MINISTERIO DE EDUCACIÓN PÚBLICA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 2023-2028

Noviembre, 2023

Tabla de contenido

Acrónimos

AI: Auditoría Interna.
CI: Control interno y Gestión del Riesgo.
CSIRT (*Computer Security Incident Response Team):* Centro de Respuesta de Incidentes de Seguridad Informática.
DIG: Dirección de Informática de Gestión.
DPI: Dirección de Proveeduría Institucional.
DPyE: Departamento de Programación y Evaluación de la Dirección de Planificación Institucional.
DRE: Direcciones Regionales de Educación.
HTTPS: (*Hyper text transfer protocol secure):* Protocolo de transferencia de hipertexto seguro.
IDS: (Intrusion detection system): Sistema de detección de intrusiones.
MEP: Ministerio de Educación Pública.
MFA (Multifactor authentication): Factor de autentificación múltiple.
MICITT: Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.
OC: Oficinas Centrales.
VPN: (*Virtual private network*): Red privada virtual.

Glosario

Análisis de registros y sistemas de gestión de eventos e información de seguridad *(SIEM):* Un sistema de Gestión de Eventos e Información de Seguridad es un sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad.
Antimalware: El antimalware es un tipo de software diseñado para detectar, prevenir y eliminar software malicioso de los ordenadores.
Antivirus: Los antivirus son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el paso del tiempo, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de estos.
Activos tecnológicos: Cualquier recurso tecnológico que pertenezca al MEP, como equipamiento computacional, software, sistemas y servicios.
Base de datos: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

Bases de datos de acceso público: Aquellos ficheros, archivos, registro u otro conjunto de estructura de datos que pueden ser consultados por cualquier persona que no estén impedidos por una norma limitativa, o sin más exigencia que el pago de una contraprestación.
Ciberataques: Son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos.
Ciberseguridad: Es la práctica de proteger sistemas, redes, bases de datos, equipos de cómputo y programas de ataques digitales, que involucran tecnología, personas y procesos. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o interrumpir la continuidad de la operación.
Consulta: Solicitud realizada a una base de datos, en la que se requiere información concreta en función de criterios de búsqueda definidos, siempre que dicha solicitud no resulte en una trasbase o réplica de la base de datos.
Contraseña: Combinación de letras (mayúsculas y/o minúsculas), números y caracteres especiales que debe teclearse para obtener acceso a un programa o partes de un sistema, terminal u ordenador personal, punto en la red, entre otros. Muchas veces se utiliza la terminología inglesa (*password*) para referirse a la clave de acceso.
Correo electrónico: Forma de comunicarse mediante mensajes enviados y recibidos a través de Internet.
CSIRT: ***(Computer Security Incident Response Team):*** Centro de Respuesta de Incidentes de Seguridad Informática. Grupo encargado de controlar y minimizar cualquier tipo de daño a la institución y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación correspondiente. De esta forma, se conocerá el contexto del incidente, que permitirá determinar su origen y posibles consecuencias.
Cuentas de usuario: Colección de información que indica al sistema operativo, los archivos y carpetas a los que puede obtener acceso. Permite que se comparta el mismo equipo entre varias personas, cada una de las cuales tiene sus propios archivos, configuraciones y acceso a ella con un nombre y contraseña.
Datacenter: Se denomina centro de procesamiento de datos al edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y electrónico.
Datos en la nube: Archivo, fichero, registro u otro conjunto estructurado de datos a los cuales se acceda haciendo uso de Internet.
Datos personales de acceso irrestricto: Son los contenidos en bases de datos públicas de acceso general, según dispongan leyes

especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

Datos personales de acceso restringido: Son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

Datos personales: cualquier dato relativo a una persona física identificada o identificable.

Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

Deber de confidencialidad: obligación de los responsables de bases de datos y el personal a su cargo de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por el marco normativo, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos.

Delito informático: Acción ilícita cometida en el ciberespacio mediante el uso de tecnología informática o de comunicaciones. Lo anterior en apego a los tipos penales previstos en el Código Penal, Ley N° 4573, la Ley de la Administración Financiera de la República y Presupuestos Públicos, Ley N° 8131 y normativa afín, entre estos: corrupción, violación de correspondencia o comunicaciones, violación de datos personales, extorsión, estafa informática, daño informático, sabotaje informático e instalación o propagación de programas informáticos.

Dependencia: A lo interno del MEP, se conoce como dependencia, a los centros educativos, direcciones regionales de educación, supervisiones de circuito, viceministerios, direcciones, departamentos y unidades, que conforman la institución y que dependen jerárquicamente del ministro o ministra de educación.

Dispositivo informático personal:
Aparatos electrónicos capaces de almacenar información y/ o conectarse a redes de internet, los cuales no pertenecen al Ministerio, en su lugar pertenecen a cada usuario.

Encargado: Toda persona física o jurídica, entidad pública o privada, o cualquier otro organismo que da tratamiento a los datos personales por cuenta del responsable de la base de datos.

Encriptación o cifrado de datos: La encriptación de datos es un proceso de codificación mediante el cual se altera el contenido de la información haciéndola ilegible, de esta manera se consigue mantener la confidencialidad de la información mientras viaja del emisor al receptor.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma, fin o modalidad de su creación, almacenamiento, organización y acceso.
Filtrado de tráfico: Mediante el filtrado de tráfico, los administradores controlan el tráfico de varios segmentos de la red. El filtrado es el proceso de analizar los contenidos de un paquete para determinar si debe ser permitido o bloqueado.
Firewall: Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada. Este software o esta unidad de hardware y software dedicado, funciona bloqueando o permitiendo los paquetes de datos de forma selectiva.
Firmware: El firmware o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.
Hardware: Todas las partes tangibles de un sistema informático y cuyos componentes pueden ser eléctricos, electrónicos, electromecánicos y mecánicos.
HTTPS: Protocolo de transferencia de hipertexto seguro. Es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web.
IDS: Sistema de detección de intrusiones. Un IDS es un dispositivo de supervisión pasivo que detecta amenazas potenciales y genera alertas, lo que permite a los analistas de un SOC o a los responsables de respuesta a incidentes investigar y responder al incidente potencial.
Interesado: persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.
Internet: Gran comunidad de computadoras conectadas entre sí, por medio de líneas de comunicaciones especiales, agrupando una gran cantidad de asociaciones y empresas.
IPSec: *IPsec* es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet autenticando y/o cifrando cada paquete IP en un flujo de datos. *IPsec* también incluye protocolos para el establecimiento de claves de cifrado.
Log: Se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema.
Malware: Malware es un término general para referirse a cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento y causar daños e interrupciones en el sistema o robar datos.

Mapa de red: Diagrama donde se documentan los componentes de red. En el mismo de enumera y documentan todas las conexiones hacia los servidores, sistemas servicios y redes del MEP.

MFA: *Multifactor authentication.* La autenticación múltiple (MFA) agrega una capa de protección al proceso de inicio de sesión. Cuando se accede a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional; por ejemplo, tienen que escanear su huella digital o especificar un código que reciben en su teléfono.

Navegador *Web*: Programa que provee una interfaz para acceder y ver archivos en Internet.

Nube (*Cloud*): Tendencia tecnológica que brinda un servicio que funciona a través de Internet, permite a los usuarios guardar información de cualquier tipo, teniéndolos alojados en servidores dedicados 24/7/365 y permitiéndoles acceder desde cualquier lugar del mundo. Conocido como computación en la nube, servicios en la nube, informática en la nube, nube de cómputo (del inglés *cloud computing*).

OneDrive: Servicio en la nube de *Microsoft* que le conecta a todos los archivos. Permite almacenar y proteger los archivos, compartirlos con otros usuarios y acceder a ellos desde cualquier lugar en todos sus dispositivos.

Parches de seguridad: son actualizaciones acumulativas enfocadas a solucionar vulnerabilidades en el sistema. Todos los sistemas tienen vulnerabilidades, y la manera de solucionarlas es mediante una actualización del sistema operativo que traiga estos parches o soluciones.

Phishing: Intentan robar las credenciales o los datos confidenciales de los usuarios como, por ejemplo, números de tarjetas de crédito. En este caso, los estafadores envían a los usuarios e-mails o mensajes de texto diseñados para que parezca que provienen de una fuente legítima, utilizando hipervínculos falsos

Pruebas de penetración: La prueba de penetración es un ejercicio de seguridad en el que un experto en Ciberseguridad intenta encontrar y aprovechar las vulnerabilidades de un sistema informático. El objetivo de este ataque simulado es identificar cualquier punto débil en las defensas de un sistema que los atacantes podrían aprovechar.

Ransomware: Es un malware sofisticado que se aprovecha de las debilidades del sistema y utiliza un cifrado sólido para mantener los datos o la funcionalidad del sistema como rehenes.

Recursos informáticos de la institución: Todos aquellos componentes de hardware y software que son necesarios para el buen funcionamiento y optimización del trabajo con computadores y sus periféricos, tanto a nivel Individual, colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos. Los recursos son las

aplicaciones, herramientas, dispositivos (periféricos) y capacidades con los que cuenta una computadora.

Red de datos institucional: Infraestructura de comunicaciones por medio de la cual se proveen los servicios asociados a ella. Entiéndase por datos, cualquier formato en el que los mismos puedan ser representados (texto, voz, imagen, entre otros).

Responsable de la base de datos: Persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.

Segmentación de redes: La segmentación de la red es un modelo arquitectónico que divide una red en varios segmentos o subredes, cada uno de los cuales funciona como una pequeña red propia. Esto permite a los administradores de red aplicar políticas detalladas para controlar el flujo de tráfico entre las distintas subredes.

Seguridad de la información: La seguridad de la información, que suele abreviarse como InfoSec, es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción. InfoSec comprende la seguridad física y del entorno, el control de acceso y la Ciberseguridad.

Sistema de prevención de intrusiones: Un sistema de prevención de intrusiones (IPS) ayuda a las organizaciones a identificar el tráfico malicioso y bloquea de manera proactiva el ingreso de dicho tráfico a su red.

Software: Equipamiento o soporte lógico de un sistema informático; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

SPAM: El spam es cualquier forma de comunicación no solicitada que se envía de forma masiva

Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

UPS: Dispositivo de alimentación eléctrica ininterrumpida.

Usuario externo: Persona(s) física(s) o jurídica(s) ajena(s) a la Institución que utilizan bienes o servicios que el MEP provee.

Usuario interno: Persona que labora en el este ministerio y que utiliza o accede a cualquier bien o servicio que el MEP provee.

VPN: *Virtual private network*. Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

I. Introducción

En este documento se describen aspectos generales, reglas y recomendaciones para mantener un nivel adecuado de seguridad de la información en el Ministerio de Educación Pública (MEP); procurando la seguridad, el resguardo, confidencialidad, integridad y disponibilidad de la información, así como las responsabilidades que conllevan. Esta es una política que contempla las normativas vigentes emitidas por el MICITT en la cual se abarcan generalidades que unificarán criterios y términos relacionados a los lineamientos técnicos establecidos por las autoridades competentes del MEP, constituyéndolos como complemento para procurar la seguridad de la información de la institución.

1.1. Antecedentes

Mediante el oficio DFOE-SEM-0858 enviado el 2 de junio del 2023, la Contraloría General de la República (CGR) hace referencia al cumplimiento de la disposición 4.8 del informe N° DFOE-CAP-IF-00016-2022 de fecha 14 de noviembre de 2022, sobre la gestión de recursos tecnológicos destinados a los procesos de enseñanza y aprendizaje en el Ministerio de Educación Pública, donde se solicita lo descrito en el siguiente párrafo:

"4.8. *Elaborar, oficializar, divulgar e implementar una política de seguridad de la información en el MEP, que contemple, entre otros, los recursos tecnológicos destinados a los procesos de enseñanza y aprendizaje, incluyendo al menos, la gestión de activos de información, la gestión de incidentes y la relación con terceros."*

En los hallazgos descritos por la CGR en el informe N° DFOE-CAP-IF-00016-2022, se estima responden a la ausencia de una política de seguridad de la información en el Ministerio de Educación Pública (MEP), resultando necesaria la misma para la correcta gestión de los recursos tecnológicos destinados a los procesos de enseñanza y aprendizaje que se dotan por medio los diferentes programas MEP, que permita mantener la integridad, confiabilidad y disponibilidad de los datos que se almacenan en los recursos tecnológicos de los centros educativos y dependencias ministeriales en general y que

considere la gestión de activos de información, la gestión de incidentes y la relación con terceros.

1.2. Deberes *in vigilando*

1.2.1. El presente documento debe ser de conocimiento y aplicación **obligatoria** para todos los funcionarios del MEP. Cualquier aclaración a dudas sobre la aplicación de esta política puede realizarse mediante el correo seguridadinformaticadig@mep.go.cr, de la Dirección de Informática de Gestión (DIG).

1.2.2. Esta política debe ser revisada, actualizada y comunicada anualmente.

1.3. Alcance

Esta política tiene un alcance temporal que comprende el período que va desde el año 2023 al año 2028 de acuerdo con la temporalidad de la Estrategia Nacional de Ciberseguridad.

Aplica a todos los funcionarios del MEP con la finalidad de proteger los recursos informáticos que son utilizados para su gestión y los procesos de enseñanza y aprendizaje permitiendo mantener la integridad confidencialidad y disponibilidad.

II. Marco Diagnóstico de Referencia

2.1. Dimensión Legal

El marco normativo aplicable a esta política institucional, aunado a los lineamientos institucionales o nacionales vigentes en la materia comprende:

- Ley de la Administración Financiera de la República y Presupuestos Públicos, Ley Nº 8131, Artículo 111. Delito Informático.
- Ley del Sistema Nacional de Archivos 7202, Archivo Nacional, 1990.
- Ley General de Control Interno, Contraloría General de la República, N° 8292 de 2002.

- Ley de Certificados y Firmas Digitales y Documentos Electrónicos, N°8454 de 30 de agosto de 2005.
- Ley 8968: Ley de Protección de la Persona frente al tratamiento de sus datos personales.
- Decreto Ejecutivo N°31659-MP-RE-SP-H-J-MOPT, Crea la Comisión Interinstitucional sobre Terrorismo (CISTE).
- Decreto Ejecutivo N°36274-MICIT, Creación de la Comisión Nacional de Seguridad en Línea.
- Decreto Ejecutivo N°37052-MICIT, Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR.
- Decreto Ejecutivo N°40199-MP, Establece la apertura de los datos públicos.
- Decreto Ejecutivo N°40546 – RREE, Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001).
- Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central. Decreto Ejecutivo, N° 37549-J.
- Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Decreto Ejecutivo N° 37554-JP.
- Reglamento Ejecutivo a la Ley del Sistema Nacional de Archivos, decreto N° 40554-C de 29 de junio de 2017.
- Estrategia Nacional de Ciberseguridad, Costa Rica 2023-2027. MICITT, 2023.
- DIRECTRIZ N° 133-MP-MICITT, Recomendaciones y medidas técnicas de MICITT y CSIRT-CR.
- Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional. MICITT, 2022.
- Código Nacional de Tecnologías Digitales, MICITT, 2023, CNTD.pdf (micitt.go.cr).
- Manual de lineamiento de uso de recursos informáticos. MEP, 2023.
- Norma técnica para la gestión de documentos electrónicos en el Sistema Nacional de Archivos, publicada en el Alcance Nº 105 a La Gaceta Nº 88 del 21 de mayo de 2018.

- Propuesta: Política Nacional para la gestión y conservación de documentos para garantizar la transparencia y acceso a la Información Pública, febrero 2018.
- Informe N° DFOE-CAP-IF-00016-2022 de fecha 14 de noviembre de 2022, Informe De Auditoría De Carácter Especial Sobre La Gestión De Recursos Tecnológicos Destinados A Los Procesos De Enseñanza Y Aprendizaje En El Ministerio De Educación Pública
- Plan Estratégico de Tecnología de la Información. MEP 2020.

2.2. Dimensión Situacional

Con el desarrollo del internet y de los sistemas informáticos las personas accesan e interactúan en los sistemas de información por medio de un nuevo espacio de interacción denominado "ciberespacio", donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día" (Alonso García, Javier. 2015. Derecho penal y redes sociales. Madrid: Aranzadi). Igualmente se empiezan a materializar un conjunto de amenazas concretas derivadas del uso malicioso de las tecnologías digitales, de sus limitaciones y vulnerabilidades intrínsecas, esto, con el único fin de lesionar la integridad individual y/o colectiva en favor del crimen cibernético y del ciberterrorismo.

Hoy en día, los ataques maliciosos que se dan en el ciberespacio son una de las principales amenazas a las que se enfrentan las empresas, personas y gobiernos, estos ataques se dan en todas las escalas, sin importar tamaño o relevancia de la instancia atacada, por lo que lograr una ciberseguridad robusta se convierte en uno de los mayores retos en la actualidad.

A nivel mundial, los expertos, coinciden en que los ciberataques representan la mayor amenaza no solo para el individuo, sino también para la sociedad en su conjunto por lo que a nivel mundial se inician esfuerzos para contrarrestar su alcance, tipificando las diversas actividades realizadas en el ciberespacio, dirigidas a diversos objetivos, que por su naturaleza serían constitutivos de delito, esto por medio del Consejo de Europa, en su Convenio sobre la

ciberdelincuencia promulgado el 23 de noviembre de 2001 en Budapest, donde se engloban las actuaciones de esta naturaleza.

A partir de ese momento, las empresas, instituciones internacionales y gobiernos inician una carrera a contra reloj para atacar el tema, minimizando las consecuencias de los crímenes de los ciberdelincuentes, detectando y anticipando las amenazas para evitar que se produzcan.

Ante este panorama mundial, Costa Rica, implementa varias acciones preventivas como lo son la creación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), por medio del D.E. Nº 37052-MICITT, por otra parte, desde el 22 de setiembre de 2017 ratifica su adhesión al Convenio sobre Ciberdelincuencia (Convenio de Budapest). En el año 2018, el país es elegido beneficiario del Programa GLACY+ (iniciativa de apoyo del Consejo de Europa para la implementación del Convenio), adicionalmente, el 13 de junio de 2022, se firmó el Segundo Protocolo Adicional al Convenio destinado a mejorar la cooperación y la divulgación de pruebas electrónicas. Por otra parte, se formuló la Estrategia Nacional de Ciberseguridad 2017-2021, el objetivo general de esta estrategia nacional era desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país.(extraído del documento llamado "*Revisión de la Estrategia Nacional de Ciberseguridad (ENC) de Costa Rica (2017)*"), publicado por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

Por lo anteriormente indicado, el MICITT se consolidó como la entidad líder en ciberseguridad a nivel nacional, así mismo, estos avances lograron que el país mejorara la puntuación para el año 2020 del Global Cybersecurity Index (CGI) de la Unión Internacional de Telecomunicaciones (UIT) ya que se situó a Costa Rica en la posición 76 a nivel global mejorando 39 lugares respecto de la medición del 2018.

Esta puntuación se afectó, ya que el domingo 17 de abril del 2022 el grupo de origen ruso Conti inició una serie de ciber ataques (ransomware), en perjuicio de distintas instituciones públicas de Costa Rica, incluido el Ministerio de Hacienda, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Instituto Meteorológico Nacional (IMN), la Radiográfica Costarricense Sociedad Anónima (RACSA), el Ministerio de Trabajo y Seguridad Social (MTSS), el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC) y la Caja Costarricense del Seguro Social (CCSS), solicitando un rescate de 10 millones de dólares estadounidenses a cambio de no liberar la información sustraída del Ministerio de Hacienda.

Como medida de respuesta, el Gobierno emitió el Decreto Ejecutivo No. 43542-MP-MICITT de 2022, declarando Estado de Emergencia Nacional en todo el sector público iniciando el desarrollo e implementación de varias medidas para contrarrestar los efectos de los ciberataques, así como el robustecimiento de la ciberseguridad en el país.

Según indica la INTERPOL, en el sitio web: *https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf* consultado el 13-11-2023 a las 7:42 pm, programa de secuestros de información y datos "*El ransomware, el suplantación de identidad (phishing), las estafas en línea y la intrusión informática son las tendencias de ciberdelincuencia que perciben los países con mayor frecuencia como amenazas "altas" o "muy altas" a nivel mundial."* por otra parte, el The Global Risks Report 2022 del World Economic Forum señala que para el 2020 se tuvo al nivel mundial un incremento del 435% en programa de secuestros de información y datos (ransomware).

Actualmente, se estima que la industria del crimen cibernético vale más de 700 billones de dólares, aunque hay quienes dicen que su valor llega a rondar arriba de un trillón de dólares. Lo que es un hecho, como ya hemos apuntado, es que se trata de una industria en constante ascenso y de gran atractivo para los criminales de la web. Tomado del articulo llamado "Perspectivas Amenazas cibernéticas,

Un peligro en constante evolución" consultado en el sitio web https://www2.deloitte.com/ni/es/pages/about-deloitte/news/2019/amenazas-ciberneticas-un-peligro-en-constante-evolucion.html el 13-11-2023 a las 12 56 pm.

Adicionalmente, el costo de recuperarse de un ciberataque, basado en factores como tiempo de inactividad, costos de red, horas de trabajo, oportunidades perdidas y más, es cada vez más alto. Por ejemplo, el costo total promedio global de una violación de datos alcanzó los US$4,5 millones de dólares en 2023, representando un aumento del 15% en tres años dato proporcionado por IBM, en el informe llamado "Cost of a Data Breach Report 2023" consultado el 13-11-2023 en el link https://www.ibm.com/reports/data-breach, a las 6 30 pm.

Según la Contraloría General de la República (CGR) en la Memoria Anual 2022, en el apartado llamado *"Opiniones y sugestiones: Emergencia Cibernética: obstáculo para la transformación digital y el bienestar social; retroceso para la transparencia y la rendición de cuentas"*, los ciberataques afectaron las labores ordinarias de al menos 45.535 personas funcionarias, afectando 49 tipos de trámites y servicios; y provocando pérdida de ingresos institucionales; así como la pérdida de información, o bien, su calidad o disponibilidad, lo cual incidió en la toma de decisiones, la transparencia y la rendición de cuentas. Hoy en día se estima que estos ataques le han costado al país más de 13 mil millones de colones, dato extraído del periódico digital CRHOY.com en el apartado "La estrategia" el 13-11-2023 a las 6:24 pm en el link:

https://www.crhoy.com/tecnologia/presentacion-de-estrategia-de-ciberseguridad-estuvo-marcada-por-problemas-tecnicos/

De la misma manera, el informe de la CGR resalta que el 68,5% de las instituciones públicas cuentan con niveles medio o alto de riesgo en ciberseguridad, como aliciente a esta alta exposición de riesgo, existen marcadas asimetrías sectoriales, en cuanto a la amenaza potencial de los ciberataques y a los factores que inciden en la vulnerabilidad institucional por todo lo anteriormente mencionado el Gobierno central nacional decide replantear su posición frente a la ciberseguridad en todos los niveles.

Se crea el *"Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional"* consecuencia de la DIRECTRIZ N° 133-MP-MICITT, logrando que el país cuente con un protocolo de nivel nacional que defina las acciones que se deben implementar en el nivel nacional, ante una amenaza de ataque cibernético; además, se desarrolla la Estrategia Nacional de Ciberseguridad 2023-2027, cuyo objetivo es: "*Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y a la ciudadanía de las ciber amenazas".* La meta al año 2027, lograr que el ecosistema digital de Costa Rica sea confiable y contribuya al esfuerzo global para asegurar el ciberespacio.

A raíz de lo anterior es que resulta indispensable que el Ministerio de Educación Pública adopte las medidas necesarias que garanticen la seguridad de la información institucional.

III. Marco Propositivo de la Política

Cumplir a cabalidad con los aspectos mencionados en esta política es responsabilidad compartida de todos los funcionarios para garantizar la protección de los activos de información crítica del MEP. Así mismo, las jefaturas de la Dirección de Informática de Gestión (DIG) y la Dirección de Recursos Tecnológicos para la Educación (DRTE), así como, las que se consideren pertinentes, tienen la responsabilidad de velar por la aplicación de los aspectos descritos en este documento, procurando un comportamiento ético y profesional de sus colaboradores sin comprometer los recursos informáticos de la institución. Al adherirse rigurosamente a esta política, se busca salvaguardar la confidencialidad, integridad y disponibilidad de la información. De igual forma, se pretende mantener la confianza del Ministerio y las partes interesadas.

Todos los funcionarios del MEP son un componente vital del enfoque proactivo hacia la Ciberseguridad. Se espera que todos los funcionarios comprendan y apliquen los principios establecidos en esta política. Además, es esencial cumplir con la legislación de protección de datos presente en la Ley N°8968, Ley de Protección de

la Persona frente al tratamiento de sus datos personales y de delitos informáticos desarrollada en la Ley N°4573, Código Penal y normas conexas.

De la misma manera, las dependencias deben encargarse de sensibilizar a las personas que hagan uso de los recursos informáticos de la institución, sobre la responsabilidad en la gestión de la información para evitar escenarios de fuga de esta.

Para lograr una sólida postura de seguridad, es imprescindible cumplir con las mejores prácticas y normas de seguridad nombradas en este documento, o demás documentos proporcionados por las autoridades competentes del MEP y los entes rectores en la materia. Además, el personal ministerial debe participar activamente en los programas de formación y sensibilización en seguridad, logrando conocimientos actualizados sobre las últimas amenazas y tácticas empleadas por atacantes cibernéticos.

El incumplimiento de esta política y sus directrices expone al MEP a riesgos innecesarios y poner en peligro la seguridad de la información de las personas y de la institución. Como tal, el cumplimiento de esta política es de carácter obligatorio para todos los funcionarios y su inobservancia puede acarrear entre otras posibles responsabilidades administrativas y sanciones disciplinarias. A su vez, se reitera el deber de las personas funcionarias de proceder con la denuncia de toda situación que amerite la intervención de las autoridades judiciales u otras instancias de la Administración, esto según las disposiciones vigentes en los protocolos de actuación que al efecto establezca el Ministerio de Educación Pública y el marco normativo vigente.

3.1. Enunciado central

El MEP cuenta con redes y recursos informáticos institucionales para el uso de sus colaboradores, por lo cual todos deben cumplir pautas de seguridad informática, para prevenir un ataque que atente contra la misma, pérdida de información o cualquier afectación a nivel de Ciberseguridad.

Se proporcionan pautas generales de los elementos que deben ser contemplados para mejorar la seguridad de la información. Esto puede incluir aspectos sobre la gestión de activos de información y manejo de incidentes, la realización de copias de seguridad, la instalación de actualizaciones de software, la identificación y manejo de amenazas, entre otros procesos clave.

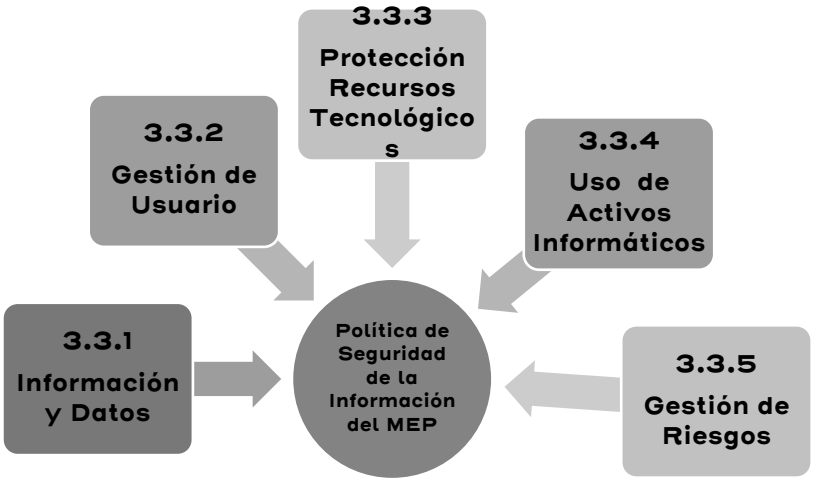
3.2. Objetivo General

El objetivo general de la presente Política se ha definido en los siguientes términos, "*Establecer la política de seguridad de la información MEP, aplicable a la gestión de los recursos tecnológicos de la institución, incluyendo aquellos destinados a los procesos de enseñanza y aprendizaje en los centros educativos.*"

3.3. Definición de Ejes

La presente Política de Seguridad de la Información, se conforma por los siguientes ejes, considerados cada uno como elementos trascendentales a considerar para lograr una Política de Seguridad de la Información del MEP de manera integral.

Imagen 1.



Fuente: Elaboración propia, MEP, 2023.

3.4. Tabla 1. Cadena de Resultados

Tabla 1.

Insumos	Actividades	Productos	Resultados	Impacto
Talento humano especializado Recursos Financieros Recursos tecnológicos Marco legal y regulatorio cibernético Información actualizada en materia.	Desarrollo de procesos de educación sobre las amenazas a la seguridad de la información del MEP.	Conjunto de lineamientos, directrices, manuales, documentos aprobados por parte de las autoridades ministeriales e implementados por parte de los funcionarios MEP y la comunidad educativa.	Afinamiento de las capacidades institucionales para enfrentar de manera prospectiva, actualizada y bajo los más altos estándares de seguridad, un ataque cibernético contra el MEP.	Robustecimiento de la gobernanza de ciberseguridad nacional.
	Realización de controles referentes a las soluciones basadas en software (y hardware) diseñadas para proteger los sistemas de información del MEP.			
	Implementación de medidas de control técnico administrativos que a nivel interno de la DIG y la DRTE se deben incorporar para el aseguramiento de la información del MEP.			
	Implementación de medidas que promuevan una adecuada gestión del riesgo cibernético.			
	Realización de espacios de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio.			
	Implementación de medidas tendientes a vigorizar la infraestructura de la información del MEP.			

Fuente: Elaboración propia, MEP, 2023.

IV. Marco de Actividad y Evaluación

Esta política en seguridad de la información del MEP, es la primera iniciativa institucional que pone sobre la mesa la importancia de abordar con absoluta diligencia este tema, después de lo suscitado en 2022 con los hackeos a diversas instituciones públicas de nuestro país, afectado la continuidad del negocio.

Se parte de una situación en la que el MEP debe ordenar y establecer de manera prioritaria la forma en que se implementarán las medidas de seguridad de la información, para esto se toma en consideración las disposiciones emitidas por parte del MICITT en el *Protocolo para el desarrollo de las acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional, versión 001, en* la *Estrategia Nacional de Ciberseguridad 2023-2027*, así como, otros elementos de orden normativo.

En este sentido, se parte de cero, planteando acciones estratégicas relacionadas con la prevención, detección, la corrección y la coordinación como elementos intrínsecos para lograr la eficacia, eficiencia y confianza en cuanto a la seguridad de la información.

Se busca que los cinco ejes estratégicos, sean la base para la formulación e implementación de todos aquellos lineamientos, directrices, circulares manuales y otros indispensables para lograr el objetivo.

De esta manera se ha de aclarar que el plan de acción que complementa esta estrategia no sólo se limita al cumplimiento de lo ahí planteado, sino, que, además, se brinde el seguimiento correspondiente a fin de que cada producto cumplido sea implementado por los funcionarios MEP y la comunidad educativa.

Para lograrlo será labor preponderante el liderazgo, compromiso y seguimiento que la Dirección de Informática de Gestión aporte dentro de este marco de acción.

4.1. Operacionalización

La Política está conformada por un total de 5 ejes los cuales a su vez comprenden una serie de acciones estratégicas tendientes a garantizar la seguridad de la información del MEP. Cada uno de los ejes se describe a continuación:

Información y Datos hace referencia a los lineamientos, directrices, y otras disposiciones por parte de la DIG y DRTE en donde se establece las medidas que deberán implementar los usuarios del MEP para lograr el cumplimiento y la seguridad de la información.

Gestión de Usuario hace referencia a los lineamientos, directrices, y otras disposiciones por parte de la DIG y DRTE en donde se establece las medidas que deberán implementar los usuarios del MEP para acceder de manera segura la información y establecer los privilegios de acceso de cada usuario.

Protección de Recursos Tecnológicos hace referencia a las soluciones basadas en (software y hardware) diseñadas para proteger la infraestructura tecnológica, así como la información se aloja y se trasmite en la misma.

Uso de Activos Informáticos se refiere a las acciones que cada funcionario del MEP debe adoptar para salvaguardar la información y mantener un entorno seguro de los dispositivos que tiene bajo su responsabilidad. La capacitación y sensibilización son fundamentales para proteger de amenazas los activos del MEP.

Gestión de Riesgos se refiere a los controles administrativos preventivos que proporcionan una base para la forma en que el MEP implementa la gestión de riesgos de la institución, tanto internamente como externamente con terceros. Incluyendo controles para la identificación, análisis y evaluación, asimismo como proteger, detectar, responder y recuperarse ante una vulnerabilidad o materialización que afecte la seguridad de la información.

4.2 Plan de Acción

A continuación, se detalla el plan de acción a desarrollar por parte del MEP. La DIG y DRTE deberán elaborar protocolos, procedimientos y herramientas que describan a detalle las pautas establecidas a continuación. De igual manera la DIG y la DRTE deben informar cuales son los protocolos, procedimientos y herramientas que se encuentran disponibles para los encargados de la revisión y evaluación los implementen en sus auditorias.

De acuerdo con el Decreto Ejecutivo 38170-MEP, le corresponde a la Dirección de Planificación Institucional y en forma específica al Departamento de Programación y Evaluación, la revisión de los planes operativos y la realización de las evaluaciones y la posterior realimentación de los hallazgos para las autoridades superiores del MEP.

Para la elaboración de la metodología por utilizar, se toma como base lo señalado por el Ministerio de Planificación y Política Económica (MIDEPLAN), como rector del Sistema Nacional de Planificación (SNP) y del Sub-sistema Nacional de Evaluación (SINE).

Establece MIDEPLAN que el seguimiento se centra en conocer el avance de las metas establecidas en el Plan Operativo Anual, comparando los resultados programados con los resultados alcanzados; la evaluación por su parte es una valoración sistemática sobre algún aspecto (diseño, gestión, resultados) de las intervenciones públicas que contribuye a: i) apoyar la toma de decisiones en la gestión pública basada en evidencia; ii) promover la mejora continua y el aprendizaje; y iii) ampliar los mecanismos de rendición de cuentas disponibles. Los resultados de dicho seguimiento deberán ser informados al Despacho Ministerial y deberá especificar las acciones necesarias que se ejecutarán en aquellas metas que muestran algún rezago.

4.3. Prácticas asociadas a cada eje

En las pautas descritas a continuación, se describen aspectos generales, reglas y recomendaciones para mantener un nivel adecuado de seguridad de la información en el Ministerio de Educación Pública (MEP); procurando la seguridad, el resguardo, confidencialidad, integridad y disponibilidad de la información, así como las responsabilidades que conllevan. Estos lineamientos contemplan las normativas vigentes emitidas por el MICITT, en la cual se abarcan generalidades que unificarán criterios y términos relacionados a los lineamientos técnicos establecidos por las autoridades competentes del MEP, constituyéndolos como complemento para procurar la seguridad de la información de la institución.

Estas pautas pueden incluir directrices sobre la gestión del uso adecuado del correo electrónico y las redes, la clasificación de la información, el control de acceso, la protección de datos personales, relación con terceros entre otros aspectos.

Se procuran también, medidas técnicas y físicas que se deben implementar en todas las dependencias MEP para proteger la información y los sistemas. Esto puede incluir el uso de firewalls, cifrado, sistemas de detección de intrusiones, políticas de limpieza de escritorios, seguridad física en los centros de datos, entre otros aspectos.

Se establecen requisitos de capacitación y sensibilización en seguridad de la información para los funcionarios. Esto puede incluir programas de capacitación periódicos, pruebas de conocimientos, campañas de sensibilización y actividades de divulgación.

EJE INFORMACIÓN Y DATOS

Sobre la protección de datos

1. Cuando sea requerido recopilar información en bases de datos o afines, con el fin de garantizar el principio de autodeterminación informativa, el MEP, sus dependencias y funcionarios deben especificar al usuario o encargado legal el tipo de información que se recopila y su destino, esto según las disposiciones vigentes en la Ley N° 8968, Ley de Protección de la Persona frente al tratamiento de sus datos personales, entre estos datos es posible detallar datos personales de acceso irrestricto, datos personales de acceso restringido y datos sensibles. La recopilación de información asociada a datos personales de acceso restringido y datos sensibles, en atención al artículo 8 incisos e) y f) de la Ley N° 8968, se encuentra autorizada al MEP, esto con el fin de garantizar la adecuada prestación de servicio público de educación y la eficaz actividad ordinaria de la Administración. No obstante, esta atribución no es libre y la información solicitada debe ser adecuada a los fines para los que fue recolectada, los cuales deben ser determinados, explícitos y legítimos. Adicionalmente, los datos no deberán ser tratados posteriormente de manera incompatible con los motivos con que se recabaron; sin embargo, es posible usarlos para fines históricos, estadísticos o científicos, siempre que se establezcan las garantías oportunas para salvaguardar los derechos implicados. Todo lo anterior, considerando que es obligación de la Administración y el MEP, garantizar la seguridad y confidencialidad del tratamiento de los datos.
2. El funcionario o instancia responsable, debe verificar según la clasificación de los datos que se van a recabar y de acuerdo con ésta, determinar si es requerido brindar el respectivo consentimiento informado. Se debe considerar además que el consentimiento es tanto para el tratamiento de los datos y para la transferencia de estos en caso de ser necesario. El mismo se

emitirá según las disposiciones vigentes en la Ley N° 8968 y su Reglamento, Decreto Ejecutivo N° 37554-JP.

3. Se debe describir en el protocolo de usos de los datos, cómo las personas titulares de la información o sus encargados legales pueden acceder, corregir, actualizar o solicitar la eliminación de su información personal, esto al amparo del artículo 7 de la Ley N° 8968. También debe explicar sus derechos con respecto al uso de sus datos personales.
4. Como desarrollo del artículo 10 de la Ley N° 8968, se deben describir en el protocolo de usos de los datos, las medidas de seguridad implementadas para proteger los datos personales de supuestos como el acceso no autorizado, pérdida, alteración o divulgación indebida, Esto puede incluir el uso de cortafuegos, cifrado, políticas de acceso restrictivas y otras medidas de seguridad.
5. En atención al artículo 14 de la Ley N° 8968, los responsables de las bases de datos MEP, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en dicha norma. Sin embargo, como excepción a la autodeterminación informativa de las personas, el artículo 8 inciso d) de la Ley N° 8968 de cita, habilita el funcionamiento y traslado de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, esto previo al desarrollo del proceso se anonimizarían de datos, a efecto de que estos no contengan datos personales identificables. El traslado de bases de datos a terceros ya sea para procesamiento, análisis u otros fines habilitados a nivel normativo, debe contar con la documentación que establezca los procesos y las medidas tomadas para garantizar la protección de los datos compartidos.
6. Cada dependencia MEP debe determinar el período de retención de los datos personales y los criterios utilizados para determinar este período.
7. El Ministerio tiene el deber y se reserva el derecho de cambiar su política de protección de datos en cualquier momento y cómo

se comunicarán estos cambios a las personas afectadas, para garantizar que siga siendo relevante y eficiente en un entorno cambiante.

Sobre categorización de la información

1. Deben utilizarse las categorías claramente definidas por la ley N°8968 para catalogar la información según su nivel de confidencialidad. La categorización debe realizarse de acuerdo con lo establecido por la normativa vigente.
2. Cada categoría debe definirse en términos de su contenido y los criterios utilizados para asignar la categorización. Esto ayuda a los funcionarios a comprender qué tipo de información se debe considerar en cada categoría.
3. El funcionario o dependencia responsable de la recopilación de la información debe asignar la categoría de la información basándose en la ley 8968. Esto puede incluir personal de seguridad de la información o personas responsables de cada departamento o unidad de la institución.
4. Deben desarrollarse procedimientos claros para catalogar la información. Esto puede incluir la documentación de los próximos pasos, la revisión y aprobación de las categorizaciones por parte de los funcionarios responsables y la implementación de herramientas o sistemas de gestión de categorizaciones según sea necesario.
5. Las categorías de información se pueden etiquetar y mostrar en documentos físicos y electrónicos utilizando una variedad de formatos. Esto puede incluir marcas de agua, marcas de color, encabezados especiales o metadatos asociados con archivos electrónicos.
6. Definir cómo se gestionará el acceso y el intercambio de información teniendo en cuenta su tipo de categorización. Esto puede incluir permisos basados en roles y controles de acceso, así como protocolos o convenios para compartir información entre dependencias o terceros, así como los deberes y responsabilidades de las partes involucradas.
7. Las direcciones a cargo de la gestiones administrativas y educativas deben brindar a los funcionarios capacitación y

sensibilización sobre las políticas de categorización de la información implementar actualizaciones en etapas en lugar de actualizar todos los sistemas a la vez. Esto le permite evaluar el impacto de una actualización en un grupo más pequeño antes de implementarla en toda la institución. Los funcionarios deben comprender los criterios de categorización, el impacto de la categorización errónea y las mejores prácticas para proteger la información.

8. Los criterios de categorización de la información deben ser actualizados en los documentos internos según lo dispuesto en la ley N°8968. Esto asegura que la categorización siga siendo relevante y eficiente a medida que cambien las necesidades y los requisitos de la institución.

Sobre almacenamiento y copias de seguridad

1. Las direcciones a cargo de la gestiones administrativas y educativas deben definir el área técnica responsable de realizar los respaldos de información, con qué frecuencia y cuando mantenerse como una prioridad.
2. Las direcciones a cargo de la gestiones administrativas y educativas deben definir los métodos y técnicas utilizados para almacenar datos de forma segura. Esto puede incluir sistemas de almacenamiento en disco, almacenamiento en la nube, u otras soluciones, según las necesidades y requisitos de la institución.
3. Las direcciones a cargo de la gestiones administrativas y educativas deben de definir la ubicación o ruta en la cual la información debe ser almacenados de manera segura.
4. Las direcciones a cargo de la gestiones administrativas y educativas deben definir en conjunto con las dependencias y los mandatos del Archivo Central MEP, si se requieren establecer períodos de retención de datos de respaldos de información que ya no sean necesarios, los mismos deben determinarse de acuerdo con las leyes vigentes como por ejemplo “Ley del Sistema Nacional de Archivos, Ley N° 7202”, reglamentos aplicables y las necesidades operativas del Ministerio. Esto ayudará a garantizar

que los datos se conserven durante un período de tiempo adecuado y se eliminen de forma segura cuando así corresponda.

5. Las direcciones a cargo de la gestiones administrativas y educativas deben establecer un plan de respaldo regular que defina la frecuencia, la hora y los datos que se respaldarán. Esto incluye realizar copias de seguridad completa, diferencial o incremental según sea necesario y programar trabajos de copias de seguridad para evitar la interrupción de las operaciones normales.
6. Las direcciones a cargo de la gestiones administrativas y educativas deben implementar medidas de seguridad físicas y lógicas para proteger las copias de seguridad almacenadas. Esto puede incluir el uso de sistemas de encriptación para proteger los datos y almacenarlos en un lugar seguro contra incendios, inundaciones u otros riesgos.
7. Las direcciones a cargo de la gestiones administrativas y educativas deben verificar las copias de seguridad regularmente para garantizar que los datos se respalden correctamente y se puedan restaurar sin problemas. Esto ayuda a garantizar la integridad de los datos de respaldo y la eficiencia del proceso de recuperación.
8. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben realizar un protocolo de respaldo de información en carpetas institucionales de uso compartido para oficinas centrales y direcciones regionales o los repositorios de almacenamiento compartido asociados a las cuentas institucionales asignadas a los funcionarios y a los centros educativos.
9. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben mantener diversos respaldos de las copias de seguridad para reducir el tiempo de recuperación de la información y las operaciones.
10. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben contar con una lista de todos los privilegios que tiene un usuario para que estos sean revocados cuando no esté activo

11. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben crear un protocolo de eliminación segura de información, contemplando mecanismos de eliminación segura a nivel del software como de hardware, contemplando todos los equipos que el MEP utilice en Centros educativos, oficinas centrales, o equipos de arrendamiento.
12. Cada dependencia debe definir las responsabilidades y roles de los miembros del equipo con respecto al almacenamiento y respaldo de datos. Esto incluye la designación de personas responsables de las actividades de respaldo y recuperación y la asignación de responsabilidades para monitorear y hacer cumplir las políticas establecidas.
13. Cada dependencia debe incluir disposiciones para el mantenimiento y la actualización de los sistemas y tecnologías utilizados para almacenar y realizar copias de seguridad de los datos. Esto incluye seguir las mejores prácticas, evaluar regularmente las soluciones de respaldo y almacenamiento e implementar mejoras o actualizaciones según sea necesario.
14. Revisar y actualizar regularmente las pautas mencionadas para garantizar su relevancia y eficiencia en un entorno cambiante.

EJE GESTION DE USUARIO

Sobre las credenciales

1. La DIG debe establecer por escrito las normas de requisitos de complejidad para las contraseñas, como la longitud mínima, el uso de caracteres alfanuméricos, letras mayúsculas y minúsculas, números y símbolos especiales. Cuanto más compleja sea la contraseña, más difícil será adivinarla o descifrarla. Una buena práctica es utilizar frases en las contraseñas, cumpliendo siempre los requisitos de complejidad.
2. Es necesario realizar cambios periódicos de contraseña. Esto ayuda a evitar el uso a largo plazo de contraseñas filtradas y proporciona una capa adicional de seguridad.

3. Debe evitarse la reutilización de contraseñas antiguas. Cada cuenta o servicio debe tener una contraseña única para reducir el impacto del descifrado de contraseñas.
4. Se debe enfatizar la importancia de no compartir las contraseñas y mantenerlas seguras. Se pueden recomendar administradores de contraseñas o soluciones de almacenamiento cifrado para la protección de contraseñas.
5. La autenticación de múltiples factores puede recomendarse o requerirse si el recurso se encuentra disponible, en caso de que el recurso se encuentre disponible, para agregar una capa adicional de seguridad. Esto incluye el uso de otro método de verificación, como un código enviado por mensaje de texto, una aplicación de autenticación o un dispositivo físico.
6. Las direcciones de Informática de Gestión, Recursos tecnológicos en conjunto con las oficinas encargadas de divulgar información y la oficina encargada de capacitación deben de velar porque los funcionarios tengan conocimiento sobre las buenas prácticas de contraseñas y los riesgos asociados cuando estas son débiles o mal administradas. Los usuarios deben ser conscientes de la importancia de proteger sus credenciales y tomar medidas para garantizar su seguridad.
7. La DIG debe encargarse del monitoreo y vigilancia para detectar actividades sospechosas o intentos de acceso no autorizado. Esto puede incluir el registro de intentos de inicio de sesión fallidos o el registro de actividades inusuales.
8. Las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente por el ente encargado de la ciberseguridad para garantizar que siga siendo relevante y eficiente en un entorno cambiante.

Sobre control de acceso

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben especificar métodos y requisitos para la autenticación de usuarios para garantizar que sólo el personal autorizado pueda acceder a los sistemas y datos. Además, deben

definir mecanismos de autorización que especifiquen los niveles de acceso y los privilegios otorgados a cada usuario.

2. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben de establecer requisitos para crear y gestionar contraseñas seguras. Esto puede incluir estándares de complejidad, periodicidad, prohibir el uso de la misma contraseña en diferentes plataformas y se recomienda implementar mecanismos para proteger y almacenar contraseñas de forma segura.
3. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben abordar el control de acceso físico a equipos y recursos de información críticos. Esto puede incluir el uso de tarjetas de acceso, cámaras de seguridad, sistemas de registro de visitantes y acceso restringido a áreas sensibles.
4. Debe de existir una bitácora donde se documente la información de las personas que ingresen a los centros de cómputo e indique por lo menos nombre completo, número de identificación, la fecha, hora y una descripción del motivo de ingreso.
5. En cada Unidad Operativa debe de existir una bitácora que documente la información de las personas que ingresan al edificio que sean ajenas al mismo.
6. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación definirán, los procesos de gestión de usuarios y cuentas en el sistema de información. Esto puede incluir la creación y eliminación de cuentas de usuario, un protocolo de eliminación de privilegios de acceso, en caso de cese de funciones laborales. También debe existir una revisión y actualización periódica de los permisos y la desactivación inmediata privilegios de las cuentas de usuario cuyos accesos no hayan sido revocados luego del cese.
7. La Dirección de Informática en Gestión ejecuta el proceso establecido para inactivación, desactivación o eliminación de las cuentas de correo electrónico institucional asignadas a los funcionarios.
8. Donde sea posible y aplicable debe haber un control de acceso basado en roles, donde los usuarios tienen acceso solo a los recursos y datos necesarios para realizar sus funciones. Esto

ayuda a reducir el riesgo limitando el acceso a información confidencial y reducir las amenazas potenciales.

9. Debe existir un registro de acceso a sistemas de información el cual pueda ser consultado y analizado con la finalidad de identificar posibles actividades sospechosas o infracciones de seguridad.
10. Si se permite el acceso remoto a los sistemas de la institución, las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer lineamientos y requisitos específicos para habilitar este acceso. Esto puede incluir la autenticación de multi factores y la limitación de los dispositivos y redes a los que se puede acceder de forma remota.
11. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación en conjunto con la oficina encargada de la capacitación en el ministerio deben incluir un programa de capacitación y sensibilización sobre control de acceso que informe a los usuarios sobre las mejores prácticas, los riesgos asociados y la responsabilidad individual para la protección de la información y el cumplimiento de la política.
12. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación definirán, las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente para garantizar que siga siendo relevante y eficiente en un entorno cambiante.

Gestión de cuentas de usuario

Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben:

1. Establecer un procedimiento formal para crear nuevas cuentas de usuario, definiendo requisitos y responsabilidades para su aprobación y verificación.
2. Velar porque todos los funcionarios que tengan acceso a equipos institucionales utilicen políticas de autenticación sólidas, como el uso de contraseñas seguras y autenticación de múltiples factores (MFA) si el recurso se encuentra disponible.
3. Definir los movimientos de personal que deben ser notificados a la dependencia encargada de actualizar la gestión de cuentas de usuario y privilegios.

4. Contar con una lista de todos los privilegios que tiene un usuario para que estos sean revocados cuando no esté activo
5. Establecer requisitos para la gestión de contraseñas, como la longitud mínima, el uso de caracteres especiales y la no reutilización de contraseñas anteriores, considerando también el uso de soluciones de gestión de contraseñas seguras.
6. Establecer los niveles de privilegios y permisos basados en el principio de menor privilegio, revisándolos periódicamente para garantizar que sean adecuados y actualizados.
7. La dirección de Informática en Gestión ejecuta el proceso para desactivar y eliminar cuentas que ya no sean necesarias, estableciendo plazos ya definidos para hacerlo después de la terminación de la relación con la dependencia.
8. Implementar mecanismos de bitácora para registrar actividades de las cuentas y supervisar regularmente los registros, para detectar posibles anomalías o actividades sospechosas.
9. Brindar capacitación a los usuarios sobre las mejores prácticas de seguridad de las cuentas de usuario, incluyendo como mínimo: la importancia de mantener contraseñas seguras y la responsabilidad de proteger sus propias cuentas.
10. El manejo de cuentas de usuario debe cumplir con las regulaciones y estándares de usos de datos aplicables, adaptándose a los requisitos específicos del Ministerio.
11. Mantener un registro de las solicitudes de creación de cuentas de usuario por parte de la dependencia gestora del servicio, y que el mismo pueda ser consultado, en caso de ser requerido.
12. Definir las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente para garantizar que siga siendo relevante, aplicable y efectiva en un entorno cambiante. Esto debe incluir como mínimo la revisión de los procesos existentes, la evaluación de nuevos actores y la incorporación de las mejores prácticas de seguridad de la información.

EJE PROTECCIÓN DE RECURSOS TECNOLÓGICOS

Sobre las actualizaciones de software

Las direcciones a cargo de la gestiones administrativas y educativas en conjunto con los encargados de la administración de software deberán:

1. Crear un proceso para evaluar las actualizaciones de software disponibles. Esto puede incluir monitorear los comunicados de seguridad del proveedor y las notas de la versión, evaluar cambios y mejoras y considerar las dependencias y los impactos potenciales en los sistemas existentes.
2. Se debe aplicar como buena práctica priorizar las actualizaciones en función de su importancia. Las actualizaciones que corrigen vulnerabilidades de seguridad o errores críticos deben tener una alta prioridad, mientras que las actualizaciones que son menos importantes o están relacionadas con funciones no esenciales se pueden programar de manera más flexible.
3. Establecer un plan y un proceso para la planificación de la actualización. Esto puede incluir establecer tiempos específicos para aplicar actualizaciones según las necesidades de la institución y el horario comercial, y evitar períodos de alta actividad o impacto en la productividad.
4. Deberán realizar pruebas de compatibilidad para garantizar que el nuevo software no entre en conflicto con otros sistemas o aplicaciones utilizados en la institución. Estas pruebas se deben de realizar antes de implementar una actualización en un entorno de producción.
5. Considerar habilitar las actualizaciones automáticas para ciertos tipos de software o sistemas. Esto ayuda a garantizar la implementación oportuna de parches y actualizaciones críticos sin la intervención manual del usuario.
6. Analizar la implementación de actualizaciones en etapas, en lugar de actualizar todos los sistemas a la vez. Esto le permite evaluar el impacto de una actualización en un grupo más pequeño antes de implementarla en toda la institución. “Esto en entornos que usan múltiples sistemas o dispositivos.”

7. Se debe contar con procedimientos de exijan copia de seguridad de los datos y puntos de restauración de datos antes de aplicar actualizaciones importantes. Esto permite revertir los cambios si algo sale mal o falla durante el proceso de actualización y garantiza la disponibilidad e integridad de los datos.
8. Establecer la obsolescencia y el ciclo de vida esperado del software y los sistemas utilizados en la institución si lo mismo corresponde. Esto ayuda a garantizar actualizaciones periódicas y reemplazar o actualizar los sistemas obsoletos para mantener la seguridad y la eficiencia.
9. Las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente para garantizar su relevancia y eficacia en un entorno cambiante.

Sobre uso de redes

Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben:

1. Definir los requisitos de acceso y autorización para la red de la institución. Esto puede incluir la autenticación de usuarios, la concesión de privilegios basados en roles y la aplicación de controles de acceso para proteger la red del acceso no autorizado.
2. Establecer reglas claras para asegurar el uso aceptable de la red de una institución. Esto puede incluir la prohibición de actividades ilegales, el uso de recursos en línea para fines personales, el acceso a contenido inapropiado o la participación en actividades que puedan comprometer la seguridad de la información.
3. Abordar las medidas de seguridad necesarias para proteger la red de posibles amenazas y vulnerabilidades. Esto puede incluir el uso de sistema de filtrado el tráfico saliente y entrante en las redes (firewall), sistemas de detección y prevención de intrusiones, encriptación de datos, segmentación de redes y actualizaciones periódicas de software y programa integrado para el funcionamiento de los dispositivos (firmware).
4. Incluir pautas para proteger los datos mientras se envían a través de la red. Esto puede incluir el uso de protocolos de comunicación

seguros como HTTPS y el cifrado de datos confidenciales para garantizar su confidencialidad e integridad.

5. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación definirán mecanismos para monitorear y registrar la actividad de la red para detectar y responder a posibles incidentes de seguridad. Esto puede incluir la supervisión de registros de eventos, registros de autorización y comprobaciones periódicas para detectar actividades inusuales o sospechosas.
6. Abordar la protección contra el programa malicioso (malware) cibernético. Esto debe incluir el uso de soluciones antivirus y detector de programas maliciosos (antimalware) actualizadas, la implementación de políticas relacionadas con el uso de dispositivos de almacenamiento extraíbles y la sensibilización para detectar y prevenir ataques de suplantación de identidad (Phishing).
7. Establecer el requisito de aplicar periódicamente actualizaciones y parches de seguridad a los dispositivos y sistemas conectados a la red. Esto garantiza que se solucionen las vulnerabilidades conocidas y que se actualice el sistema.
8. Establecer si se permite el uso de redes externas, se debe proporcionar una guía clara sobre el uso seguro de estas redes y las precauciones que se deben tomar para proteger la información de la institución.
9. Definir las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente para garantizar que siga siendo relevante y eficiente en un entorno cambiante.

Seguridad de la información en sistemas que acceden por medio de la red

En este apartado se indica que se deben seguir directrices que servirán para un manejo seguridad de la información en redes, bases de datos y sistemas; el mismo incluye: Protección de ingresos a sistemas en la nube, políticas de ingreso y/o acceso a la red del MEP desde servicios de internet, ingreso a la red interna utilizando conexión privada y segura para el uso de internet (VPN), consultas a centro de datos (datacenters) del MEP desde servicios específicos,

servicios que pueden entrar desde la red interna de la institución. De esta manera, se pretende alcanzar un nivel de seguridad óptimo para proteger a los recursos y sistemas de la institución; protegiendo a los mismos de posibles ataques de seguridad generados desde oficinas centrales, dependencias o redes externas.

Es importante, destacar que en ciertos apartados se utilizan expresiones como: en caso de que el recurso esté disponible o en caso de ser posible. Esto debido a que existen ciertos recursos que cuentan con licencia y es posible que las necesidades institucionales cambien al igual que los recursos que están siendo utilizados, en este caso, el uso de estos se recomienda como una buena práctica.

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer mecanismos para una correcta autenticación y control de acceso, con la finalidad de garantizar que solo los usuarios autorizados tengan acceso a los sistemas. Incluyendo el uso de contraseñas seguras, la gestión de roles y permisos y la autenticación múltiple (MFA) en caso de ser disponible.
2. Se solicita a las dependencias que cuenten con los recursos requeridos, cifrar los datos durante el almacenamiento y la transmisión. Utilizar protocolos de transferencia de datos seguros en internet.
3. Se solicita a las dependencias realizar copias de seguridad periódicas y procedimientos de recuperación de datos para protegerse contra la pérdida de datos. Los datos importantes deben estar respaldados de forma segura y sean recuperables en caso de un incidente. Se deben realizar periódicamente pruebas de recuperación de respaldos para asegurar que los mismos puedan ser restablecidos exitosamente en caso de requerirlo.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben monitorear y analizar continuamente los eventos de seguridad en los sistemas en la nube. Usar sistema de detección de intrusos (IDS), análisis de registros y sistemas de gestión de eventos e información de seguridad en caso de que los recursos estén disponibles.

5. Los sistemas deben instalarse y operar sobre plataformas tecnológicas seguras, que procure la máxima accesibilidad a los servicios de información que se brindan a las personas usuarias internas y externas.
6. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben mantener las aplicaciones y sistemas en la nube actualizados con los últimos parches de seguridad.
7. Cada dependencia debe mantener un inventario actualizado de los componentes y versiones de software utilizado y aplicar los parches de seguridad adecuados.
8. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer reglas claras para crear y administrar contraseñas. Usar contraseñas seguras que incorporen letras, números y caracteres especiales. Se recomienda el uso de frases compuestas y se debe exigir cambiar su contraseña con frecuencia. Impedir el uso de contraseñas comunes o débiles.
9. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben implementar programas de sensibilización y educación sobre Ciberseguridad para todos los usuarios. Capacitar a los funcionarios sobre las mejores prácticas de seguridad, como la detección de suplantación de identidad (Phishing) en correo electrónico, la gestión segura de contraseñas y la detección de actividades sospechosas.
10. Las dependencias deben usar una *conexión privada y segura para el uso de internet* (VPN) confiables y seguras que ofrezcan protocolos de seguridad, cifrados sólidos como protocolo de seguridad de la información y autenticación de multi factores (MFA) para el acceso cuando sea posible. Esto agrega una capa adicional de seguridad al requerir una segunda forma de autenticación, como un código generado por una aplicación móvil o una clave cifrada (token) de seguridad, lo que permite proteger las conexiones desde ubicaciones externas cuando el recurso esté disponible.

11. Las dependencias siempre deben tener instalado el software conexión privada y segura para el uso de internet (VPN) más reciente y estable en los dispositivos debido a que las actualizaciones a menudo incluyen correcciones de seguridad y correcciones para vulnerabilidades conocidas, por lo que mantener su software actualizado es esencial para mantener el nivel adecuado de protección.
12. En caso de que la dependencia tenga a cargo el desarrollo de sistemas de información, se recomienda realizar periódicamente análisis de vulnerabilidades que pueda incluir: evaluaciones de seguridad y pruebas de penetración en los sistemas, con la finalidad de identificar posibles brechas de seguridad que supongan una amenaza para la seguridad de la información. Se debe abordar cualquier problema encontrado durante esta revisión utilizando el proceso de incidencia.
13. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben desarrollar un protocolo claro de respuesta a incidentes para administrar y mitigar de manera efectiva cualquier brecha de seguridad o incidentes de red. Determinar los pasos a seguir, quién es responsable y los medios de comunicación requeridos en caso de una brecha de seguridad.
14. Las dependencias deben utilizar una solución de sistema de filtrado el tráfico saliente y entrante en las redes (firewall) y filtrado de tráfico de red para controlar y limitar las conexiones entrantes y salientes a las redes institucionales. Para bloquear tráfico no deseado y proteger la red contra amenazas externas.
15. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación en caso de que se gestione convenios formales con otras instituciones con que se comparten recursos, incluyendo evaluaciones de seguridad de la información, actualización de las direcciones que identifican los dispositivos en la red que están en uso, desuso y demás temas de interés en relación en la transmisión de datos entre ambas instituciones y su seguridad. Estos acuerdos deben definir claramente las responsabilidades y

obligaciones de cada parte con respecto a la protección de la información y los activos confidenciales de la institución.

16. Las dependencias deben de aplicar lo indicado en el apartado de credenciales de este documento para garantizar que las contraseñas sean robustas y únicas para la cuenta una conexión privada y segura para el uso de internet (VPN) y sistemas de información.
17. Las dependencias deben mantener los dispositivos protegidos con un software antivirus actualizado y un sistema de filtrado el tráfico saliente y entrante en las redes (firewall) personal. Mantener su aplicación de conexión privada y segura para el uso de internet (VPN) y el sistema operativo actualizados con los últimos parches de seguridad.
18. Cuando se utiliza un equipo institucional o se realiza una conexión o acceso a un sistema o sitio del Ministerio no se deben usar redes inalámbricas públicas, no seguras o de libre acceso. Estas redes están sujetas a ataques de intermediarios o escuchas ilegales, lo que puede afectar la seguridad de la conexión.
19. Al usar un servicio de conexión privada y segura para el uso de internet (VPN) institucional, cerrar la conexión después de finalizar la sesión en la intranet. Mantener abierta innecesariamente una conexión privada y segura para el uso de internet (VPN) puede aumentar los riesgos de seguridad, ya que proporciona a un atacante una ruta potencial para obtener acceso a la red o dispositivos del Ministerio.
20. No compartir credenciales de una conexión privada y segura para el uso de internet (VPN) con otras personas. Mantener siempre las credenciales privadas y no almacenarlas en dispositivos compartidos o en ubicaciones accesibles para otros usuarios.
21. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer el monitoreo de los registros de una conexión privada y segura para el uso de internet (VPN) con regularidad buscando detectar y responder rápidamente a actividades sospechosas o no autorizadas en la cuenta de conexión privada y segura para el uso de internet (VPN).

22. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben contar con un mapa de red y documentar los componentes de red, de la misma manera, se debe contar con un mapa contemple enumere y documente todas las conexiones hacia los servidores, sistemas servicios y redes de institucionales.

23. Las dependencias deben de contar con una segmentación de red para uso de invitados.

24. En las dependencias cuando sea requerido la conexión de dispositivos externos, se debe de hacer una gestión y registro de los dispositivos electrónicos personales creando un listado de dispositivos permitidos y no permitidos dentro de la red institucional.

25. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben realizar protocolos y usar dispositivos que controlen el acceso a la red institucional.

26. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben contar con un protocolo de gestión de registros digital automatizado que detalle y almacene y analice los mismos, incluyendo datos de fecha y hora, categoría y descripción.

27. Las dependencias deben contar con un inventario de dispositivos de red, tales como: impresoras, escáner, entre otros, que permitan acceder a recursos dentro de la misma.

28. Las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente para garantizar que siga siendo relevante y eficaz en un entorno cambiante. Esto puede incluir la revisión de contratos existentes, la evaluación de nuevos proveedores y la incorporación de las mejores prácticas de seguridad de la información.

EJE USO DE ACTIVOS INFORMÁTICOS

Sobre la seguridad de la información en el puesto de trabajo

1. Los trabajadores deben acatar disposiciones para usar contraseñas seguras, como elegir contraseñas complejas, no compartir contraseñas, no escribirlas o respaldarlas en medio físicos de fácil acceso y cambiarlas regularmente. Además, Se recomienda: Utilizar la autenticación de múltiple cuando el recurso se encuentre disponible.
2. Los funcionarios deben hacer uso adecuado de los sistemas informáticos y de comunicación en el lugar de trabajo. Esto puede incluir no acceder a sitios web no relacionados con el trabajo, no realizar descargas de software no autorizadas y el uso responsable de los recursos del ministerio.
3. La DIG y DRTE deben implementar medidas de seguridad para proteger los dispositivos informáticos institucionales. Esto puede incluir establecer una contraseña o un bloqueo de pantalla, establecer métodos de recuperación y borrado remoto en caso de robo, cifrar los datos almacenados en su dispositivo e instalar un software de seguridad actualizado.
4. La DIG y DRTE establecerán pautas para utilizar el correo electrónico de manera segura: brindando el apoyo para identificar correos electrónicos maliciosos o de suplantación de identidad (phishing) e instar a no abrir archivos adjuntos sospechosos y no divulgar información confidencial en el correo electrónico sin el permiso adecuado.
5. Cada usuario debe de retirar todos los días cualquier información que pueda ser considerada sensible del escritorio o sitio de trabajo.
6. Los funcionarios deben acatar las medidas de capacitación, aprendizaje de destrezas, relacionada con temas relevantes de nuestra actualidad, tales como Ciberseguridad, resguardo de la información, entre otros emitidas por las direcciones o departamento a cargo de desarrollar las capacitaciones antes descritas.

7. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación establecerán los lineamientos, tomando como referencia la ley de archivo, para la gestión de la seguridad de los documentos, como la clasificación adecuada de la información, el uso de sistemas de almacenamiento seguro y la eliminación adecuada de los documentos confidenciales que ya no estén activos o sean obsoletos cuando ya no se necesitan.
8. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación definirán en conjunto las medidas de formación y sensibilización periódicas sobre las prácticas de seguridad de la información en el lugar de trabajo. Esto puede incluir educación sobre riesgos de seguridad, mejores prácticas de seguridad, reconocimiento de ataques cibernéticos y responsabilidad personal para proteger la información.
9. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación definirán en conjunto las políticas de acceso y gestión de privilegios de los funcionarios a los sistemas y la información del ministerio. Esto incluye la autorización basada en funciones y las revisiones periódicas de acceso para garantizar que solo se otorguen los permisos necesarios.
10. Los funcionarios deben tener en cuenta las leyes 8968 Ley de Protección de la personal frente al tratamiento de sus datos personales, 7202 Ley del Sistema Nacional de Archivos y sus Reglamentos, 8148 Ley de Delitos Informáticos, Política de la seguridad de la información– Ministerio de Educación Pública y reglamentos aplicables relacionados con la seguridad de la información.
11. Las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente por las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación de manera conjunta para garantizar que siga siendo relevante y eficiente en un entorno cambiante.

Sobre el uso del correo electrónico

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación, en conjunto norman que el correo electrónico del ministerio solo se debe usar para fines laborales y no para uso personal.
2. Los funcionarios deben ser conscientes de la importancia de mantener la confidencialidad de la información enviada por correo electrónico. Deben estar capacitados para identificar y manejar información confidencial y tener pautas claras sobre cómo encriptar información confidencial y archivos adjuntos.
3. Debe existir un uso adecuado de las cuentas de correo electrónico institucional de los funcionarios. Esto incluye prohibir el intercambio de credenciales de inicio de sesión, notificación inmediata si las credenciales se pierden o son robadas y tomar medidas para proteger las cuentas de correo electrónico de posibles ataques.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación, debe brindar asesoramiento sobre el uso de herramientas de seguridad relacionadas con el correo electrónico, como software antivirus y filtros de correo no deseado. Los funcionarios deben ser conscientes de la importancia de actualizar periódicamente los sistemas y de informar sobre cualquier incidente de seguridad relacionado con el correo electrónico.
5. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación, debe capacitar a los funcionarios sobre mejores prácticas de uso del correo electrónico, lo que incluye evitar el envío de mensajes no solicitados (spam), la importancia de verificar la precisión y autenticidad de los mensajes recibidos, y no distribuir software o programa maliciosos (malware) en su contenido.
6. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben sensibilizar a los funcionarios sobre sus responsabilidades en la detección y notificación de incidentes de seguridad relacionados con el correo electrónico. Necesitan saber

a quién informar si sospechan de suplantación de identidad (Phishing), spam o actividad sospechosa.

7. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación son el ente responsable de velar que las pautas mencionadas en este apartado se revisen y actualicen regularmente para garantizar que siga siendo relevante y eficiente en un entorno cambiante.

Sobre uso aceptable de los recursos de información tecnológica.

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben definir claramente qué se considera uso aceptable de los recursos de información tecnológica de la institución. Esto debe incluir la prohibición de actividades ilegales, inapropiadas o no autorizadas y el cumplimiento de las políticas y regulaciones internas y externas pertinentes.
2. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación establecerán las medidas para proteger la información confidencial y sensible de la institución. Contemplando como mínimo prohibir la divulgación, copia o modificación no autorizadas de la información y el uso de medidas de seguridad como el cifrado de datos, la administración adecuada de contraseñas y el acceso solo a los datos necesarios para realizar las funciones laborales.
3. Las dependencias deben de asignar un responsable o grupo de responsables para cada equipo informático institucional, que deben de velar por la salvaguarda de estos.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación establecerán pautas para el uso adecuado de los recursos tecnológicos de la institución, como computadoras, dispositivos móviles, software y redes. Esto debe incluir restricciones en la instalación de software no autorizado, acceso a sitios web no relacionados con el trabajo, uso de correo electrónico y mensajería instantánea, para fines no relacionados con el trabajo y la responsabilidad de mantener los sistemas actualizados y

seguros. Para más información, revisar el documento: Manual de Lineamientos de Uso de Recursos informáticos.

5. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación abordarán el uso de redes sociales y otras formas de comunicación electrónica en el lugar de trabajo. Esto puede incluir crear conciencia sobre los riesgos asociados con la divulgación de información confidencial o delicada mediante estas plataformas, así como prohibir el acoso en línea, la difamación u otro comportamiento inapropiado.
6. Donde no esté restringido, las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación establecerán límites y requisitos para la descarga e instalación de software equipos de cómputo de la institución. Esto puede incluir abstenerse de descargar software no autorizado o ilegal, comprender los riesgos asociados con el malware y ser responsable de obtener y mantener las licencias adecuadas para el software utilizado.
7. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación, enfatizará la responsabilidad personal de cada funcionario o usuario por el cumplimiento de las normas de uso, seguridad de la información y uso de recursos informáticos. Esto puede incluir la necesidad de proteger el acceso a la información, informar eventos, correos u otra actividad sospechosa y participar en programas de capacitación y sensibilización sobre la seguridad de la información.
8. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación definirán, deberán especificar las consecuencias de no cumplir con las reglas de uso, esto según las disposiciones aplicables en materia de responsabilidad administrativa y disciplinaria.
9. La jefatura inmediata, es la responsable de informar de los movimientos de equipo informático y/o usuario que se trasladó con su equipo asignado a otra dependencia o ubicación.

Aspectos de seguridad de la información adicionales

1. Utilizar los bienes informáticos únicamente para el cumplimiento de las funciones asignadas según su clase de puesto y especialidad o uso académico en caso de estudiantes y docentes.
2. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben de considerar el uso de antivirus y o programas para combatir diferentes tipos de programa malicioso (malware), cualquier software de este tipo debe ser licenciado.
3. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben de velar porque el software de los equipos siempre esté actualizado a la última versión disponible y estable.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben de crear perfiles de usuarios y definir los privilegios y accesos de estos.
5. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben de realizar regularmente análisis de los riesgos que podrían atentar contra la seguridad de la información de la institución.
6. A los funcionarios del MEP, se les recomienda hacer uso de herramientas de almacenamiento en la nube proporcionadas por la institución con la finalidad de respaldar información importante de manera segura y procurar la continuidad de las operaciones, salvaguardando la información en caso de un incidente de seguridad informática.
7. Se recomienda el uso de carpetas compartidas en la red institucional (con uso de privilegios y control de acceso a las carpetas) para personal docente, miembros del personal para almacenar y compartir fácilmente la información.
8. Se recomienda a los centros educativos hacer copias de seguridad periódicas en dispositivos de almacenamientos externos y/o la nube de sus datos, para estar listos en caso de corrupción o destrucción deliberada de la información.

9. Las dependencias deben de asegurar la continuidad del servicio brindado por el recurso informático, por ejemplo: computadoras y/o impresoras, a los usuarios, con el fin de no entorpecer sus labores cotidianas.
10. Todo funcionario es responsable de velar por el uso seguro por los bienes informáticos asignados a él.
11. Todos los funcionarios deben tener conocimiento y estar conscientes de los compromisos, normas y reglamentos que han adquirido para el uso de los servicios o activos informáticos.
12. Todos los funcionarios deben acatar e implementar las medidas de seguridad establecidas que garanticen el resguardo necesario.
13. Todos los funcionarios deben de evitar realizar acciones que pongan en riesgo los equipos de cómputo institucional.
14. Todos los funcionarios deben verificar con el software antivirus, los medios de almacenamiento externo usados para el resguardo de información al momento de su conexión.
15. Todos los funcionarios deberán hacer respaldos de la información que se encuentra almacenada en unidades de almacenamiento y que considere crítica o de suma importancia. Esto de manera regular, como medida de contingencia ante un eventual daño en su computador. Utilizando para ello algún medio de almacenamiento masivo con que se cuente y sea utilizado únicamente para fines laborales, por ejemplo, dispositivos USB o almacenamiento en la nube.
16. Queda bajo la responsabilidad del usuario, el almacenamiento de la información institucional en la nube, las implicaciones en cuanto a confidencialidad de la información y responsabilidad de esta, así como su uso.
17. Los funcionarios no deben almacenar en las carpetas compartidas y/o unidades de almacenamiento de las computadoras del Ministerio de Educación Pública, archivos de música, archivos de video o archivos de imágenes que no sean propias de las labores

realizadas para la Institución. Los archivos no autorizados deben ser borrados por el personal técnico de forma inmediata.

18. Los funcionarios deben mantener el bien institucional informático en un entorno adecuado para este, asegurándose que el mismo no corra riesgos físicos, tales como: exposición a la humedad, polvo, altas temperaturas, agua, alimentos, bebidas y otros elementos que atenten contra el correcto funcionamiento del bien.

19. Los funcionarios deben conectar el bien informático únicamente en los sitios de alimentación eléctrica designados para este fin. Preferiblemente a un regulador de voltaje o unidad de energía ininterrumpida con regulador de voltaje (UPS).

20. Los funcionarios no deben conectar en tomacorrientes destinados para los bienes informáticos, artículos como fotocopiadoras, hornos de microondas, percoladores/coffemaker, abanicos, cargadores de teléfonos y otros artefactos electrónicos.

21. Los funcionarios deben cerrar sesión de los sistemas de información, software, bases de datos y/o servicio de red; cuando abandone el área de trabajo y/o no esté usando el equipo, para luego proceder a apagarlo.

22. Los funcionarios deben procurar el óptimo y adecuado uso de los bienes informáticos a su cargo.

23. Según lo establecido por la dependencia responsable, se debe mantener la configuración que permite que los equipos ingresen a la red.

24. Los funcionarios no deben utilizar el equipo de cómputo para actividades ajenas a sus funciones o labores.

25. Los funcionarios deben custodiar los medios de almacenamiento (CDs o memorias USB) que le fueron entregados con equipo de cómputo.

26. Los funcionarios deben reportar a la jefatura inmediata la movilización de los bienes informáticos (computadoras y/o

impresoras) que tiene bajo su responsabilidad, mediante el sistema creado para este fin.

27. Los funcionarios deben procurar el uso de regulador de voltaje o unidad de energía ininterrumpida con regulador de voltaje (UPS) cuando el recurso esté disponible para cuidar los equipos.

28. Los funcionarios deberán comunicar inmediatamente a su superior sobre cualquier inconveniente que se presente, en especial si algún bien ha sido sustraído o reporta fallas de funcionamiento.

29. Los funcionarios deben de velar que cuando realicen la devolución el equipo, este debe contar con el software preinstalado, así como todos los componentes que fueron entregados con el mismo, por ejemplo: teclado, mouse, expansor de puertos, maletín, entre otros. Cabe indicar que el equipo entregado, debe ser verificado por el funcionario que lo recibe.

30. El funcionario que requiera desinstalar software en su equipo deberá hacer solicitud a su jefatura inmediata.

31. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben revisar y actualizar estos lineamientos, así como los procedimientos de seguridad de manera regular, garantizando que reflejen las últimas prácticas recomendadas y estén alineados con las normas y regulaciones vigentes.

EJE GESTIÓN DE RIESGOS

Gestión de activos de información

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer un proceso para identificar y clasificar todos los activos de información de la institución. Esto puede incluir como mínimo sistemas, bases de datos, gestión documental, archivos electrónicos y cualquier otro tipo de información que sea de valor para la institución.

2. Debe indicarse claramente la propiedad de cada dato. Esto puede incluir la identificación del propietario, los responsables de su custodia, acceso y mantenimiento. También deben aclararse las responsabilidades de los usuarios y administradores de los recursos de información.
3. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer una guía de clasificación de la información utilizando etiquetas en el encabezado o pie de página, que muestren de manera sencilla y rápida la clasificación del documento según su nivel de confidencialidad, criticidad y sensibilidad. Esto ayudará a aplicar salvaguardas y controles apropiados para proteger la información de acuerdo con su categorización.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer lineamientos de autorización y control de acceso para garantizar que solo las personas autorizadas puedan acceder a los activos de información. Esto puede incluir la implementación de herramientas de autenticación, la concesión de privilegios basados en roles y la implementación de normativas de privilegios mínimos.
5. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben crear lineamientos detallados sobre el uso y la divulgación de los activos de información. Esto puede incluir como mínimo limitar el uso de la información solo para fines autorizados, prohibir la divulgación no autorizada de información confidencial y cumplir con las normativas y regulaciones aplicables.
6. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer una estrategia de respaldo y recuperación de la información para garantizar la disponibilidad de los activos de información en caso de un incidente o desastre. Esto puede incluir como mínimo copias de seguridad periódicas, pruebas de recuperación y almacenamiento seguro de copias de seguridad.

7. La información en función de los requisitos legales, reglamentarios y organizativos cuyos plazos de retención, deben ser definidos por la dirección de Archivo Central. También se deben establecer procedimientos claros para la eliminación segura de los activos de información cuando ya no se necesiten o se vuelvan obsoletos.
8. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer un proceso para la revisión y el control periódico de los activos de información para garantizar el cumplimiento de las políticas y los controles establecidos. Esto puede incluir revisar los registros de acceso, identificar actividades sospechosas y tomar medidas correctivas si es necesario.

Gestión de incidentes de seguridad de la información

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben definir claramente en qué constituye un incidente de seguridad de la información. Esto puede incluir como mínimo brechas de seguridad, acceso no autorizado, pérdida o robo de datos, malware, afectaciones en la integridad de la información, ataques de denegación de servicio y otros eventos que amenazan la seguridad de la información.
2. Si un funcionario se abordado por personal de la oficina de ciberseguridad o encargados de seguridad informática de la DRTE debido a que existe una situación que pueda convertirse potencialmente en un incidente de seguridad de la información, debe dar atención prioritaria.
3. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer un procedimiento claro para reportar incidentes de seguridad de la información. Esto puede incluir quién y cómo informar el incidente, así como los canales de comunicación que se utilizarán. Fomentar una cultura de denuncia temprana sin temor a represalias es esencial para una respuesta rápida.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer un sistema para clasificar y

priorizar los incidentes en función de la gravedad del incidente y su impacto potencial en la institución. Esto ayudará a asignar los recursos apropiados y tomar medidas contra cada incidente.

5. Las dependencias del Ministerio de Educación deben realizar periódicamente análisis preventivo de vulnerabilidades y riesgos que, puedan materializarse como un incidente que atente contra la seguridad de la información.
6. Cada dependencia debe de definir a un funcionario o grupo de funcionarios que funjan como un punto de contacto. Para las dependencias de oficinas centrales, Oficinas regionales y circuitos el contacto debe ser remitido a la DIG utilizando el correo: seguridadinformaticadig@mep.go.cr. En caso de instituciones educativas el contacto debe ser remitido a soportetecnicopnft@mep.go.cr. El contacto debe incluir: nombre, correo y teléfono de este funcionario. Esta o estas personas están encargadas de informar sobre los incidentes de seguridad, clasificarlos, asignarles prioridad y remitirlos a la dirección competente, o bien, atender al personal encargado de seguridad de la información que le contacte para darle seguimiento al incidente.
7. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben describir un proceso de gestión de incidentes paso a paso, desde la detección y notificación inicial hasta la resolución y el seguimiento. Esto puede incluir como mínimo la recopilación de pruebas, el análisis de la causa raíz, la mitigación de daños, la recuperación del servicio y la documentación detallada de cada paso del proceso.
8. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben comunicar la importancia de la mejora continua en el manejo de incidentes de seguridad de la información. Esto incluye analizar las lecciones aprendidas, actualizar marcos normativos y procedimientos, implementar medidas preventivas, realizar capacitaciones y pruebas periódicas para responder a incidentes.

Relación con terceros a nivel de seguridad de la información

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben definir un proceso de evaluación de seguridad con terceros basado en criterios de seguridad de la información. Esto puede incluir la revisión de las políticas y prácticas de seguridad, la evaluación de los controles de seguridad existentes y la revisión de la reputación y el desempeño de la seguridad de los proveedores o socios comerciales.
2. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben realizar convenios con terceros que fortalezcan la seguridad de la información entre ambas partes. Estos acuerdos deben definir claramente las responsabilidades y obligaciones de cada parte con respecto a la protección de la información, el alcance y los activos confidenciales de la institución.
3. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben establecer los requisitos mínimos de seguridad de la información que deben cumplir los terceros. Esto puede incluir como mínimo la implementación de controles de seguridad apropiados, encriptación de datos si está disponible, administración de acceso, derechos y notificación oportuna de incidentes de seguridad.
4. Cuando se realicen convenios con terceros, la Dirección de Asuntos Jurídicos MEP colaborará verificando que los convenios incorporen las cláusulas o disposiciones mínimas de seguridad que elaboren las instancias técnicas expertas en la materia, no así la ejecución y cumplimiento de dichas cláusulas.
5. Cuando se realicen convenios con terceros en materia relacionada con la información, ciberseguridad, software y hardware, se debe definir el Departamento/ Persona/Unidad/Dependencia o cualquier otro, que serán los responsables de realizar el seguimiento de cumplimiento de dicho convenio.
6. Si se comparten datos personales con terceros, se debe asegurar el cumplimiento de las disposiciones desarrolladas en la Ley N°

8968 y el apartado 10.1" Sobre la protección de datos" de esta política.

7. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación en coordinación con la Dirección de Asuntos Jurídicos y la Proveeduría Institucional deben describir cómo se gestionarán los cambios a terceros, incluida la actualización de convenios cuando ocurran cambios significativos. Además, se debe contemplar un plan remedial para asegurar la continuidad del negocio en caso de que la relación con el tercero sea terminada.
8. Los funcionarios deben estar capacitados y ser conscientes de los requisitos de seguridad asociados con las relaciones con terceros. Deben comprender los riesgos involucrados y cómo proteger la información confidencial al interactuar con alguna otra parte interesada.
9. Las pautas mencionadas en este apartado deben revisarse y actualizarse regularmente para garantizar que siga siendo relevante y eficaz en un entorno cambiante. Esto puede incluir la revisión de contratos existentes, la evaluación de nuevos proveedores y la incorporación de las mejores prácticas de seguridad de la información.

Mejora continua de la seguridad de la información

1. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben analizar y revisar minuciosamente cualquier incidente de seguridad de la información o ciberseguridad que ocurra en el Ministerio, así como solicitar a otras instituciones del Estado que tengan conexiones con nuestros sistemas un informe en caso de que estas hayan recibido un ciberataque o comunicar en caso de que el Ministerio de Educación haya sido el receptor de un ataque de seguridad de la información. El ministerio debe retroalimentarse de las lecciones aprendidas y utilizarlas como oportunidades para fortalecer nuestras defensas y mejorar nuestra capacidad de respuesta.

2. El MEP debe velar por la capacitación continua de los funcionarios sobre las últimas amenazas de Ciberseguridad y las mejores prácticas de seguridad de la información. Esta formación es fundamental para asegurar que todos los miembros del Ministerio estén bien informados y preparados para enfrentar los desafíos actuales y futuros.
3. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben llevar a cabo análisis periódicos de vulnerabilidades en nuestra infraestructura y sistemas para identificar posibles debilidades. Con la finalidad de aplicar las correcciones necesarias de manera oportuna.
4. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben evaluar continuamente las tecnologías emergentes en el campo de la Ciberseguridad para mejorar nuestra capacidad de detección, prevención y respuesta ante amenazas.
5. Los funcionarios encargados de velar por la Ciberseguridad del Ministerio deben mantener una relación activa con expertos en seguridad cibernética y participar en comunidades y foros relevantes para estar al tanto de las últimas tendencias y estrategias.
6. Las direcciones de Informática en Gestión y Recursos Tecnológicos en Educación deben revisar y actualizar estas pautas, así como los procedimientos de seguridad de manera regular, garantizando que reflejen las últimas prácticas recomendadas y estén alineados con las normas y regulaciones vigentes.

Tabla 2. Eje información y datos

EJE	OBJETIVOS	ACCIONES ESTRATEGICAS	METAS	INDICADORES	RESPONSABLES
Información y datos	Promover una cultura de seguridad de la información en el MEP en que la información y datos recopilados, así como la información y datos almacenados, sean correctamente categorizados y protegidos ante cualquier amenaza que ponga en riesgo su privacidad, integridad y disponibilidad.	– Crear un protocolo de manejo adecuado de los datos que contemple la recopilación de información, la modificación, adición o eliminación, almacenamiento, retención y transferencia de datos.	1 protocolo de manejo adecuado de los datos antes del año 2028.	1 protocolo de manejo adecuado de los datos elaborado y aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		–Crear un protocolo que proporcione las mejores prácticas para la categorización de la información que contemple: categorización establecida por ley, responsables de categorizar, etiquetas, acceso e intercambio de información de acuerdo con su categorización antes del año 2028	1 protocolo de mejores prácticas para la categorización de la información antes del año 2028.	1 protocolo de mejores prácticas para la categorización de la información y aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		– Crear un protocolo que estipule como se deben de almacenar, definir, ubicar, respaldar de forma segura, eliminar la información y los datos, así como periodicidad en la que se deben de respaldar.	1 protocolo de gestión de información y datos antes del año 2028.	1 protocolo de gestión de información y datos aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE

Tabla 3. Eje gestión de usuario.

EJE	OBJETIVOS	ACCIONES ESTRATEGICAS	METAS	INDICADORES	RESPONSABLES
Gestión de usuario	Promover una cultura de seguridad de la información en el MEP en que los usuarios utilicen accesos robustos, autenticación múltiple y las buenas prácticas en la seguridad de sus cuentas asignadas. Así como deben de llevar un control de acceso para funcionarios y personas ajenas a las instalaciones.	Crear un protocolo que indique los requisitos mínimos relacionados a las credenciales incluyendo: Complejidad, renovación y seguridad.	1 protocolo que indique los requisitos mínimos relacionados a las credenciales antes del año 2028.	1 protocolo que indique los requisitos mínimos relacionados a las credenciales aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear un protocolo que establezca los mecanismos que deben ser utilizados para el acceso de cuentas y a las instalaciones del MEP	1 protocolo que establezca los mecanismos que deben ser utilizados para el acceso de cuentas y a las instalaciones del MEP antes del año 2028.	1 protocolo que establezca los mecanismos que deben ser utilizados para el acceso de cuentas y a las instalaciones del aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	
		Crear un protocolo que contemple las buenas prácticas sobre la gestión, de usuarios incluyendo: credenciales, privilegios basados en roles, movimientos de personal MEP y estudiantes de los centros educativos.	1 protocolo que contemple las buenas prácticas sobre la gestión, de usuarios antes del año 2028.	1 protocolo que contemple las buenas prácticas sobre la gestión, de usuarios aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE

Tabla 4. Eje protección de recursos tecnológicos.

EJE	OBJETIVOS	ACCIONES ESTRATEGICAS	METAS	INDICADORES	RESPONSABLES
Protección de recursos tecnológicos.	Implementar procesos de evaluación y actualización de software y las pautas que establezcan el uso adecuado de acceder a las redes y las medidas de protección a las mismas.	Crear un manual para la evaluación y actualización de los softwares disponibles, incluyendo: priorización, planificación, compatibilidad, puntos de restauración. Y obsolescencia del software.	1 manual para la evaluación y actualización de los softwares disponibles antes del año 2028.	1 manual para la evaluación y actualización de los softwares disponibles aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear lineamientos en los cuales se den las pautas para la conectividad segura a las redes incluyendo: uso aceptable de la red, filtrado de tráfico, herramientas de protección de tráfico, acceso y autorización a la red.	1 manual de lineamientos en los cuales se den las pautas para la conectividad segura a las redes antes del año 2028.	1 manual de lineamientos en los cuales se den las pautas para la conectividad segura a las redes aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear directrices para implementar las medidas de protección de navegación en las redes que incluya: inventarios de dispositivos de red, gestión de registros digitales, gestión de dispositivos externos, mapa de red,	1 manual de directrices para implementar las medidas de protección de navegación en las redes antes del año 2028.	1 manual de directrices para implementar las medidas de protección de navegación en las redes aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE

Tabla 5. Eje uso de activos tecnológicos

EJE	OBJETIVOS	ACCIONES ESTRATEGICAS	METAS	INDICADORES	RESPONSABLES
Uso de Activos tecnológicos	Documentar e intercambiar buenas prácticas sobre el manejo de la seguridad de la información con el fin de que estas sean adaptadas y adoptadas por el MEP.	Crear manual sobre las buenas prácticas en el uso seguro de los activos de la información	1 manual sobre las buenas prácticas en el uso seguro de los activos de la información antes del año 2028.	1 manual sobre las buenas prácticas en el uso seguro de los activos de la información aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear manual donde se indica las pautas a seguir para el uso seguro del correo electrónico.	1 manual donde se indica las pautas a seguir para el uso seguro del correo electrónico antes del año 2028.	1 manual donde se indica las pautas a seguir para el uso seguro del correo electrónico aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear manual incluyendo: prohibición de actividades ilegales o no autorizadas, resguardo del equipo informático institucional.	1 manual incluyendo: prohibición de actividades ilegales o no autorizadas, resguardo del equipo informático institucional antes del año 2028.	1 manual incluyendo: prohibición de actividades ilegales o no autorizadas, resguardo del equipo informático institucional aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear manual que incluya las medidas de protección cotidianas a nivel de software y Hardware que se le pueden brindar a los dispositivos.	1 manual que incluya las medidas de protección cotidianas a nivel de software y Hardware que se le pueden brindar a los dispositivos antes del año 2028.	1 manual que incluya las medidas de protección cotidianas a nivel de software y Hardware que se le pueden brindar a los dispositivos aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028	DIG y DRTE

Tabla 6. Eje gestión de riesgos.

EJE	OBJETIVOS	ACCIONES ESTRATEGICAS	METAS	INDICADORES	RESPONSABLES
Gestión de riesgos	Gestionar correctamente los activos de la información, la atención de incidentes de seguridad de la información, la seguridad con los terceros y buscar la mejora continua se los procesos de la información del MEP	Crear procesos que permitan Identificar, clasificar, recuperar y respaldar los activos de la información, así como determinar responsable de los recursos de la información	1 manual de procesos que permitan Identificar, clasificar, recuperar y respaldar los activos de la información antes del año 2028.	1 manual de procesos que permitan Identificar, clasificar, recuperar y respaldar los activos de la información aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear procedimientos que permitan dar seguimiento a los incidentes relacionados con la seguridad de la información.	1 manual de procedimientos que permitan dar seguimiento a los incidentes relacionados con la seguridad de la información.	1 manual de procedimientos que permitan dar seguimiento a los incidentes relacionados con la seguridad de la información aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Crear un proceso que determine la manera en la que se debe de manejar la información con terceros	1 manual de procesos que determine la manera en la que se debe de manejar la información con terceros antes del año 2028.	1 manual de procesos que determine la manera en la que se debe de manejar la información con terceros aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE
		Brindar capacitaciones de mejora, en el área de la seguridad de la información que sean proporcionadas al MEP. Realizar análisis de vulnerabilidades.	5 capacitaciones de mejora, en el área de la seguridad de la información que sean proporcionadas al MEP. antes del año 2028.	5 capacitaciones de mejora, en el área de la seguridad de la información que sean proporcionadas al MEP. aprobado por ambas direcciones, el Despacho del Viceministerio Administrativo y el despacho ministerial antes del año 2028.	DIG y DRTE

HOJA DE REVISIÓN Y ACEPTACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – MINISTERIO DE EDUCACIÓN PÚBLICA

ELABORADO POR:

NOMBRE	CARGO	DEPENDENCIA	FIRMA
Daniel Josué Delgado Leandro	Profesional	DIG	DANIEL JOSUE DELGADO LEANDRO (FIRMA) Firmado digitalmente por DANIEL JOSUE DELGADO LEANDRO (FIRMA) Fecha: 2024.01.17 09:38:46 -06'00'

COLABORADORES:

NOMBRE	CARGO	DEPENDENCIA	FIRMA
Juan Carlos Rodríguez Valerio	Profesional	DIG	JUAN CARLOS RODRIGUEZ VALERIO (FIRMA) Firmado digitalmente por JUAN CARLOS RODRIGUEZ VALERIO (FIRMA) Fecha: 2024.01.17 09:49:03 -06'00'
Randall Alcázar Miranda	Técnico Informática	DRTE	RANDALL MAURICIO ALCAZAR MIRANDA (FIRMA) Firmado digitalmente por RANDALL MAURICIO ALCAZAR MIRANDA (FIRMA) Fecha: 2024.01.17 11:16:36 -06'00'

REVISADO POR:

NOMBRE	CARGO	DEPENDENCIA	FIRMA
Gabriel Denis Denis	Subdirector	DIG	GABRIEL ANTONIO DENIS DENIS (FIRMA) Firmado digitalmente por GABRIEL ANTONIO DENIS DENIS (FIRMA) Fecha: 2024.01.17 11:24:27 -06'00'

APROBADO POR:

NOMBRE	CARGO	DEPENDENCIA	FIRMA
Fressy Aguilar Chinchilla	Directora	DRTE	FRESSY MARIA DE JESUS AGUILAR CHINCHILLA (FIRMA) Firmado digitalmente por FRESSY MARIA DE JESUS AGUILAR CHINCHILLA (FIRMA) Fecha: 2024.01.18 10:38:49 -06'00'
Esteban Arroyo Pacheco	Director	DIG	ESTEBAN ARROYO PACHECO (FIRMA) Firmado digitalmente por ESTEBAN ARROYO PACHECO (FIRMA) Ubicación: Lic. Esteban Arroyo Pacheco , céd 109080209 Fecha: 2024.01.18 19:23:49 -06'00'

FECHA: NOVIEMBRE, 2023