, o la que haga sus" veces en los órganos desconcentrados, debe mantener una administración centralizada de las características de los dispositivos portátiles y las aplicaciones instaladas en ellos que procesan o almacenan información crítica.

5.6. Política de Seguridad Relativa a los Recursos Humanos

5.6.1. Objetivo

Asegurar una correcta gestión de los recursos humanos en el GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados, siendo los servidores parte fundamental del resguardo de la Seguridad de la Información.

5.6.2. Política

a) Antes del empleo

i. La Oficina de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe verificar los antecedentes laborales y las competencias requeridas para el puesto.

ii. La Oficina de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, deberán establecer en los acuerdos contractuales de empleo, las cláusulas de confidencialidad respecto a la Seguridad de la Información, cláusula respecto a las leyes de derecho de autor o protección de datos, según corresponda.

b) Durante el Empleo

i. La Oficina de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe comunicar a los servidores del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, sus responsabilidades con respecto a la Seguridad de la Información, siendo responsables de la Seguridad de la Información a la que tienen acceso, según las funciones o actividades que realicen.

ii. La Oficina de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados en su interés por proteger su información y los recursos de procesamiento de la misma debe establecer su compromiso de la Entidad, a través de programas de inducción para los nuevos servidores, así como, actualizaciones regulares sobre Políticas y procedimiento.

iii. La Oficina regional de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe comunicar a la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, cuando corresponda, el inicio, rotación y fin del vínculo laboral de los servidores para el otorgamiento de acceso a los Sistemas de Información.

iv. La Oficina regional de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados puede iniciar procesos disciplinarios y/o acciones legales pertinentes a los servidores que incumplan las

Políticas de Seguridad de la Información y Normativas de Seguridad de la Información establecidos.

c) Después del Empleo

La Oficina regional de Personal del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, debe comunicar a la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, cuando corresponda, la finalización del vínculo laboral del servidor al día siguiente de tomado conocimiento de la culminación del vínculo laboral a fin de realizar la desactivación de los accesos a los Sistemas de Información y demás recursos.

5.7. Política de Gestión de Seguridad de Activos de Información

5.7.1. Objetivos

Identificar los activos de información de la Entidad y definir las responsabilidades de protección apropiadas.

5.7.2. Política

a) Inventario de Activos de Información

La Oficina Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los órganos desconcentrados, debe mantener un inventario de activos de información actualizada y revisada periódicamente, asimismo, dicho inventario debe contar con un propietario de activo de información que es responsable de la gestión del activo de información durante todo su ciclo de vida.

b) Uso de Activos de Información

i. Los servidores deben usar los activos de información para los fines y objetivos del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados, de acuerdo con los documentos normativos, la política, y procedimientos que se definan, y considerando criterios de buen uso.

ii. En el marco de las relaciones que el GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados establezca con terceros, los convenios, contratos y órdenes, según corresponda, consignarán cláusulas o disposiciones referidas a la confidencialidad de la información que se entregue o a la que tengan acceso, así como sobre la cesión de derechos de corresponder.

iii. Todos los órganos y unidades orgánicas del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo los lineamientos de seguridad de la información que deben mantenerse alineados con la normatividad vigente del estado peruano.

c) Retorno de Activos de Información

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o quien haga sus veces en los órganos desconcentrados debe establecer el procedimiento para el retorno de los activos de información de la Entidad de los servidores que dejan de laborar en la Entidad.

d) Clasificación de la información

i. Los propietarios de activos de información son responsables de clasificar la información que manejan en cada proceso o proyecto, de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.

ii. Los propietarios de los activos de información deberán etiquetar la información según la clasificación realizada, y que sea conforme a los lineamientos que se establezcan en la Entidad.

	DEFINICIÓN	EJEMPLO
Información Confidencial	Aquella información que es considerada como confidencial de acuerdo a lo establecido en el Texto Único Ordenado de la Ley N° 27806 Ley de Transparencia y Acceso a la Información	Incluye a los datos de carácter personal y sensible de servidores, clientes y demás personas naturales sobre las que el GOBIERNO REGIONAL DE MADRE DE DIOS efectúa algún tratamiento de información para un fin determinado declarado como banco de datos personales. Este tipo de información debe estar protegido del acceso no y autorizado.

Información Pública	Aquella información que es de acceso público de acuerdo a lo establecido: en el Texto Único Ordenado de la Ley N°27806, Ley Transparencia y Acceso a la Información Pública El GOBIERNO REGIONAL DE MADRE DE DIOS cataloga esta. información en Información Publicada e Información de Uso Interno	Información Publicada: aquella que de acuerdo a la normativa nacional vigente se encuentra publicada en el de Portal de Transparencia estándar. información de Uso Interno: aquella información pública que no se encuentra en la Intranet de la Entidad

e) Gestión de Medios Removibles:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los órganos desconcentrados, debe establecer el procedimiento para la gestión de medios removibles considerando las labores realizadas por los servidores de acuerdo a la necesidad de uso.

ii. La Oficina de Tecnologías de la Información del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los órganos desconcentrados, debe establecer controles a todo tipo de transferencia de información por medios físicos, manteniendo lineamientos para los servicios de mensajería y transporte de información en distintos soportes.

5.8. Política de Control de Accesos

5.8.1. Objetivo

a) Garantizar que la autorización de acceso a la información se realice de acuerdo con las atribuciones, funciones y/o tareas a desarrollar por el servidor.

b) Controlar los accesos a la información.

c) Prevenir accesos no autorizados a los sistemas de información y a los servicios de red.

5.8.2. Política

a) Requerimientos para el control de accesos:

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe establecer que todos los accesos a los recursos de información deben basarse en la necesidad y rol del usuario, tomando en cuenta los siguientes aspectos:

i. Los requerimientos de seguridad de cada una de las aplicaciones.

ii. Identificación de toda la información relacionada a las aplicaciones y los riesgos a la está expuesta.

iii. Uso de perfiles de usuarios estandarizados definidos según roles.

iv. Revisión periódica de los controles de acceso.

v. Revocación de los derechos de acceso

b) Gestión de acceso del personal:

i. Con el propósito de impedir accesos no autorizados a los recursos de información, La Oficina de Unidad de Informática de la Información del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe establecer procedimientos formales para asignar los derechos de acceso a los sistemas.

ii. Los responsables de las unidades orgánicas son los encargados de autorizar el acceso del servidor a su cargo, a los recursos de tecnologías de información, conforme al procedimiento que se establezca para tal efecto.

iii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe asignar un usuario y password que identifique única y exclusivamente al servidor para el uso de los recursos informáticos, ya sea de forma temporal o permanente.

iv. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe definir normas y procedimientos de control a nivel de sistema operativo de red, de manera que no se compartan identificadores entre

diferentes usuarios ni pueda detectarse la duplicidad de sesiones de usuarios.

v. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe establecer, en sus respectivos ámbitos, las normas y procedimientos para la asignación y cambio de contraseñas. Al respecto, se informa al servidor sobre lo siguiente:

- Debe seleccionar secuencias de caracteres o palabras claras y fáciles de recordar. Se debe considerar una longitud mínima de 6 caracteres considerando un número, un carácter alfanumérico y caracteres especiales cuando menos.

- No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, teléfono, etc.).

- Cada servidor es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que, mediante su uso, terceras personas pueden realizar.

- Las contraseñas son estrictamente personal e intransferible y el servidor es responsable de mantener su confidencialidad.

c) Control de acceso a las redes informáticas:

i. El acceso a los recursos de red, internos y externos, debe ser controlado por La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, de manera que el servidor no comprometa la seguridad de los activos de información.

ii. Para la seguridad en las redes informáticas, se deben tener en cuenta los siguientes aspectos:

- Lineamientos de uso de la red.
- Segmentación de redes.
- Control de conexiones a redes en base a la política. Controles de enrutamiento de redes.

d) Control de acceso a los sistemas operativos:

i. El acceso a los sistemas operativos de las estaciones de trabajo del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe

ser debidamente controlado por la Oficina de Tecnologías de la Información del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, a fin de evitar accesos no autorizados a recursos o información.

ii. Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:

- Identificación automática de estación de trabajo.
- Procedimientos de inicio de sesión seguros.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.

e) Control de acceso a las aplicaciones:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los Programas Sociales, debe establecer los lineamientos de control de accesos a la información y a las aplicaciones, restringiendo para uso exclusivo del personal debidamente autorizado; asimismo, revisar periódicamente los accesos concedidos, revocando los derechos cuya vigencia de autorización haya caducado.

ii. Se deben aislar los sistemas identificados con información sensible, asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos.

f) Conexiones externas:

En cualquier caso, para el acceso remoto (todo acceso a la información del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados fuera del centro de trabajo) se debe utilizar la tecnología y acceso seguro (SSL-VPN) y su uso debe ser autorizado solo en caso de ser necesario por el jefe del órgano o unidad orgánica la Oficina de Unidad de Informática, o la que haga sus veces en los órganos desconcentrados, con el conocimiento del Oficial de Seguridad de la Información.

5.9. Política de Seguridad Física y del Entorno

5.9.1. Objetivos

Tomar las medidas necesarias para evitar el acceso físico no autorizado, los daños e interferencia a la información de la Entidad y a los recursos de tratamiento de la información.

5.9.2. Política

a) El servidor del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados que atienda a personas externas a la Entidad (incluyendo proveedores) debe asegurar que los datos de todas las visitas de personas externas a la Entidad quedan anotados en el registro de visitas, para su publicación respectiva en el portal de transparencia.

b) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe implementar controles Biométricos al Centro de Datos para su debida protección.

c) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, debe establecer una clasificación de las áreas para definir el nivel de seguridad de las mismas, las cuales se describen a continuación:

AREA	DESCRIPCION
Restringida	Son zonas seguras donde la información que se genera, trata o almacena es crítica para la Entidad. Los accesos a estos despachos son controlados
Común	Son zonas de uso común para el servidor del GOBIERNO REGIONAL DE MADRE DE DIOS
Pública	Son zonas que son de utilización pública y de recepción de personas externas a la Entidad

d) Toda persona externa al GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados puede acceder a las áreas definidas como restringidas, siempre que cuente con la autorización respectiva del jefe del órgano o unidad orgánica y debe estar siempre acompañado por un servidor de la Entidad.

e) El servidor del GOBIERNO REGIONAL DE MADRE DE DIOS y en sus órganos desconcentrados debe portar en todo momento su fotocheck para su debida identificación.

f) Los visitantes que ingresan a las instalaciones del GOBIERNO REGIONAL DE MADRE DE DIOS y en sus órganos desconcentrados deben portar en todo momento su pase de visita.

g) El personal de GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados debe seguir el procedimiento establecido de Gestión de Bienes Muebles establecido por la Oficina de Control Patrimonial para el retiro de un equipo de cómputo.

h) Todos los equipos de cómputo que ingresan al GOBIERNO REGIONAL DE MADRE DE DIOS y a sus órganos desconcentrados debe ser previamente registrados por el personal de la Unidad de Vigilancia responsable.

i) El GOBIERNO REGIONAL DE MADRE DE DIOS y a sus órganos desconcentrados a través de los Órganos u Unidades Orgánicas de acuerdo a su responsabilidad debe de implementar medidas de protección contra amenazas externas y ambientales, dichas medidas de protección, debe incluir:

- Controles de acceso y seguridad física
- Detectores de humo. Extintores
- Sistema de alimentación ininterrumpida (UPS)
- Sistema de puesta a Tierra
- Sensores de aniego
- Grupo Electrógeno
- Pararrayos (Unidades ubicadas en las zonas que el clima lo requiera)

j) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, debe proteger los equipos de Tecnologías de la Información de fallas por falta de suministro de energía y otras anomalías eléctricas.

k) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, debe proteger el cableado de la red de comunicaciones y suministro de energía para evitar intercepción o daño.

l) El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información, debe contar con un sistema de pozo a tierra, el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.

m) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe mantener un programa de mantenimiento de los equipos de Tecnologías de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y sistemas de detección fuego del Data Center, a fin de garantizar la continuidad de los servicios.

n) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe implementar una Política de Escritorio

Limpio y Pantalla Limpia, a fin de evitar el acceso no autorizado y el uso indebido de la información.

5.10. Política de Seguridad de las Operaciones

5.10.1. Objetivo

Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras

5.10.2. Política

a) Procedimientos Operativos Documentados:

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, debe documentar procesamientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente, asimismo, estos deberán estar a disposición de los servidores autorizados.

b) Gestión de Cambios:

I. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los Programas Sociales, debe mantener un registro de control de cambios de los sistemas, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso, a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.

II. Todos los cambios deben ser solicitados a la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, por el propietario de la Información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado, se revertirá al estado anterior al cambio.

c) Gestión de la Capacidad:

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe garantizar la capacidad de los recursos a fin de asegurar el desempeño requerido de los Sistemas de Información.

d) Separación de Entornos:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe separar entornos de desarrollo, pruebas y producción a fin de prevenir riesgos de acceso no autorizado o cambios al entorno operativo.

ii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe definir y documentar procedimientos para pases de desarrollo a producción, asimismo, el entorno de pruebas debe ser en lo posible, igual al ambiente de producción en lo referido a recursos de Tecnologías de información.

e) Protección contra Software Malicioso:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadoras portátiles, estaciones de trabajo, etc.

ii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo y que éste se encuentre actualizado. Asimismo, debe garantizar que el sistema operativo y los aplicativos de oficina cuenten con las últimas actualizaciones de seguridad (parches).

iii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, es responsable de la renovación de licencias de software, y debe definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso ilegal de software.

iv. El Software utilizado por el GOBIERNO REGIONAL DE MADRE DE DIOS y en los órganos desconcentrados debe ser autorizado en forma expresa por la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, de corresponder.

v. El personal de soporte técnico de la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, como medida de prevención, si detecta que alguna estación de trabajo o computadora portátil se encuentra infectada con algún tipo de

malware, debe de aislarla inmediatamente, desconectándola de la red corporativa.

f) Respaldo de Información:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe establecer procedimientos rutinarios para el respaldo de la información, de acuerdo con su criticidad, realizando copias de seguridad y pruebas de recuperación, conforme a un cronograma definido.

ii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe resguardar las copias de seguridad en un ambiente distinto al de la Entidad (es decir, fuera de las instalaciones de la Entidad), que reúna las condiciones adecuadas.

iii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe asegurar que los equipos y los medios de respaldo cuentan con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.

iv. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe estimar anticipadamente la cantidad necesaria de medios magnéticos u otros requeridos para realizar las copias de respaldo y, en caso de no contar con ello, solicitar su oportuna adquisición.

v. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas, a través del personal de soporte técnico.

vi. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados debe de realizar pruebas de restauración a las copias de seguridad a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.

vii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

g) **Registro y Monitoreo:**

i. Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados.

ii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, la que haga sus veces en los Órganos desconcentrados, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.

iii. Las actividades de los operadores y administradores de los sistemas de La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe ser monitoreadas, registradas, verificadas regular y periódicamente por la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados.

iv. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los Órganos desconcentrados, debe contar con registro de fallas en los sistemas de información para seguimiento, registros de auditoría y monitoreo pertinente.

v. Cada servidor del GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados es responsable de las actividades realizadas a través de sus cuentas de acceso de red, correo electrónico, sistemas de información asociados y sistemas.

h) **Sincronización de Reloj:**

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe mantener sincronizado los relojes en los Sistemas de Información con una fuente exacta que establece la "Hora Oficial de la República del Perú", a fin de garantizar la exactitud de los registros.

i) **Control de Software Operacional:**

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe implementar mecanismos de restricción para la instalación de software en los equipos de cómputo por parte de los usuarios no autorizados.

j) Controles de Auditoria de los Sistemas de Información:

i. Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de La Oficina de Unidad de Informática, o la que haga sus veces en los Órganos desconcentrados.

ii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.

5.11. Política de Seguridad de las Comunicaciones

5.11.1. Objetivos

a) Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

b) Proteger la información de las redes y la infraestructura que la soporta.

c) Monitorear las actividades de procesamiento de información no autorizadas.

5.11.2. Política

a) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los órganos desconcentrados, debe implementar mecanismos de control y procedimientos necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; asimismo, vela por que se cuente con controles de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

b) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los órganos desconcentrados debe realizar la segregación de redes, a fin de garantizar su debida protección.

c) Seguridad de Correo Electrónico

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los órganos desconcentrados, puede efectuar la desactivación de la cuenta de correo electrónico institucional por algún uso indebido que transgreda lo establecido en el presente documento.

ii. Cada servidor es responsable por la información que se transmita desde la cuenta de correo electrónico que le haya asignado la Entidad.

iii. En caso el servidor reciba mensajes con asuntos sospechosos y/o de origen desconocido, estos no deben ser abiertos y deben comunicar inmediatamente a la La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, según corresponda, así como al Oficial de Seguridad de la Información para los fines correspondientes y luego deben ser eliminados

iv. El envío de mensajes masivos de correo electrónico dentro de la Entidad está permitido solo para el personal o dependencias autorizados por la Oficina de Tecnologías de la Información del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los Órganos desconcentrados.

d) Acuerdo de Confidencialidad

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, asegura la protección de la información en el momento de ser transferida o intercambiada y establece los procedimientos y controles necesarios para el intercambio de información; asimismo, se establecen Acuerdos de Confidencialidad y/o de Intercambio de Información con terceras partes y/o con quienes corresponda.

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, vela por el uso de Tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; de acuerdo a lo establecido en los acuerdos que contraiga.

5.12. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

5.12.1. Objetivo

a) Asegurar que los sistemas cumplan con los requisitos de seguridad de la Entidad.

b) Evitar pérdidas, modificaciones o mal uso de la información que se encuentra dentro de los sistemas.

c) Proteger la confidencialidad, autenticidad e integridad de los sistemas del sector.

5.12.2. Política

a) Metodología para la adquisición, desarrollo y mantenimiento de los sistemas:

   i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados, debe aprobar un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas.

   ii. Todo desarrollo y/o mantenimiento de sistemas debe ser documentado, con la finalidad de que personas no familiarizadas con ellas en el GOBIERNO REGIONAL DE MADRE DE DIOS y en sus Órganos desconcentrados, ejecuten las actividades con facilidad.

b) Requisitos de seguridad de los sistemas:

   i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Programas Sociales, debe definir un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de los sistemas.

   ii. Todo sistema desarrollado por los servidores de la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o de la que haga sus veces en los Programas Sociales, o por terceros, debe satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de los sistemas. En el caso de los terceros, el desarrollo de los sistemas debe constar en el respectivo contrato de prestación de servicios.

   iii. El servidor debe cumplir los controles, estándares y metodologías referidas al desarrollo de los sistemas seguras que se hayan implementado.

   iv. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe verificar que los acuerdos sobre materia informática a suscribir con terceros, incluyan cláusulas relativas a la cesión de derechos y confidencialidad de la información, para el resguardo de la propiedad intelectual del GOBIERNO REGIONAL DE MADRE DE DIOS y de sus Órganos desconcentrados.

   iv. Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de

procesamiento de información, deben cubrir los requisitos de seguridad necesarios.

v. Todos los sistemas desarrollados por los servidores son de propiedad del GOBIERNO REGIONAL DE MADRE DE DIOS y de los órganos según corresponda.

c) Procesamiento correcto de los sistemas:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe implementar controles de seguridad apropiados en los sistemas utilizadas por el GOBIERNO REGIONAL DE MADRE DE DIOS, o sus órganos desconcentrados para validar los datos de entrada, el procesamiento interno y los datos de salida.

ii. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe identificar los requerimientos para asegurar la autenticidad y la integridad de los mensajes en los sistemas, debiendo definirse e implementarse los controles apropiados.

d) Seguridad de los archivos de los sistemas:

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, deben implementar controles sobre lo siguiente:

i. Control de los sistemas en Producción: Comprende la formulación y puesta en práctica de procedimientos orientados a controlar la instalación de los sistemas en producción.

ii. Protección de Datos de Prueba: Los datos de prueba de los sistemas deben ser cuidadosamente seleccionados, protegidos y controlados.

e) Control de acceso al Código Fuente de los sistemas:

La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, deben implementar los siguientes controles:

i. Restringir y controlar el acceso al código fuente de los sistemas o programas.

ii. Contar con un responsable del acceso al código fuente de los sistemas, quien debe implementar un registro de uso, si es que el código es requerido.

f) Seguridad en los procesos de desarrollo y pase a producción:

i. Procedimiento para el desarrollo de los sistemas:
Todo el desarrollo y mantenimiento de los sistemas en el GOBIERNO REGIONAL DE MADRE DE DIOS y de sus órganos desconcentrados deben ser realizados conforme a los procedimientos establecidos, debiendo considerarse la NTP ISO/IEC 12207 y otros estándares pertinentes.

ii. Procedimiento para pase a producción:

- Los servidores encargados del desarrollo y mantenimiento de los sistemas, así como los terceros, no tendrá acceso a los datos de producción.

- Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo al personal autorizado

- El pase a producción debe ser realizado exclusivamente por la persona autorizada por l La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, quien lleva un control de los pases efectuados y/o actualizaciones de los sistemas en un registro.

- Todo desarrollo, antes de su pase a producción, debe ser revisado por La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, para asegurar que se cumplan los estándares establecidos.

g) Control de cambios de los sistemas:

i. El control, registro y monitoreo de los cambios de los sistemas del GOBIERNO REGIONAL DE MADRE DE DIOS y de sus Órganos desconcentrados debe ser supervisado y registrado por La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados.

ii. Todo acceso a la librería de los programas fuente debe ser controlado por La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, a fin de evitar accesos y/o cambios no autorizados.

h) Gestión de vulnerabilidades técnicas:

i. La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe programar la realización de pruebas de comprobación técnica a cargo de especialistas para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.

ii. Para los sistemas que requieren una actualización de seguridad (parches), La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe probar y evaluar su efectividad en un ambiente de pruebas; asimismo, se deben considerar los riesgos asociados a su aplicación y, en todas las cosas, se deben cumplir los controles establecidos para la gestión de cambios.

5.13. Política de Relación con Proveedores

5.13.1. Objetivos

Garantizar la protección de los activos de información del GOBIERNO REGIONAL DE MADRE DE DIOS y de sus órganos desconcentrados, que son accesibles por los Proveedores.

5.13.2. Política

a) Todo proveedor que brinde servicios a GOBIERNO REGIONAL DE MADRE DE DIOS y a sus órganos desconcentrados, debe suscribir un acuerdo de confidencialidad, la misma que será parte del contrato de prestación de servicios como anexo.

b) Los proveedores sólo podrán desarrollar para GOBIERNO REGIONAL DE MADRE DE DIOS o sus Órganos desconcentrados, aquellas actividades cubiertas bajo el correspondiente contrato u orden de prestación de servicios.

c) Todo proveedor de servicios debe velar porque su personal que presta los servicios directamente a GOBIERNO REGIONAL DE MADRE DE DIOS y a sus òrganos desconcentrados, cumpla con las políticas de seguridad de la información recogidas en el presente documento. En caso de incumplimiento, GOBIERNO REGIONAL DE MADRE DE DIOS se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los Órganos desconcentrados, de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.

d) Cualquier tipo de intercambio de información que se produzca entre el GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los Órganos desconcentrados y el proveedor se debe entender que ha sido realizado dentro del marco establecido por el contrato u orden de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.

e) Todo proveedor que tenga acceso a la información del GOBIERNO REGIONAL DE MADRE DE DIOS o la que haga sus veces en los órganos desconcentrados, en ejecución de un contrato u orden de prestación de servicios, debe considerar que dicha información, es confidencial y sujeto a la Ley de Protección de Datos Personales.

f) Ningún proveedor puede utilizar la información del GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados para beneficio propio o de terceros. La información a la que tenga acceso el proveedor, únicamente puede ser utilizada para los fines específicamente indicados en el contrato u orden de prestación de servicios. Toda información proporcionada por el GOBIERNO REGIONAL DE MADRE DE DIOS u Órganos desconcentrados, sigue siendo de propiedad de esta última.

g) El proveedor y su personal únicamente puede utilizar la información y activos tecnológicos autorizados por el GOBIERNO REGIONAL DE MADRE DE DIOS o de sus Órganos desconcentrados para el desarrollo de los servicios contratados.

h) La distribución de la información ya sea en formato digital o papel, se realiza mediante los recursos determinados en el contrato de prestación de servicios y para la finalidad exclusiva de facilitar las funciones asociados a dicho contrato. El GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados, se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre los recursos de difusión.

i) Los recursos que el GOBIERNO REGIONAL DE MADRE DE DIOS o de los Órganos desconcentrados que pone a disposición del proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. El GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados se reservan el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

j) El proveedor debe notificar a La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, cualquier incidencia que se

detecte y que afecte o pueda afectar a la seguridad de la Información de la Entidad.

5.14. Política de Gestión de Incidentes de Seguridad de la Información

5.14.1. Objetivo

Asegurar que los incidentes de seguridad de la información del GOBIERNO REGIONAL DE MADRE DE DIOS y los de sus órganos desconcentrados sean comunicados oportunamente a las instancias correspondientes, con la finalidad de adoptar acciones preventivas y correctivas que correspondan.

5.14.2. Política

a) Los incidentes relativos a la seguridad de la información deben ser comunicados a la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.

b) El servidor del GOBIERNO REGIONAL DE MADRE DE DIOS y de sus Órganos desconcentrados deben conocer el procedimiento de gestión de incidentes de seguridad de la información, e informar de su ocurrencia tan pronto tome conocimiento de ellos.

c) Cualquier servidor del GOBIERNO REGIONAL DE MADRE DE DIOS y de sus órganos desconcentrados debe comunicar al Oficial de Seguridad de la Información del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los órganos desconcentrados las sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que puede tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.

d) El servidor del GOBIERNO REGIONAL DE MADRE DE DIOS y sus órganos desconcentrados deben conocer su responsabilidad respecto a la comunicación de los incidentes de seguridad que tome conocimiento, debiendo ser notificados de los resultados una vez que el incidente haya sido resuelto.

e) Reportados los incidentes de seguridad de la información a la Oficina de Tecnologías de la Información del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que hagas sus veces en los órganos desconcentrados, y al Oficial de Seguridad de la Información, debe proceder a su exhaustivo análisis por parte del servidor que designe la referida oficina o dependencia del programa, a efectos de adoptar las acciones que correspondan.

f) Los incidentes de seguridad serán evaluados por el Oficial de Seguridad de la información del GOBIERNO REGIONAL DE MADRE DE DIOS y de sus órganos desconcentrados, a efectos de proponer las acciones preventivas que correspondan, para lo sucesivo.

g) Periódicamente, la Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS o la que hagas sus veces en los Órganos desconcentrados, debe analizar las actividades realizadas y estudiar posibles mejoras cambios que puedan proponerse al Comité de Gestión de Seguridad de la Información para prevenir la ocurrencia de futuros incidentes de Seguridad de la Información.

5.15. Política de Continuidad de la Seguridad de la Información

5.15.1. Objetivos

Asegurar que los incidentes de seguridad de la información del GOBIERNO REGIONAL DE MADRE DE DIOS y los de sus órganos desconcentrados sean comunicados oportunamente a las instancias correspondientes, con la finalidad de adoptar acciones preventivas y correctivas que correspondan.

5.15.2. Política

a) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los Órganos desconcentrados, debe incluir la continuidad de la seguridad de la información dentro del proceso de gestión de continuidad operativa.

b) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los Órganos desconcentrados, debe verificar los controles de continuidad de seguridad de la información que se han implementados regulares para asegurar que sean válidos y efectivos.

c) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los Órganos desconcentrados, debe asegurar la existencia de recursos redundantes para el tratamiento de la información a fin de cumplir con los requisitos de disponibilidad.

d) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o quien haga sus veces en los Órganos desconcentrados, debe realizar las pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que

se encuentran conforme a los objetivos de continuidad de la seguridad de la información, estas pruebas deben quedar documentadas.

5.16. Política de Cumplimiento

5.16.1. Objetivo

a) Prevenir incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

b) Garantizar que la seguridad de la información se implementa y opera de acuerdo con la política y procedimientos de la Entidad.

5.16.2. Política

a) Todos los órganos y unidades orgánicas del GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados deben cumplir con todos los requisitos legislativos, regulaciones y requerimientos contractuales relativas a seguridad de la información, asimismo, deben ser identificadas y documentadas.

b) Todos los órganos y unidades orgánicas del GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados deben asegurar el cumplimiento a los derechos de propiedad intelectual, para lo cual todo el software que utiliza en la Entidad debe contar con la respectiva licencia de uso.

e) Los servidores del GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados no deben destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.

c) El GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados a través del Órgano o Unidad Orgánica responsable de acuerdo a su competencia, debe de garantizar la protección y la privacidad de los datos personales conforme a la legislación aplicable.

d) El GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados a través del Órgano o Unidad Orgánica responsable de acuerdo a su competencia, debe establecer los términos, condiciones y finalidades para datos personales en cumplimiento con la Ley existente y su Reglamento.

e) La Oficina de Unidad de Informática del GOBIERNO REGIONAL DE MADRE DE DIOS, o la que haga sus veces en los Órganos desconcentrados, debe asegurar que la seguridad de la información este implementada y operada, a través de revisiones

independientes de la seguridad de la información mediante auditorías para asegurar que se mantenga de forma eficaz, eficiente y efectiva.

6. ANEXO: DEFINICIONES

Para los fines del presente Lineamiento, se establecen las siguientes definiciones

- **Activo de Información:** Información que tiene valor para la Entidad, pudiendo además ser aquel recurso (humano, tecnológico, etc.) que efectúa el tratamiento directo o indirecto de la información que soporta uno o más procesos de la Entidad.

- **Antecedentes Laborales:** Información que permite identificar los antecedentes (Policiales, Penales, Judiciales) del servidor.

- **Clasificación de Información:** Conjunto de actividades que permiten identificar y clasificar los activos de información en términos de la sensibilidad e importancia para el GOBIERNO REGIONAL DE MADRE DE DIOS y sus Órganos desconcentrados.

- **Confidencialidad:** Característica/propiedad por la cual la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **Disponibilidad:** Característica/propiedad por la cual la información permanece accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Evento:** Un suceso o serie de sucesos que pueden ser interno o externo al GOBIERNO REGIONAL DE MADRE DE DIOS o sus Órganos desconcentrados, originados por una misma causa, que ocurren durante el mismo periodo de tiempo.

- **Incidente de Seguridad de la Información:** Evento no deseado que tiene una probabilidad significativa de comprometer las operaciones de la Entidad y que genera amenazas a la seguridad de la información.

- **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

- **Integridad:** Característica/propiedad por la cual la información conserva su exactitud y se encuentra completa.

- **Medios Removibles:** Son aquellos dispositivos que se insertan en los conectores externos de los equipos informáticos para almacenar

información, tales como memoria USB, disco duro externo o tarjetas de memoria.

- **Oficial de Seguridad de la Información:** Servidor responsable de la Seguridad de la Información, designado mediante Resolución Ejecutiva Regional N° 107-2020-GOREMAD/GR

- **Propietario de Activo de Información:** Una persona, cargo, proceso o grupo de trabajo designado por la organización, quien tiene la responsabilidad de definir los controles y/o lineamientos para el cuidado de los activos de información, bajo su responsabilidad. Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos.

- **Seguridad de la Información:** Son todas las actividades orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento, independientemente de la forma en que éste se presente.