DTCI

TETÃ REMBIAPO
HA MARANDU
Motenondeha
Ministerio de
OBRAS PÚBLICAS
Y COMUNICACIONES

RESOLUCIÓN N° 963

POR LA CUAL SE APRUEBA LA POLÍTICA OPERACIONAL DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEPENDIENTE DEL GABINETE DEL MINISTRO DE OBRAS PÚBLICAS Y COMUNICACIONES, DENTRO DEL MARCO DE LA IMPLEMENTACIÓN DEL MODELO ESTÁNDAR DE CONTROL INTERNO DEL PARAGUAY - MECIP 2015, DE ESTA CARTERA DE ESTADO, QUE FORMAN PARTE COMO ANEXO DE LA PRESENTE RESOLUCIÓN.

Asunción, 01 de junio de 2023

VISTO: El memorándum DTCI – MECIP N.° 23/2022, de la Dirección Técnica de Control Interno, por medio del cual se solicita iniciar los trámites para la aprobación de la Política Operacional de la Dirección de Tecnologías de la Información y Comunicación, y;

CONSIDERANDO: Que la Ley N.° 167/1993 "QUE APRUEBA CON MODIFICACIONES EL DECRETO-LEY No. 5 DE FECHA 27 DE MARZO DE 1991, QUE ESTABLECE LA ESTRUCTURA ORGÁNICA Y FUNCIONES DEL MINISTERIO DE OBRAS PÚBLICAS Y COMUNICACIONES" establece en su Artículo 4°: "el Ministro de Obras Públicas y Comunicaciones es la autoridad máxima designada por el poder ejecutivo para administrar y desarrollar las actividades del ministerio. Como jefe superior de la cartera, es de su competencia y responsabilidad el despacho de los negocios del ministerio por la constitución nacional, la presente estructura y funciones orgánicas o disposiciones legales pertinentes"; y, en su Artículo 42°: "Facúltese al Ministerio de Obras Públicas y Comunicaciones a reglamentar la organización y funciones de todas las unidades dependientes de la Cartera, de conformidad con el presente Decreto-Ley".

Que el Decreto N.° 962/2008, que modifica el Título VII del Decreto N.° 8127/2000 "POR EL CUAL SE ESTABLECEN LAS DISPOSICIONES LEGALES Y ADMINISTRATIVAS QUE REGLAMENTAN LA IMPLEMENTACIÓN DE LA 1535/99, DE ADMINISTRACIÓN FINANCIERA DEL ESTADO Y EL FUNCIONAMIENTO DEL SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA (SIAF)", en los siguientes términos: "CAPITULO II – Modelo Estándar de Control Interno para las Entidades Públicas del Paraguay – Mecip, definido en el Anexo que forma parte de este Decreto".

Que la Resolución N.° 922, de fecha 13 de agosto del año 2008 "POR LA CUAL SE ADOPTA EL MODELO ESTANDAR DE CONTROL INTERNO PARA LAS ENTIDADES PÚBLICAS DEL PARAGUAY – MECIP Y SE DISPONEN LAS MEDIDAS TENDIENTES AL INICIO DE SU IMPLENTACIÓN AL INTERIOR DE ESTE MINISTERIO".

TETÃ REMBIAPO
HA MARANDU
Motenondeha
Ministerio de
OBRAS PÚBLICAS
Y COMUNICACIONES

RESOLUCIÓN N° 963

POR LA CUAL SE APRUEBA LA POLÍTICA OPERACIONAL DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEPENDIENTE DEL GABINETE DEL MINISTRO DE OBRAS PÚBLICAS Y COMUNICACIONES, DENTRO DEL MARCO DE LA IMPLEMENTACIÓN DEL MODELO ESTÁNDAR DE CONTROL INTERNO DEL PARAGUAY - MECIP 2015, DE ESTA CARTERA DE ESTADO, QUE FORMAN PARTE COMO ANEXO DE LA PRESENTE RESOLUCIÓN.

Que la Resolución N.° 1019, de fecha 07 de julio de 2020 "POR LA CUAL SE APRUEBA LA POLÍTICA DEL CONTROL INTERNO DEL MINISTERIO DE OBRAS PÚBLICAS Y COMUNICACIONES - CONFORME A LA NORMA DE REQUISITOS MÍNIMOS PARA UN SISTEMA DE CONTROL INTERNO - MECIP :2015".

Que la Resolución CGR N.° 377, de fecha 13 de mayo de 2016 "POR LA CUAL SE ADOPTA LA NORMA DE REQUISITOS MÍNIMOS PARA UN SISTEMA DE CONTROL INTERNO DEL MODELO ESTÁNDAR DE CONTROL INTERNO PARA INSTITUCIONES PÚBLICAS DEL PARAGUAY - MECIP 2015".

Que la Resolución CGR N.° 147, de fecha 25 de marzo del año 2019 "POR LA CUAL SE APRUEBA LA MATRIZ DE EVALUACIÓN POR NIVELES DE MADUREZ", A SER UTILIZADA EN EL MARCO DEL SISTEMA DE CONTROL INTERNO PARA INSTITUCIONES PÚBLICAS DEL PARAGUAY MECIP: 2015".

Que conforme lo establece el Manual de Requisitos Mínimos, la Institución debe definir Políticas Operacionales que permitan estructurar y direccionar el buen desempeño del Modelo de Gestión por Procesos.

Que las Políticas Operacionales deben definir parámetros de diseño de las actividades y tareas requeridas para dar cumplimiento a los objetivos de los procesos.

Que la Dirección de Asuntos Jurídicos, se ha expedido favorablemente, según Dictamen DAJ N.° 1076/2023, de fecha 01 junio de 2023.

POR TANTO; en ejercicio de sus atribuciones legales,

EL MINISTRO DE OBRAS PÚBLICAS Y COMUNICACIONES

R E S U E L V E :

Artículo 1°.- Aprobar la Política Operacional de la Dirección de Tecnologías de la Información y Comunicación, dependiente del Gabinete del Ministro de Obras Públicas y Comunicaciones, conforme al Anexo que forma parte de la presente Resolución y al siguiente detalle:

COPIA

M.O.P.C.

TETÃ REMBIAPO
HA MARANDU
Mocemondeha
Ministerio de
OBRAS PÚBLICAS
Y COMUNICACIONES

RESOLUCIÓN N° 963

POR LA CUAL SE APRUEBA LA POLÍTICA OPERACIONAL DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEPENDIENTE DEL GABINETE DEL MINISTRO DE OBRAS PÚBLICAS Y COMUNICACIONES, DENTRO DEL MARCO DE LA IMPLEMENTACIÓN DEL MODELO ESTÁNDAR DE CONTROL INTERNO DEL PARAGUAY - MECIP 2015, DE ESTA CARTERA DE ESTADO, QUE FORMAN PARTE COMO ANEXO DE LA PRESENTE RESOLUCIÓN.

- **Política Operacional:** Análisis y Desarrollo de Sistemas Informáticos.
- **Política Operacional:** Seguridad Informática.

Artículo 2°.- Encomendar al responsable del proceso, realizar revisiones de acuerdo a requerimientos de los mismos, a fin de asegurar su conveniencia y adecuación.

Artículo 3°.- Encargar al Director del sector, como responsable de la implementación de la presente norma.

Artículo 4°.- La falta de cumplimiento de las disposiciones establecidas en el presente ordenamiento, dará lugar a la aplicación de las sanciones correspondientes en los términos prescriptos en la Ley N.° 1626/2000 "DE LA FUNCIÓN PÚBLICA", en los Artículos 82°, 83° y 84° de la Ley N.° 1535/1999 "DE ADMINISTRACIÓN FINANCIERA DEL ESTADO" y concordantes del Decreto Reglamentario N.° 8127/2000.

Artículo 5°.- Publicar la presente Resolución y su Anexo, en el portal web institucional.

Artículo 6°.- Dejar sin efecto todas aquellas disposiciones contrarias a la presente Resolución.

Artículo 7°.- Comunicar a quienes corresponda y cumplido archivar.

Ing. RODOLFO SEGOVIA COLMÁN
Ministro

RSC/ee

COPIA

MINISTERIO DE OBRAS PÚBLICAS Y COMUNICACIONES
SECRETARÍA GENERAL

M.O.P.C.

12 Doce |.

MOPC	POLÍTICA OPERACIONAL Análisis y Desarrollo de Sistemas Informáticos	Revisión: 00 Código: --- Vigencia: 01/06/2023

I. OBJETIVO

La presente Política Operacional del proceso Análisis y Desarrollo de Sistemas Informáticos, tiene por objetivo establecer las directrices para un adecuado desarrollo, adquisición e implementación de sistemas informáticos, además de asegurar la disponibilidad y resguardo de los mismos.

II. IDENTIFICACIÓN

Objetivo Estratégico: Disponer de la información y sistemas claves para la ejecución de la estrategia.

Macroproceso: Gestión de TIC
Procesos: Análisis y Desarrollo de Sistemas Informáticos

III. ALCANCE

- Los lineamientos que se detallan en el presente documento, aplica a toda información generada en el ámbito operativo de la institución.
- Diseño e implementación de los mecanismos apropiados (sistematizados o manuales) que permitan un acertado control sobre las tecnologías de la información de la institución.
- Los procedimientos para la correcta utilización y comprensión de los sistemas y recursos informáticos/tecnológicos de la institución.

IV. RESPONSABLE DE APLICACIÓN:

- **Ministro**
- **Director**
- **Coordinador**
- **Jefes de Departamentos**
- **Funcionarios**

V. DEFINICIONES:

- **MOPC:** Ministerio de Obras Publicas y Comunicaciones.
- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
- **TI:** Tecnologías de la Información.
- **TIC:** Tecnologías de la Información y las Comunicaciones
- **Interoperabilidad:** Capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos.
- **Licenciamiento:** Contrato en virtud del cual el titular de los derechos patrimoniales de un software, autoriza al usuario el derecho a ejercer alguna forma de explotación del mismo, en las condiciones acordadas en el mismo.
- **Actualización:** Proceso de modificación, revisión y/o mejoras dentro de la generación de un programa y del Código Fuente. Las actualizaciones realizadas en el sistema y en el Código Fuente se regirán por este mismo contrato.
- **Usuario:** Individuo o persona jurídica, autorizados a utilizar un sistema o software.
- **Proveedor:** La persona física o jurídica que suscriba algún contrato o acepte alguna orden para la provisión o locación de bienes, o para la prestación de servicios de cualquier naturaleza.

Lic. Raúl A... Coordinador Depto. Tecnico - Dirección TIC's

MINISTERIO DE OBRAS PUBLICAS Y COMUNICACIONES DIRECCION DE TIC'S

Lic. Miguel A. Calderón P. Coordinador Dirección TIC's - MOPC

Mgtr. Eduardo Bergottini Director Dirección Tic's

MINISTERIO DE OBRAS PUBLICAS Y COMUNICACIONES SECRETARIA GENERAL

MOPC	POLÍTICA OPERACIONAL Análisis y Desarrollo de Sistemas Informáticos	Revisión: 00 Código: --- Vigencia: 01/06/2023

VI. DELINEAMIENTOS

1. POLÍTICAS GENERALES

1.1. El MOPC, desarrollará una Política Operacional de Análisis y Desarrollo de Sistemas Informáticos que sea oportuna, eficaz, eficiente y aplicable a las circunstancias y contexto en el que se sitúa el negocio, dando cumplimiento el reglamento interno y normas locales vigentes.

1.2. El MOPC, establece los siguientes lineamientos para el Análisis y Desarrollo de Sistemas Informáticos:

- Establecer y hacer uso de una Política Operacional de Análisis y Desarrollo de Sistemas Informáticos, como parte de sus instrumentos de gestión, así como para la definición de los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

- El cumplimiento de la Política Operacional de Análisis y desarrollo de Sistemas Informáticos es de aplicación obligatoria para todos los funcionarios en la institución. En caso de incumplimiento y/o violación de la misma, la institución se reserva el derecho a tomar las medidas correspondientes.

- Las excepciones a cualquier cumplimiento de la Política Operacional de Análisis y Desarrollo de Sistemas Informáticos, deben ser ajustadas y aprobadas por los Directivos; Jefes de Áreas de TI de la institución. Además, deben ser formalmente documentadas, registradas y revisadas por los mismos.

- Las modificaciones o adiciones de la Política Operacional de Análisis y Desarrollo de Sistemas Informáticos serán propuestas por los funcionarios del área, validándose las mismas por el Jefe de Departamento de Sistemas y aprobadas por el Director de TIC.

- Esta Política Operacional debe ser verificada, analizada y ajustada, como mínimo una vez al año o cuando sea necesario, para adaptarla a los acontecimientos cambiantes del entorno operativo.

- Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las posibles consecuencias de la no conformidad.

- Esta Política Operacional atenderá los criterios, técnicas, métodos y normativas internas establecidas por la institución.

2. POLÍTICAS DE OPERACIÓN

2.1. Análisis, Desarrollo y Adquisición e Implementación de Sistemas

2.1.1. Todos los proyectos de software que deban ser desarrollados o adquiridos por el MOPC, deberán de contar con el análisis de viabilidad del Departamento de Sistemas para la posterior aprobación del Director.

2.1.2. Es responsabilidad del Departamento de Sistemas, acompañar, si así amerite, la adquisición, implementación o actualización de los sistemas, asegurando la calidad de los sistemas entregados, para que estén de acuerdo con criterios de innovación, confiabilidad, disponibilidad, seguridad e interoperabilidad, para que sirvan de soporte a la productividad de los funcionarios en los procesos.

2.1.3. Al desarrollar los procesos de negocio, aplicaciones y repositorios de información de sistemas, estos deben estar basados en las especificaciones acordadas.

Lic. Raúl Ariel Pineda
Coordinador
Coord. Técnico - G.V.M.A.P.

Ingº Eduardo Bergottir
Director

Lic. Ángel A. Cabrera F.
Coordinador
Dirección TIC's - MOPC

2.1.4. La propiedad intelectual de los desarrollos realizados por los funcionarios, utilizando los recursos de la institución, será propiedad de la misma.
2.1.5. El proceso de adquisición de un software o sistema informático, dependerá de la metodología de adquisición, y deberá regirse por las normas propias de cada metodología.
2.1.6. El proceso de desarrollo de sistemas, debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones. Es necesario, documentar todos los componentes de la solución acorde a los estándares definidos y mantener el control de la versión sobre los mismos y la documentación asociada.
2.1.7. La documentación de cada uno de los sistemas implementados en la institución debe contener el "manual de usuario" conforme a los instrumentos estándares de la institución para brindar soporte a los mismos.
2.1.8. El MOPC, deberá acoger los criterios de seguridad mínimos para el desarrollo y adquisición de software e implementaciones con software de terceros de manera a poder cumplir con los controles establecidos.
2.1.9. Para la aprobación de los proyectos de desarrollo o actualización de sistemas informáticos se tendrán en cuenta las siguientes excepciones:
- Las solicitudes de las dependencias del MOPC sobre la modificación de algún sistema informático, que no tenga, un impacto importante en la estructura de la base de datos y evite afectar el funcionamiento de otros módulos de dicho sistema a modificar, podrán ser aprobadas por el Jefe del Departamento de Sistemas, evitando el circuito de aprobación definido en el manual de procesos para el efecto.
- Cuando la recepción de solicitudes no implique la modificación, acceso o eliminación de datos de la base de datos institucional, estas podrán ser aprobadas por el Jefe del Departamento de Sistemas, evitando el circuito de aprobación definido en el manual de procesos para el efecto.
- Cuando el resultado del análisis de factibilidad de la solicitud de desarrollo de un nuevo sistema informático o modificación de un sistema existente recibido, no sobrepase el tiempo de desarrollo superior a seis (6) meses o requiera la designación de más de un analista de sistemas, estas podrán ser aprobadas por el Jefe del Departamento de Sistemas, evitando el circuito de aprobación definido en el manual de procesos para el efecto.

2.1.10. Para casos en los que el Director de TIC se encuentre ausente o las solicitudes recibidas no manifiesten ningún punto mencionado anteriormente, deberá autorizar al Jefe de Departamento de Sistema la aprobación de dichas solicitudes.
2.1.11. La realización de pruebas de los desarrollos informáticos, serán indispensables para la aprobación de los mismos, y estos deben ser realizados según lo siguiente:
- **Pruebas Unitarias:** La realización de pruebas unitarias del sistema informático desarrollado o modificado será responsabilidad de un funcionario interno del Departamento de Sistemas de la institución, precisando del parecer favorable de este para la siguiente instancia de verificación.
- **Pruebas Integrales:** La realización de pruebas integrales será responsabilidad del área solicitante, corroborando que lo solicitado se encuentre acorde a las necesidades manifestadas al equipo de TI.

2.2. Proveedores de Software

2.2.1. Asegurar, en los casos que son necesarios, que cuando los proveedores estén involucrados en el desarrollo de una solución, el mantenimiento, soporte, estándares y licenciamiento estén correctamente contemplados en las obligaciones contractuales.
2.2.2. La Jefatura de Departamento de Sistemas y sus áreas responsables, podrán asesorar en la adquisición de software al área contratante del mismo.
2.2.3. El área contratante deberá administrar los productos entregables de cada una de las etapas.
2.2.4. El área contratante será responsable del seguimiento para el cumplimiento del contrato y los cronogramas establecidos.

Ing. Eduardo Bergottir
Director TIC's

Lic. Miguel A. Calderón I.
Coordinador
Dirección TIC's - MOPC

MOPC	**POLÍTICA OPERACIONAL** **Análisis y Desarrollo de Sistemas Informáticos**	**Revisión: 00** **Código: ---** **Vigencia:** 01/06/2023

Elaborado por:	Revisado por:	Aprobado por:
Cargo: Jefa de Area.	**Cargo:** Jefa de Dpto	**Cargo:** Director.
Fecha de elaboración:		

Ing. Eduardo Bergonzi
Director
Dirección TICs

Lic. Miguel A. Calderón F.
Coordinador
Dirección TICs - MOPC

COPIA

MINISTERIO DE OBRAS PUBLICAS Y COMUNICACIONES
SECRETARIA GENERAL

Lic. [illegible]
Coordinador
Secretaría General - MOPC

Lic. [illegible]
Coordinador
Coord. Técnico - D.V.M.A.R.

MOPC	**POLÍTICA OPERACIONAL** **Seguridad Informática**	**Revisión:** 00 **Código:** ---- **Vigencia:** 01/06/2023

I. OBJETIVO

La presente Política Operacional del proceso Seguridad Informática, tiene por objetivo establecer las directrices para prevenir, minimizar y mitigar los eventos que pueden alterar la integridad, confidencialidad y disponibilidad de la información de la institución.

II. IDENTIFICACIÓN

Objetivo Estratégico: Disponer de la información y sistemas claves para la ejecución de la estrategia.

Procesos: Seguridad Informática

III. ALCANCE

- Los lineamientos que se detallan en el presente documento, aplica a toda información generada en el ámbito operativo de la institución.
- Diseño e implementación de los mecanismos apropiados (sistematizados o manuales) que permitan un acertado control sobre las tecnologías de la información de la institución.
- Los procedimientos para la correcta utilización y comprensión de los sistemas y recursos informáticos/tecnológicos de la institución.

IV. RESPONSABLE DE APLICACIÓN:

- **Ministro**
- **Director**
- **Coordinador**
- **Jefes de Departamentos**
- **Funcionarios**

V. DEFINICIONES:

- **TI:** Tecnologías de la Información.
- **Dispositivos:** Activos de tecnología de la información (TI) utilizados entre los miembros de una empresa y/o institución durante el trabajo, fuera del horario laboral o cualquier otro propósito.
- **Información:** conjunto organizado de datos procesados.
- **Seguridad Informática:** Protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas.
- **Estándares:** patrón o parámetro que permite establecer uniformidad en características de equipos, sistemas de cómputo, y procedimientos de operación, con el cual se pretende garantizar la integridad, compatibilidad y racionalidad en los procesos tecnológicos de la institución.
- **Sistema Informático:** es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso.
- **Servicio:** Se refiere a una funcionalidad de software o un conjunto de funcionalidades de software, como la recuperación de información especificada o la ejecución de un conjunto de operaciones.
- **Cuentas de usuario:** Una identidad creada para una persona en una computadora o sistema informático.
- **DTIC:** Dirección de Tecnología de la Información y Comunicación.

Lic. Rafael Arte' Peñaloza
Coordinador
Coord. Técnico - G.V.M.A.R.

Ing. Eduardo Bergottini
Director
Dirección TIC's

Lic. Rafael A. Valderón F.
Coordinador
Dirección TICs - MOPC

MOPC	POLÍTICA OPERACIONAL Seguridad Informática	Revisión: 00 Código: ---- Vigencia: 01/06/2023

VI. DELINEAMIENTOS

1. POLÍTICAS GENERALES

1.1. El MOPC., desarrollará una Política de Seguridad Informática de manera oportuna, eficaz, eficiente y aplicable a las circunstancias y contexto en el que se sitúa el negocio, dando cumplimiento al reglamento interno y normas locales vigentes.

1.2. El MOPC., establece los siguientes lineamientos para la Seguridad Informática:

- Establecer y hacer uso de una Política Operacional de Seguridad Informática, como parte de sus instrumentos de gestión, así como para la definición de los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

- El cumplimiento de la Política Operacional de Seguridad Informática es de aplicación obligatoria para todos los funcionarios de la institución. En caso de incumplimiento y/o violación de la misma, la institución se reserva el derecho a tomar las medidas correspondientes.

- Las excepciones a cualquier cumplimiento de la Política Operacional de Seguridad Informática, deben ser ajustadas por el Jefes de Dpto. de Seguridad Informática y aprobadas por el Director de TIC de la institución. Además, deben ser formalmente documentadas, registradas y revisadas por los mismos.

- Las modificaciones o adiciones de la Política Operacional de Seguridad Informática serán propuestas por el Jefe del Departamento de Seguridad Informática, validándose las mismas por este último, y aprobadas el Director de TIC.

- Esta Política Operacional debe ser verificada, analizada y ajustada, como mínimo una vez al año o cuando sea necesario, para adaptarla a los acontecimientos cambiantes del entorno operativo.

- Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las posibles consecuencias de la no conformidad.

- Esta Política Operacional atenderá los criterios, técnicas, métodos y normativas internas establecidas por la institución.

2. POLÍTICAS DE OPERACIÓN

2.1. Seguridad

El usuario es responsable de la información contenida en el equipo a su cargo y por lo tanto debe estar resguardada.

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida por cada funcionario, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de la institución.

Lic. Eduardo Bergottini
Director
Dirección Tic's

Lic. Miguel A. Calderón
Coordinador
Dirección TICs - MOPC

El usuario debe asegurar que el recurso tecnológico asignado tenga los mecanismos de seguridad que permitan el bloqueo automático del mismo cuando no esté presente físicamente, y será activado en un tiempo no mayor a **5 minutos**.

2.1.1. Inventario de dispositivos y software autorizados y no autorizados

Se debe gestionar activamente todo dispositivo de hardware y software en la red (inventario, seguimiento y corrección), de tal manera que solo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados y no gestionados sean detectados y se prevenga que obtengan acceso.

Hardware

- Utilizar una herramienta de descubrimiento activo para identificar equipos conectados a la red de la institución y actualizar el inventario de activos hardware.
- Utilizar una herramienta de descubrimiento pasivo para identificar dispositivos conectados a la red de la institución y actualizar automáticamente el inventario de activos.
- Mantener un inventario veraz y actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la institución.
- Asegurar que el inventario de activos de hardware registre, como mínimo, las direcciones de red, nombre, propósito, responsable, departamento de cada activo, así como también si el activo de hardware ha sido aprobado o no para ser conectado a la red.
- Asegurar de que los activos no autorizados se eliminen de la red, se pongan en cuarentena o el inventario se actualice oportunamente.

Software

- Mantener una lista actualizada de todo el software autorizado que es requerido en la institución para todos los fines de negocio y todos los sistemas de negocio.
- El inventario de software debe obtener el nombre, la versión, el autor y la fecha de instalación de todo el software, incluidos los sistemas operativos autorizados por la institución.
- El inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.
- Asegurar que el software no autorizado es removido, o que sea incluido en el inventario oportunamente.

2.1.2. Protección contra amenazas

Los sistemas deben tener mecanismos de protección adecuadas, actualizadas y activas (antivirus, antimalware, antispam).

Se deben de revisar y evaluar regularmente la información sobre nuevas posibles amenazas.

2.1.3. Seguridad en las redes

Las redes y la infraestructura de apoyo deben ser adecuadamente gestionadas y aseguradas para protegerlas de amenazas y para mantener la seguridad de los sistemas y aplicaciones.

Lic. [illegible] Coordinador Comp. Tecnica - DVMAA

M. Sc. [illegible] Director Dirección Tic's

Lic. Mirella [illegible] Asesor Coordinador Dirección TICs - MOPC

COPIA

MINISTERIO DE OBRAS PUBLICAS Y COMUNICACIONES
DIRECCION GENERAL

Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.

El Departamento de Seguridad Informática debe realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.

2.1.4. Registros de Auditoría

Se deben generar y conservar registros de auditoría de las actividades de los usuarios, de las excepciones o incidentes de información y mantenerlos durante un periodo acordado, para ayudar en investigaciones futuras y en el seguimiento y monitoreo del control de acceso:

Se incluirá como mínimo en los registros, los siguientes datos:

- Identificadores de usuarios.
- Registro de intentos de acceso al sistema exitosos y rechazados.
- Registro de intentos de acceso a los recursos y a los datos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de dispositivos y aplicaciones del sistema.
- Archivos a lo que se ha accedido y la clase de acceso.
- Alarmas por el sistema de control de acceso.
- Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión.
- Cambios o intentos de cambios en las posiciones y en los controles de seguridad del sistema.

2.1.5. Gestión de usuarios y contraseñas

El Departamento de Seguridad Informática, debe garantizar la necesidad de autenticar todo acceso a los activos de información.

Se debe de administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas, documentadas y autorizadas por los gestores individuales designados.

Todos los usuarios que acceden a recursos informáticos de la Red requieren de una única e intransferible identidad o login (nombre de usuario) para una persona. Esta identidad se usa para representar un usuario o dispositivo en los ambientes informáticos de la Red.

La Jefatura de Seguridad Informática, proporcionará este identificador como parte del proceso de autorización mediante pedido realizado por la jefatura encargada del funcionario, mediante sistema informático, facilitando la información requerida, el nombre y apellido de la persona, número de documento de identidad, el área en el cual se encuentra y el cargo, además de los respaldos correspondientes.

Se debe de mantener los derechos de acceso de los usuarios de acuerdo a los requerimientos de las funciones y procesos del área, basándose en los principios de **menor privilegio**, necesidad de tener y necesidad de conocer, es decir, sólo deben tener acceso a funcionalidades de los sistemas y servicios vinculadas a su grupo de responsabilidad, asegurando la mitigación de accesos excesivos y resguardando la confidencialidad de la información.

Director
Dirección Tic's

Coordinador
Dirección TICs - MOPC

COPIA

Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades conforme al perfil y nivel de autoridad del funcionario de la institución.

Los identificadores concedidos son dados de baja cuando la Jefatura encargada o Jefatura del Departamento de Talento Humano solicita procesar la baja correspondiente a dicho identificador de usuario por desvinculación u otro evento del funcionario de la institución.

El usuario asignado a un funcionario es personal e intransferible, cada usuario es responsable de los servicios y recursos que le sean asignados bajo esas credenciales.

En caso de ser necesario una reactivación de usuario (por pérdida u olvido de contraseña) será necesario un correo electrónico del usuario, o de su Jefe inmediato superior a la Jefatura de Seguridad Informática.

La Dirección de TIC a través del Departamento de Seguridad Informática, deberá asegurar que todos los usuarios internos, externos y temporales, y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) sean identificables unívocamente.

Caracteristicas de las contraseñas

- Las Contraseñas deben ser de un mínimo 8 (ocho) caracteres de longitud y estar compuestas por una combinación de números, letras minúsculas, letras mayúsculas y caracteres especiales.
- Las Contraseñas es de uso personal es intransferible
- Las contraseñas no deben ser igual al nombre de usuario
- Las contárselas nuevas no deben ser igual a las anteriores ni modificar solo un parte de ellas.
- Las Contraseñas no deben estar guardados en los navegadores, ni deben ser almacenadas en forma legible en los archivos, o en cualquier forma de donde puedan ser recuperadas.
- Las Contraseña fijas de procesos o equipos de computación que no requieran de cambios periódicos, deben ser modificadas anualmente.
- Toda vez que sospeche o sepa que su Contraseña de acceso pudo haber sido utilizada por otra persona debe inmediatamente:
  - Informar a la Dirección de TICs.
  - Solicitar el cambio de su Contraseña.
  - Las Contraseñas no deben tener:
  - Series de números o letras iguales o consecutivas
  - Palabras del diccionario
  - Referencias al entorno personal como nombres propios, nombres de familiares, nombres de mascotas.
  - Número de documento de identidad
  - Número de legajo
  - Dirección.

2.1.6. Correo electrónico

- El uso del correo se encuentra condicionado a lo estrictamente laboral. De recibirse correos electrónicos que no correspondan al destinatario, el mismo debe ser reencaminado y/o eliminado.

- Cada usuario es directamente responsable de todo lo enviado a través de sus cuentas de correo electrónico.
- Los correos corporativos siempre deberán estar firmados por el redactor de la misma.
- Los mensajes de correo electrónico deben ser considerados como documentos formales. Cuando se redactan los correos electrónicos, los usuarios deben respetar lineamientos éticos y buenas costumbres en el uso del lenguaje.
- Los sistemas de correo electrónico deben brindar la facilidad de mitigar que un usuario reciba correos de un remitente que puede poner en peligro los recursos de la Institución, o que contenga material no autorizado.
- El correo electrónico debe ser utilizado solo para actividad que esté relacionada con la Institución.
- Los mensajes de Correo Electrónico deben ser considerados como documentos formales. Cuando se redactan los Correos Electrónicos, los Usuarios deben respetar lineamientos éticos y buenas costumbres en el uso del lenguaje.
- Los sistemas de Correo Electrónico de la Institución no deben ser utilizado para:
  - Cadenas de mensajes.
  - Envío de mensajes de seguridad, que no fueron originados por la Dirección de Tecnología de la Información y Comunicación.
  - Actividades ilegales, no éticas o inapropiadas.
  - Propósitos ajenos de la Institución.
  - No enviar información privada a destinatarios externos con Correos Electrónicos de la Institución.
  - Los Usuarios no deben utilizar el Correo Electrónico de otra persona.
  - Las utilizaciones de Casillas de Correo Genéricas deben cumplir con los procedimientos de solicitud correspondientes.
  - La institución establecerá las restricciones o límites en cuanto a almacenamiento de correo electrónico por usuario.

2.1.7.Acceso a Internet

- El uso de Internet se encuentra condicionado a lo estrictamente laboral.
- Cada usuario es directamente responsable de su usuario y contraseña para acceder a Internet.
- La utilización del Internet proveído por la institución para fines laborales, debe limitarse exactamente a eso, y en ellos no se consideran fines personales, políticos, religiosos o actividades que sean contrarias a las políticas y normas de la institución.
- Los accesos a lugares obscenos, que distribuyan libremente material pornográfico, o bien materiales ofensivos con los recursos proveídos por la institución, son considerados como uso indebido.
- La conectividad a Internet debe ser otorgada mediante una autorización de la DITC para propósitos relacionados con la Institución.
- La administración del proceso de otorgar autorizaciones de acceso a los Clientes/Usuarios para acceder desde la Red Pública a los servidores de Internet de la Institución debe ser realizada por el Personal de la DTIC.
- Las Contraseñas utilizadas para identificar a Usuarios y/o Clientes que acceden a servidores de la Institución desde la Red Pública (Internet) deben cumplir con los requisitos establecidos por DTIC.
- Los Usuarios autorizados para acceder a Internet, deben utilizar como medio de comunicación el software y el hardware de salida provisto por la Institución.
- La conexión a Redes Públicas como Internet para casos de equipos externos debe ser realizada desde un Firewall que controle que la totalidad del tráfico entrante y saliente a la Red Interna es el autorizado. El uso de Internet debe ser verificado periódicamente por el Encargado de Seguridad de la Información. Si existe alguna

Ing. Eduardo Bergottini
Director
Dirección Tic's

Lic. [illegible]
Coordinador
Dirección TICs - MOPC

COPIA

MINISTERIO DE OBRAS PUBLICAS Y COMUNICACIONES
SECRETARIA GENERAL

razón para creer que la seguridad está siendo violada, el Encargado de Seguridad de la Información puede revisar el contenido de las comunicaciones de Internet.
- Los Usuarios deben tomar conocimiento que el acceso a Internet está siendo registrado y verificado.

2.2. Gestión de Incidentes

Todos los incidentes ocurridos en ámbitos de TI en la institución deben ser notificados, registrados, clasificados, actualizados, escalados, resueltos y cerrados.

La gestión de incidentes debe ser supervisada y revisada. Se deben realizar informes de los problemas gestionados.

La Dirección de TIC y sus jefaturas, deberán preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo.

Se debe de establecer y aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes.

2.3. Sensibilización en Seguridad Informática

La Jefatura del Departamento de Seguridad Informática impulsará las campañas de concientización en materia de seguridad informática, de modo a mitigar los riesgos existentes en este ámbito.

2.4. Almacenamiento y Respaldo de Datos.

Las copias de Seguridad de los Servidores de la institución, deberán ser realizadas cumpliendo con una planificación definida.

El Departamento de Seguridad Informática, deberá realizar las copias de respaldos de los sistemas de Networking (físicos o virtuales) indispensables de la institución, de forma periódica según disponibilidad de almacenamiento en el servidor de Backup, ya sea de forma manual y/o automática según sea el caso.

El Departamento de Seguridad informática, deberá realizar las copias de respaldos de los servidores (físicos o virtuales) indispensables de la institución (Servidor de correo institucional, sistemas internos, sitios webs, entre otros) de forma periódica según disponibilidad de almacenamiento en el servidor de Backup, ya sea de forma manual y/o automática según sea el caso.

Para la realización de copias de respaldos, será necesario considerar:
- Frecuencia (mensual, semanal, diaria, etc.)
- Modo de copias seguridad
- Tipos de copias de seguridad
- Copias de seguridad automatizadas en línea
- Localización física y lógica de las fuentes de los datos
- Seguridad y derechos de accesos
- Tiempos de conservación

Se deberán probar y mantener legibles las copias de seguridad.

COPIA

MINISTERIO DE OBRAS PÚBLICAS Y COMUNICACIONES
SECRETARÍA GENERAL

Mgtr. Eduardo Bergottini
Director
Dirección TIC's

Dirección TICs - MOPC

MOPC	**POLÍTICA OPERACIONAL** **Seguridad Informática**	**Revisión:** 00 **Código:** ---- **Vigencia:** 01/06/2023

*** *** ***

Elaborado por:	Revisado por:	Aprobado por:
		Mgtr. Eduardo Bergottini Director Dirección Tic's
Cargo: Jefe Dpto.	**Cargo:** Jefe Dpto.	**Cargo:** Dirección Tic's
Fecha de elaboración:		

Mgtr. Eduardo Bergottini
Director
Dirección Tic's

Lic. Miguel A. Calderón F.
Coordinador
Dirección TICs - MOPC

COPIA

MINISTERIO DE OBRAS PÚBLICAS Y COMUNICACIONES
SECRETARÍA GENERAL

Lic. Prof. Informática
Coordinador
Gestión e.G.U.I.A.F.