UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Tema: MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR.

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor: Ing. Patricio Neptali Vaca Escobar.

Director: Ing. David Omar Guevara Aulestia, Mg.

Ambato – Ecuador

2019

A la Unidad Académica de Titulación de la Facultad en Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia Magister, e integrado por Ingeniero Franklin Oswaldo Mayorga Mayorga Magister, Ingeniero Jaime Bolívar Ruiz Banda Magister, designados por la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas Electrónica e Industrial la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "**MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR**", elaborado y presentado por el Ingeniero Patricio Neptali Vaca Escobar, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia Mg.
Presidente del Tribunal

Ing. Franklin Oswaldo Mayorga Mayorga Mg.
Miembro del Tribunal

Ing. Jaime Bolívar Ruiz Banda Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: Modelo de gestión de Seguridad lógica de la información en la protección de los datos sensibles de los Distritos de Educación del Ecuador, le corresponde exclusivamente a: Ingeniero Patricio Neptali Vaca Escobar, Autor bajo la Dirección del Ingeniero David Omar Guevara Aulestia Mg., Director del trabajo de titulación.

Ing. Patricio Neptali Vaca Escobar

C.C. 1718102815

AUTOR

Ing. David Omar Guevara Aulestia, Mg.

C.C. 1802605749

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. Patricio Neptali Vaca Escobar

C.C. 1718102815

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

AGRADECIMIENTO

A Dios por guiar mis pasos y protegerme en cada instante y cada fase de mi vida.

A mi esposa, mi hija, mi madre y mis hermanos por ser un apoyo y motivadores fundamentales para que este sueño sea cumplido.

A mi director de trabajo de investigación Ing. David Omar Guevara Aulestia, Mg, debido a que con sus conocimientos ha dedicado su valioso tiempo para que el presente trabajo de investigación pueda ser culminado.

Patricio.

DEDICATORIA

A Dios, debido a que he visto y sentido todas las bendiciones derramadas hacia mi persona.

A mi madre Marcia Marlene, que ha inculcado en mí el deseo de superación constante y ha sido siempre mi motivación por su infinito amor que me tiene.

A mi padre Tulio Patricio, que pese a todo siempre ha estado para darme consejos y formarme como un hombre de bien y con buenos valores.

A mi esposa Magaly Patricia, que por medio de su amor demostrado es fuente de mi inspiración para conseguir mis objetivos de vida.

A mi hija Sofia Valentina, que con su corta edad se ha ganado mi amor y es por la que voy a seguir preparándome para ser convertirme en ejemplo para ella.

A mis hermanos, para que vean que en la vida mediante la dedicación, esfuerzo y fe todo se puede conseguir.

A mis abuelitos Fanny y Neptali, que me apoyaron cuando más los necesite y siempre viendo por mi bienestar en todos los sentidos.

Con mucho cariño para ustedes va este trabajo, son y serán la razón por la cual seguir preparándome como persona y como profesional.

Patricio.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

"MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR".

Autor : Ing. Patricio Neptalí Vaca Escobar.

Tutor : Ing. David Omar Guevara Aulestia, Mg.

Fecha : 17-09-2019

RESUMEN EJECUTIVO

La evolución de las tecnologías ha apalancado el desarrollo de las organizaciones en todos los aspectos. Esta mejora se ha visto directamente relacionada con el uso del activo más preciado en la actualidad y también llamado como el petróleo del siglo XXI como son los datos. Dentro de las categorías de los datos que se capturan procesan y almacenan en las organizaciones se encuentran los datos personales y entre ellos datos de carácter sensible, es importante mencionar que así como los datos llevan al crecimiento de las organizaciones, estos pueden generar pérdidas devastadoras que van desde la perdida de la reputación, consecuencias legales que van desde sanciones administrativas, civiles y hasta penales, desencadenado en secuelas económicas, si es que no se los trata de una manera correcta y eficiente.

En el presente documento se lo desarrolló con el objetivo de brindar lineamientos para el correcto manejo de los datos de carácter altamente confidencial, por medio de un modelo de gestión de seguridad en el tratamiento de la información sensible que se capturan, almacenan y procesan en los Distritos de Educación del Ecuador, y en este caso en la Dirección Distrital Educación 23D01.

El modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles cuenta con lineamientos necesarios para salvaguardar los datos en los aspectos de confidencialidad, integridad y disponibilidad de la información sensible, alineados al marco de referencia Planear, Hacer, Verificar y Actuar que persigue la mejora continua establecida por la normativa ISO 9001:2015. Además, se hace constar una serie de documentos anexos al presente trabajo de investigación entre ellos: políticas de seguridad de la información, mecanismos de control, acuerdos de confidencialidad, entre otros. Por otra parte, se detallan mecanismos de control definidos en la ISO 27001:2013 que detallan buenas prácticas en la preservación de la información.

El diseño del modelo se fundamentó principalmente en normas y estándares internacionales, así como del estudio de modelos de protección de datos ya puestos en marcha en países como México que cuenta con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) publicada el 5 de julio de julio del 2010 y entro en vigor el 6 de julio del mismo año, el Régimen General de Protección de Datos Personales ley 1581 del 2012 de Colombia, y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales de España que entró en vigor el 25 de mayo del 2018. Todas estas leyes existentes fueron la base para la construcción del modelo propuesto, además del anteproyecto de la Ley Orgánica de Protección de Datos personales (LOPDP) presentado por la Dirección Nacional de Registro de Datos Públicos (DINARDAP) del Ecuador.

Descriptores: Modelo de gestión de datos, seguridad de la información, datos sensibles, seguridad informática, protección de datos, políticas de seguridad de la información, mecanismos de seguridad de la información, vulnerabilidades, controles de seguridad, seguridad informática en distritos de educación, tratamiento de datos personales.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

"MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR".

Author : Ing. Patricio Neptali Vaca Escobar.

Directed By : Ing. David Omar Guevara Aulestia, Mg.

Date : 17-09-2019

EXECUTIVE SUMMARY

The evolution of technologies has leveraged the development of organizations in all aspects. This improvement has been directly related to the use of the most precious asset today and also called as the oil of the 21st century as are the data. Within the categories of the data that are captured process and store in the organizations are the personal data and among them sensitive data, it is important that they are found as well as the data that lead the growth of the organizations, these can generate losses devastating losses ranging from loss of reputation, legal consequences ranging from administrative, civil and even criminal penalties, triggered in economic aftermath, if it is not treated in a correct and efficient manner. In this document, verify with the objective of providing guidelines for the correct handling of highly confidential data, through a security management model in the treatment of sensitive information that is captured, stored and processed in the Districts of Education of Ecuador, and in this case in the District Education Directorate 23D01.

The logical information security management model in the protection of sensitive data has the necessary guidelines to safeguard data in the aspects of confidentiality,

integrity and availability of sensitive information, aligned with the Plan, Do, Verify and reference framework. Act that pursues the continuous improvement established by ISO 9001: 2015. In addition, a series of documents attached to this research work are included, among them: information security policies, control mechanisms, confidentiality agreements, among others. On the other hand, modified control mechanisms are detailed in ISO 27001: 2013 that detail good practices in the preservation of information.

The design of the model is mainly based on international norms and standards, as well as the study of data protection models and implementation in countries such as Mexico that has the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) published on July 5, 2010 and effective on July 6 of the same year, the General Regime for the Protection of Personal Data law 1581 of the 2012 of Colombia, and the Organic Law of Data Protection and Guarantee of Digital Rights of Spain that entered into force on May 25, 2018. All of these affected laws were the basis for the construction of the proposed model, in addition to the draft of the Organic Law on Protection of Personal Data (LOPDP) presented by the National Directorate of Data Registry Public (DINARDAP) of Ecuador.

Keywords: Data management model, information security, sensitive data, computer security, data protection, information security policies, information security mechanisms, vulnerabilities, security controls, computer security in education districts, treatment of personal information

INTRODUCCIÓN

En la actualidad la información se ha constituido como un bien preciado para las organizaciones que dentro de sus objetivos estratégicos buscan el cambio constante mediante las acertadas decisiones tomadas. Las decisiones se constituyen como el entregable fundamental de los gerentes y a su vez se consideran como el mecanismo mediante el cual afectan la realidad operativa de las organizaciones.

Aunque suene contraproducente todos los logros y objetivos conseguidos por cualquier organización, pueden ser afectados por la deficiente gestión de la Seguridad Informática (SI), es así que: Neira y Spohr señalan que la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización para la preservación de su confidencialidad, integridad y disponibilidad (Neira & Spohr, 2010).

La evolución de la tecnología constituye un medio para que los ciberdelincuentes se especialicen en el uso y aplicación de materiales y métodos para encontrar vulnerabilidades en los sistemas de información, desde la utilización de keyloggers (software que captura todo lo que se digita en el teclado), hasta ataques de fuerza bruta, que (prueba todas las combinaciones posibles para obtener credenciales de acceso). Domínguez et al, en su publicación mencionan datos de ataques suscitados desde el 2009 al 2015, años en los cuales se observa un crecimiento del 66% con un total de 42,8 millones de incidentes, equivalentes a 117,339 ataques por día (Domínguez L., Maya O., Peluffo O., & Crisanto Ñ., 2016).

Eset, en su reporte estadístico publicado en el 2016 ubica al Ecuador como el tercer país de Latinoamérica al contar con el 51,9% de empresas que se vieron afectadas por algún tipo de malware. Por otra parte, en este mismo reporte Eset menciona que Ecuador se ubica en el primer lugar con el 24% de las empresas que se vieron afectadas por ataques de Phishing seguido por Perú y Guatemala con el 22% y 20% respectivamente (ESET, 2017).

El gobierno del Ecuador consciente de los ataques ha planteado un anteproyecto de Ley Orgánica de Protección de Datos Personales (LOPDP), que en el artículo 6 sobre los términos y definiciones de este anteproyecto acerca de los datos sensibles se detalla: “Se consideran datos sensibles a aquellos datos personales que

gozan de protección reforzada, tales como los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, estado de salud, datos biométricos, datos de geolocalización y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas" (DINARDAP, 2019).

En la ciudad de Santo Domingo y específicamente en el Distrito de Educación (23D01) al manejar y administrar sistemas de información con datos sensibles, estos pueden ser susceptibles a actos de vulnerabilidad y llegar a la mano de personas con malas intenciones.

Cumpliendo con los requerimientos y todo tipo de viabilidad existente y por dar solución a lo explicado en el capítulo I del contexto del problema, surge la necesidad de proponer un Modelo de gestión de Seguridad lógica de la información en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

Debido a los antecedentes ya mencionados, el presente documento de investigación se lo estructuró de la siguiente manera:

El CAPÍTULO I, EL PROBLEMA contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

El CAPÍTULO II MARCO TEÓRICO contiene: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

El CAPÍTULO III METODOLOGÍA contiene: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

EL CAPITUO IV ANÁLISIS E INTERPRETEACIÓN DE RESULTADOS contiene: análisis de resultados, formulario de evaluación y medición, validación

de las respuestas obtenidas, interpretación del resultado del formulario de evaluación y medición.

EL CAPITULO V CONCLUSIONES Y RECOMENDACIONES contiene: las conclusiones y recomendaciones que se obtienen a partir de la investigación del marco teórico y el resultado de las respuestas que dan paso al desarrollo de la propuesta investigativa.

El CAPITULO VI PROPUESTA contiene: datos informativos, antecedentes de la propuesta, justificación, objetivos, análisis de factibilidad, elaboración de la propuesta, y el modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

CAPÍTULO I

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 TEMA DE INVESTIGACIÓN

Modelo de Gestión de Seguridad Lógica de la Información en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

1.2 Planteamiento del Problema

1.2.1 Contextualización

La evolución de las tecnologías nacientes ha apalancado el desarrollo de las organizaciones mismas que hacen uso de los datos, procesándolos y convirtiéndoles en información, lo cual es un factor clave para la toma de decisiones. La información se ha convertido en el activo más valioso de toda institución por tal razón es importante que se garantice tres principios de la SI tales como: la confidencialidad el cual tiene como propósito el asegurar que solo la persona correcta acceda a la información que se pretende distribuir, la integridad hace referencia a que la información no haya sido alterada en su contenido y por último la disponibilidad permitiendo que la información llegue en el momento oportuno y cuando se la requiera (Dussan Clavijo, 2006).

En Latinoamérica países como Argentina, Chile, Colombia, Perú, por citar a países cercanos a la región del Ecuador se han interesado en el Hardening de sus sistemas de información mediante el uso de marcos de referencia, modelos, normas, políticas, mecanismos y estándares tales como COBIT, ISO 27001, ITIL, ICREA adaptándolos en sus sistemas que se encuentran expuestos hacia los ataques cibernéticos que se conocen en la actualidad.

En el Ecuador a pesar de que se conoce que la información se relaciona directamente con el desarrollo de las instituciones, dichas entidades no apuestan por la implementación de un modelo de gestión de seguridad lógica de la información para proteger su información y datos sensibles.

En su estudio Veloz et al, indican que Ecuador se encuentra en el quinto lugar de países de América del Sur con mayor amenazas web con un promedio de ataques de 9.425, en el mes de septiembre del 2015 (Veloz, Alcivar, Salvatierra, & Silva,

2017). Por otra parte Kapersky Labs empresa dedicada a la seguridad informática y con presencia en más de 200 países del mundo, mediante su boletín de seguridad estadísticas generales de 2017, menciona ver Figura 1 sobre la neutralización de los exploits más utilizados por los atacantes siendo los navegadores de internet (Browser) el mayor usado por el 42,56% de los ciberdelincuentes, por otra parte las aplicaciones Android ocupan un 27,13% esto se debe a la facilidad de crear un apk con fines maliciosos y en tercer lugar los exploits se los ocultan en archivos de office representado el 17,63% (Kapersky, 2017).

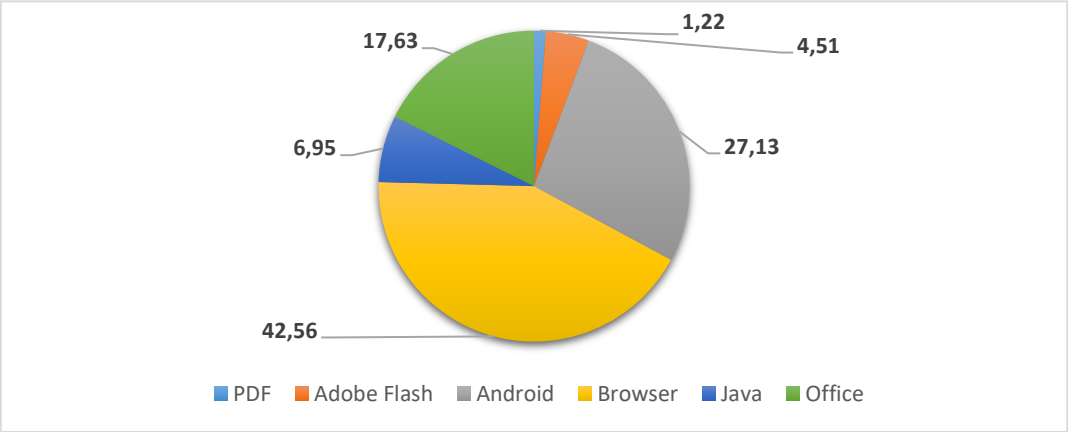


Figura 1 Estadísticas de aplicaciones vulnerables

Fuente: Kaspersky labs boletín de seguridad de estadísticas generales (2017)

En la ciudad de Santo Domingo y específicamente en el Distrito de Educación 23D01 carece de un modelo de gestión de seguridad lógica de la información lo cual como lo mencionan Gaona, Montenegro & Barón una entidad se puede ver vulnerada desde distintos tipos de ataques tales como: SQL injection, Session management and broken authentication, Cross-site scritpting (XSS) por mencionar algunos (Gaona-garcía, Montenegro-marín, & Barón Velandia, 2016).

El objeto de investigación del presente trabajo se basará principalmente en un modelo de gestión de seguridad lógica de la información de los Distritos de Educación del Ecuador. La razón del presente estudio en este tipo de instituciones se debe a que el Ministerio de Educación del Ecuador realizó una fuerte inversión tecnológica dotándolas de infraestructura, equipos informáticos y demás hardware

y software que se adaptan a los requerimientos del trabajo de investigación, además de que todos los procesos utilizan sistemas de gestión tales como Mogac, Spryn, eSbye, eSigef, Cas, Quipux, entre otros, en los cuales los funcionarios a diario exponen esta información sensible mediante el uso de la red y del internet.

Por otra parte, en el Acuerdo Ministerial No. 020-12 publicado el 07 de marzo del 2012 y actualizado por la Dirección Nacional de la Normativa Jurídico Educativa del Ministerio de Educación (MINEDUC) a 10 de marzo del 2016, específicamente en el Artículo 38 de la Gestión Estratégica de la Unidad Distrital de Tecnologías de la Información y Comunicaciones (UDTICs), se da a conocer la misión de este departamento: "Aplicar e implementar las políticas, normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información orientados a la optimización de recursos, sistematización y automatización de los procesos en el ámbito de su gestión". Misión que claramente representa la gestión genérica de las UDTICs de los distritos del MINEDUC. Además, en este acuerdo se dan a conocer las atribuciones, responsabilidades y productos que la UDTICs deben cumplir:

Tabla 1 Atribuciones, Responsabilidades y Productos de la Unidad de Distrital de Tecnologías de Información y Comunicaciones.

Atribuciones y Responsabilidades	Productos
a) Aplicar políticas y normativas alineadas a los estándares para la ejecución de proyectos de sistematización, automatización, adquisición y/o contratación de bienes y/o servicios tecnológicos informáticos del distrito. **b) Proporcionar soporte en los procesos tecnológicos del distrito.** **c) Monitorear de forma permanente los servicios tecnológicos del distrito.** **d) Administrar la infraestructura tecnológica en el nivel distrital.** **e) Supervisar el buen uso de las herramientas e infraestructura tecnológica del distrito.** **f) Apoyar en la coordinación de los proyectos realizados por la Dirección Nacional de Tecnologías Educativas y el SITEC.**	a) Plan Anual de Inversiones (PAI) de la Unidad Distrital de Tecnologías Educativas de la Información y Comunicaciones. b) Plan Operativo Anual (POA) de la Unidad Distrital de Tecnologías Educativas de la Información y Comunicaciones. c) Informes de ejecución de políticas y normativas. d) Informes de equipo informático en buen funcionamiento. e) Informes mensuales de soporte técnico efectuado. f) Reportes de disponibilidad de servicios tecnológicos. g) Informes de disponibilidad de la infraestructura tecnológica. h) Solicitudes de requerimiento de infraestructura tecnológica.

Fuente: Acuerdo Ministerial 020-12.
Elaborado por: Vaca Patricio, (2019).

Aunque es de vital importancia para una organización cuente con un monitoreo de los servicios tecnológicos y que se emitan entregables como informes de disponibilidad de servicios por mencionar algunos, se está dejando a un lado la seguridad de la información y la protección de los datos sensibles que se almacenan en los distritos de educación.

1.2.2 Análisis Crítico

Actualmente el resguardo de la información juega un papel fundamental en el desarrollo socioeconómico y bienestar de las instituciones y que esta no se vea vulnerada por el personal interno o externo, y ciberdelincuentes informáticos, se hace indispensable contar con modelos de seguridad de la información, con políticas internas y mecanismos que permitan mitigar estos ataques y a su vez medir su impacto, crecimiento y uso. Como lo menciona Solórzano & Rezabala & Aranda (2013), la información al ser considerada como el activo más importante de las empresas puede verse afectada por muchos factores como robos, incendios, fallas de disco, virus, además del desconocimiento o falta de cultura, quien en su publicación da a conocer las técnicas que la gente conoce para protegerse de una amenaza, siendo tendencia "uso de antivirus o programas" con un 44%, seguido de "No abro cualquier página o no descargo casi nada" con 22% y "No dejo que nadie use la pc más que yo" con 18%, lo cual refleja el poco conocimiento de las personas en cuanto a seguridad informática se refiere. Por esta razón es pertinente que en los Distritos de Educación se implemente un modelo de gestión de seguridad lógica de la información con la integración de políticas y la tendencia hacia un cambio de cultura.

Referente a lo mencionado anteriormente en este epígrafe y teniendo en cuenta la deficiente atención que se le presta a la seguridad de la información se presentan los siguientes riesgos:

- El departamento de Tecnologías de la información TI no cuenta con un modelo de gestión de seguridad lógica de la información que contribuya de manera eficiente a la reposición ante un ataque informático.
- La seguridad informática se enfoca en entender el riesgo y las consecuencias que una vulnerabilidad lleva consigo, que además puede terminar como causante de grandes pérdidas en la organización, nace con esto la necesidad

de proveer políticas internas y mecanismos de seguridad que contribuyan en la mitigación de los mismos basándose principalmente en la protección de la confidencialidad, integridad y disponibilidad.

- La organización no dispone de una cultura o conocimiento de políticas y mecanismos de prevención de la seguridad informática por parte de los funcionarios tiende a que sean causantes directos en la apertura de puertos para que un atacante vulnere cualquier sistema de información de la entidad.
- Falta de alineación de la seguridad informática con los objetivos estratégicos de los Distritos de Educación debido que se toma más importancia a los procesos de negocio que a la protección de los datos e información.
- Se cuenta con pocos o ningún estándar en la gestión, control y seguridad de la información lo que impide el desarrollo de la organización.
- Creencias o suposiciones de que la responsabilidad de la seguridad de la información solo recae sobre el departamento de TI lo que genera que los demás departamentos no le tomen la debida importancia.
- Deficiente control en los sistemas de gestión, lo que conlleva a que exista perdida de la integridad, confiabilidad y disponibilidad de los datos.

1.2.3 Prognosis

Si no se implementa un modelo de gestión de seguridad lógica de la información mediante el uso de políticas aumentará el riesgo de que ocurran pérdidas de información, fallos en la integridad de los datos, así como la denegación de servicios o suspensiones al momento de realizar la recuperación de datos.

Se tiene una primera alerta sabiendo que no se cuenta con un modelo de gestión de seguridad lógica de la información en el que se incluya las normas y procedimientos para actuar o reponerse ante un ataque informático o los datos de carácter sensible se vean comprometidos.

1.2.4 Formulación del Problema

¿Incide un modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los Distritos de Educación del Ecuador?

1.2.5 Interrogantes

- ¿Cuáles son los procesos que actualmente se ejecutan para la protección de los datos sensibles en la dirección distrital 23D01 de Educación de Santo Domingo de los Tsáchilas?
- ¿Cómo se caracteriza y protege la información sensible en las instituciones públicas del Ecuador?
- ¿Cuál es el estado actual de la protección de los datos sensibles que la Dirección Distrital 23D01 de Educación de Santo Domingo de los Tsáchilas gestiona y su eficiencia y reposición ante cualquier ataque informático?
- ¿A través de un modelo de gestión de la seguridad de la información para la Dirección Distrital 23D01 de Educación de Santo Domingo de los Tsáchilas se puede contribuir en la protección de los datos sensibles?

1.2.6 Delimitación del objeto de investigación

Campo: Sistemas.

Área: Seguridad Informática.

Aspecto: Modelo de gestión de seguridad lógica.

1.2.7 Delimitación Espacial:

Distrito de Educación 23D01 de la ciudad de Santo Domingo.

1.2.7.1 Delimitación Temporal:

Desde octubre 2018 a abril 2019.

1.2.7.2 Unidades de Observación:

Distrito de Educación 23D01 de la ciudad de Santo Domingo.

1.3 Justificación

El presente estudio se origina con el interés de mejorar la gestión de la seguridad de la información en los Distritos de Educación del Ecuador mediante la implementación de un modelo de gestión de seguridad lógica con lo cual se contribuirá en la protección de los datos sensibles de los distritos de Educación del Ecuador y para que se mejore desarrollo sostenible del país con una buena gestión educativa.

El documento expuesto cuenta con la originalidad establecida dentro de los márgenes de lo legal fundamentándose en contenido científico con temas relacionados al tema de investigación.

El alcance del proyecto se basará principalmente en ser un documento de apoyo para las instituciones distritales de educación del Ecuador y que pretendan utilizar el modelo de gestión como base del proceso de salvaguardar la información sensible de la entidad.

- **Factibilidad Técnica:**

  Técnicamente es factible el desarrollo del presente documento debido a que se cuenta con la infraestructura, herramientas tecnológicas y software suficiente para llevar a cabo la presente investigación.

- **Factibilidad Operativa:**

  Operativamente es factible el desarrollo de la presente investigación, ya que se tiene la apertura y acceso a todo tipo de documento e información por parte de la máxima autoridad de la institución.

- **Factibilidad Económica:**

  Los gastos que implicarán el desarrollo de este proyecto serán asumidos por el investigador quedando como factible en el ámbito económico.

1.4 Objetivos

1.4.1 Objetivo General

Determinar cómo incide un modelo de gestión de seguridad lógica en la protección de la información sensible del Distrito de Educación 23D01 de la ciudad de Santo Domingo.

1.4.2 Objetivos Específicos:

- Identificar las problemáticas existentes en cuanto a la gestión de la información y su relación con la seguridad lógica de sistemas.
- Desplegar un modelo de gestión de seguridad lógica de la información en el Distrito de Educación 23D01 de la ciudad de Santo Domingo.
- Proponer un modelo de gestión de seguridad lógica en la protección de la información sensible del Distrito de Educación 23D01.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Después de un análisis en distintas fuentes de información referente a la presente investigación, se acudió a la consulta de artículos científicos de varias universidades del Ecuador, tesis y libros que tienen similitud con las variables propuestas del presente tema, sin embargo, las mismas constan de una amplia diferenciación en cuanto a los objetivos, esto se debe a la solución que pretenden realizar los autores en cada publicación. De tal manera se detallan a continuación cada una de estas, focalizándose principalmente en lo que se consiguió con los temas expuestos:

Para Rea & Sánchez & Feliu & Manzano (2017), la seguridad informática es un proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso. Además, menciona que un modelo proporciona un punto de partida con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos. De un total de 201 artículos que mencionan modelos de madurez publicados desde el 2012 hasta el 2017 se concluye que:

- Todos los modelos expuestos en este estudio toman como referencia el modelo de madurez CMM, además del marco de referencia Cobit.
- Los modelos de seguridad informática actuales toman como referencia y son adaptaciones de otros modelos.
- También se identificó que los modelos de seguridad informática no son adaptables completamente a las necesidades particulares de una organización.

Según Sánchez et al (2014), con el aumento del volumen de la información surge la necesidad de reforzar la seguridad de los datos personales para garantizar su privacidad. Es pertinente tomar atención en cuanto a las amenazas existentes tales como: divulgación accidental, empleado curioso, violación de la privacidad de los datos personales sea este por parte de un individuo externo o interno de la organización y la intrusión no autorizada la red del sistema. Para lo cual los autores concluyen:

- Debido a la gran cantidad de procedimientos, normativas y estándares disponibles para la protección de los datos, y a las dificultades técnicas inherentes, resulta difícil para los trabajadores sanitarios encontrar una referencia o documento que reúna las buenas prácticas de seguridad informática en el tratamiento de la salud.
- La constante capacitación en cada uno de los funcionarios, en lo que a ciberseguridad se refiere, es de vital importancia para evitar errores que comprometen el sistema informático de la organización.

Los autores Parada & Flórez (2018), dan a conocer que las organizaciones se encuentran conformadas en primer nivel por tres elementos genéricos: los actores tales como los directivos, jefes, autoridades en si todo el recurso humano, en segundo nivel los métodos, actividades o políticas que orientan al proceso del negocio y en tercer nivel por la infraestructura tecnológica, es decir, las tecnologías de la información. Haciendo referencia a la importancia que tienen las TI en la evolución de las comunicaciones, y la manera que estas se puedan ver comprometidas en su trabajo o normal funcionamiento, debido a sus vulnerabilidades inherentes, bien sea por omisión o por fallas de configuración del responsable de su administración, lo que conlleva una probabilidad intrínseca para la materialización de amenazas, la cual puede desencadenar en fugas, pérdidas, alteraciones, destrucción entre otras anomalías sobre la información. Concluyendo los autores en la investigación con lo siguiente:

- Como resultado de las simulaciones empleadas en este estudio, se observa que los controles juegan un papel importante en la valoración de los activos.
- En los escenarios donde se realizan inversión en controles de seguridad de la información tienden a ser más sobrevalorados, a diferencia de escenarios donde los activos al no tener con que salvaguardarse de la materialización del riesgo, llegan a un punto en el cual se deprecian hasta llegar a cero.
- La dinámica de sistemas permite realizar simulaciones que pueden considerarse como experimentos en un sistema para su comprensión o pronóstico.

En la publicación de Roldán & Almache & Sila & Yevseyeva & Basto (2017), después de haber realizado una investigación bibliográfica detallada sobre la estructura de las Tics y las herramientas de recopilación de datos de ciberseguridad

se menciona herramientas como: Nessus, Saint8, Retina, Security Scanner, entre otras, que son de gran ayuda para establecer métricas de seguridad en una organización tales como: confidencialidad, impacto de integridad, etc. concluyendo con esta investigación:

- En el artículo se presentó un estudio para el desarrollo de un sistema de análisis y gestión de riesgos de ciberseguridad.
- Mediante los lineamientos de un modelo de referencia en context-aware, se abordaron las capas de percepción, comprensión, proyección y decisión/acción, llevando a cabo un análisis de las características de recopilación de datos de infraestructura de TI.

2.2 Fundamentación Filosófica

Por características propias, el presente trabajo de investigación se enmarcará en el paradigma Crítico Propositivo, siendo Crítico porque se realizará un análisis crítico de la situación actual del Distrito de Educación 23D01 y Propositivo ya que se planteará una solución ante el problema.

2.3 Fundamentación Legal

La presente investigación se fundamenta en el acuerdo ministerial N° 166 publicado mediante Registro Oficial No. 88 del 25 de septiembre de 2013 que textualmente indica *"En concordancia con el Plan Nacional de Gobierno Electrónico 2014-2017 del Ecuador, reforzando el principio de garantizar seguridad y confianza y como parte del Plan Estratégico de Seguridad y Protección de Datos, el EGSI es un instrumento de vital importancia para todos los actores del Plan Nacional: ciudadanos, servidores, empresas, y gobierno y otros actores del estado".*

La Ley Orgánica del Servicio Público, en su artículo 22, literal h) "***Establece como deberes de los servidores públicos, ejercer sus funciones con lealtad institucional, rectitud y buena fe".***

La norma de control interno (NCI) 401-10 – Seguridad de la tecnología de la información determina que: ***"La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra perdidas y fugas de los medios físicos y la información que se procesa mediante sistemas informáticos"***

2.4 Categorías Fundamentales

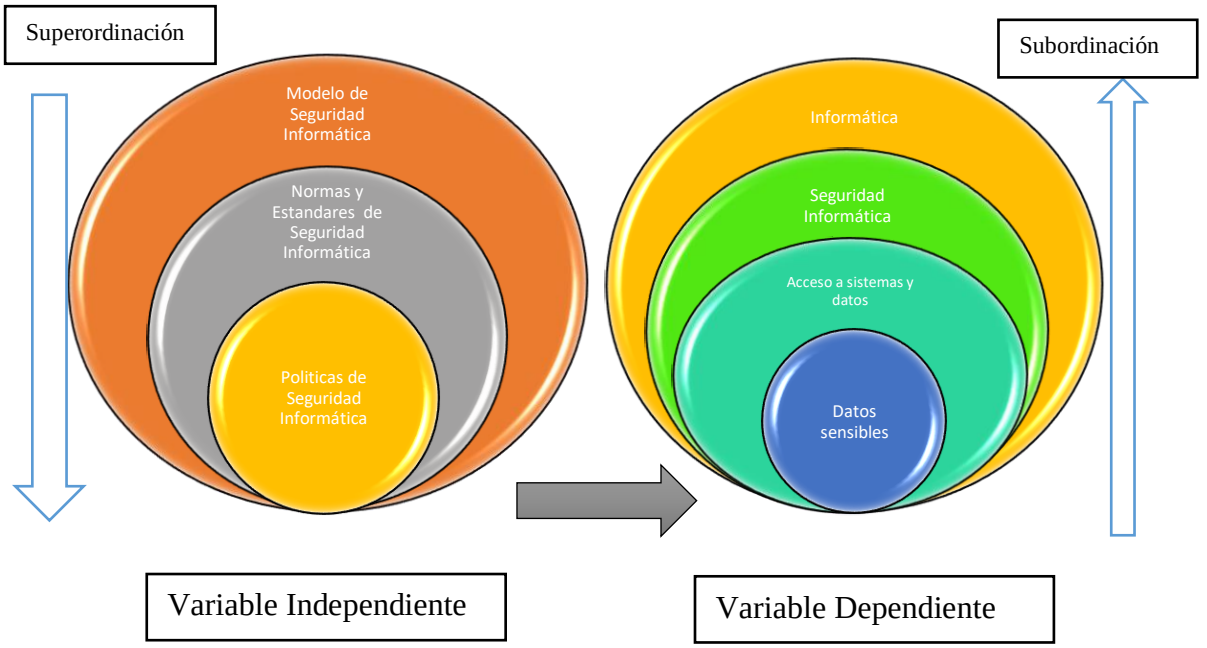


Figura 2 Inclusiones Conceptuales

Elaborado por: ***Vaca, P (2018)***

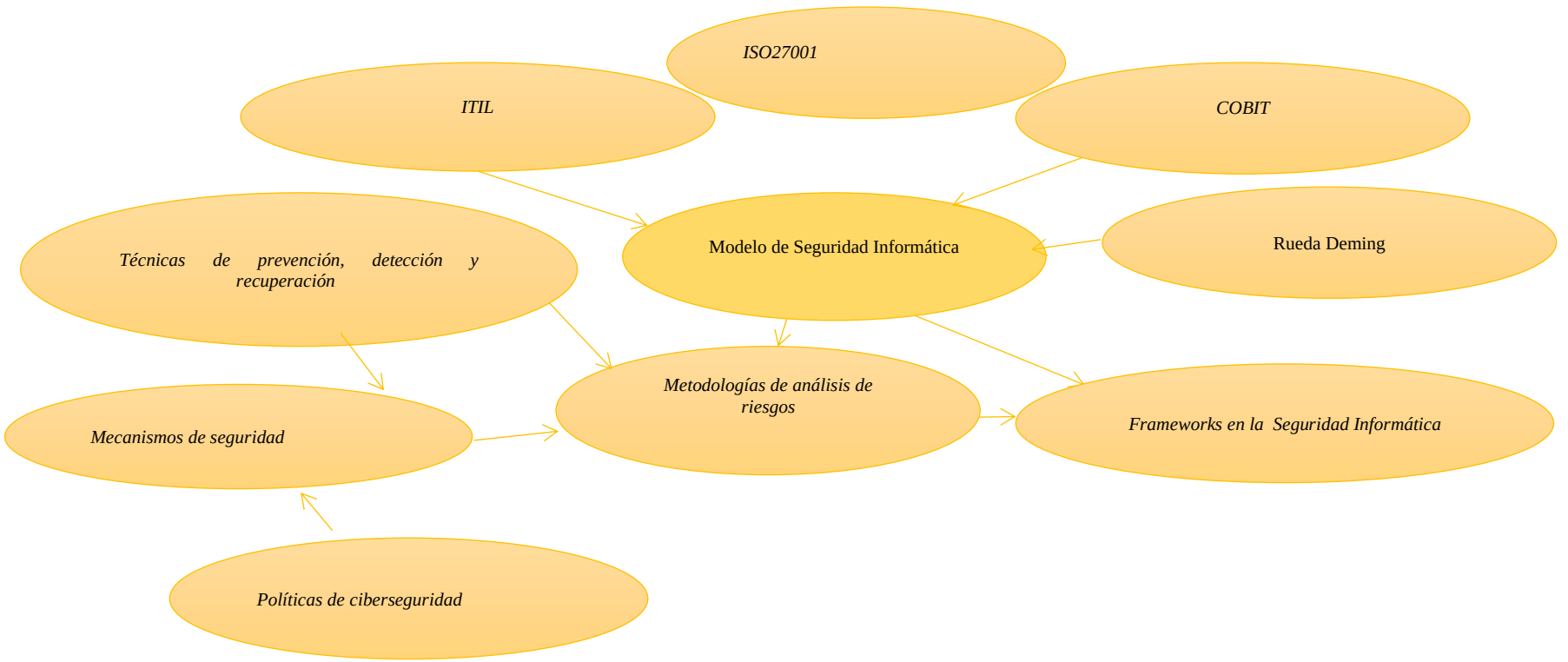


Figura 3 Constelación de Ideas de la Variable Independiente

Elaborado por: *Vaca, P (2018)*

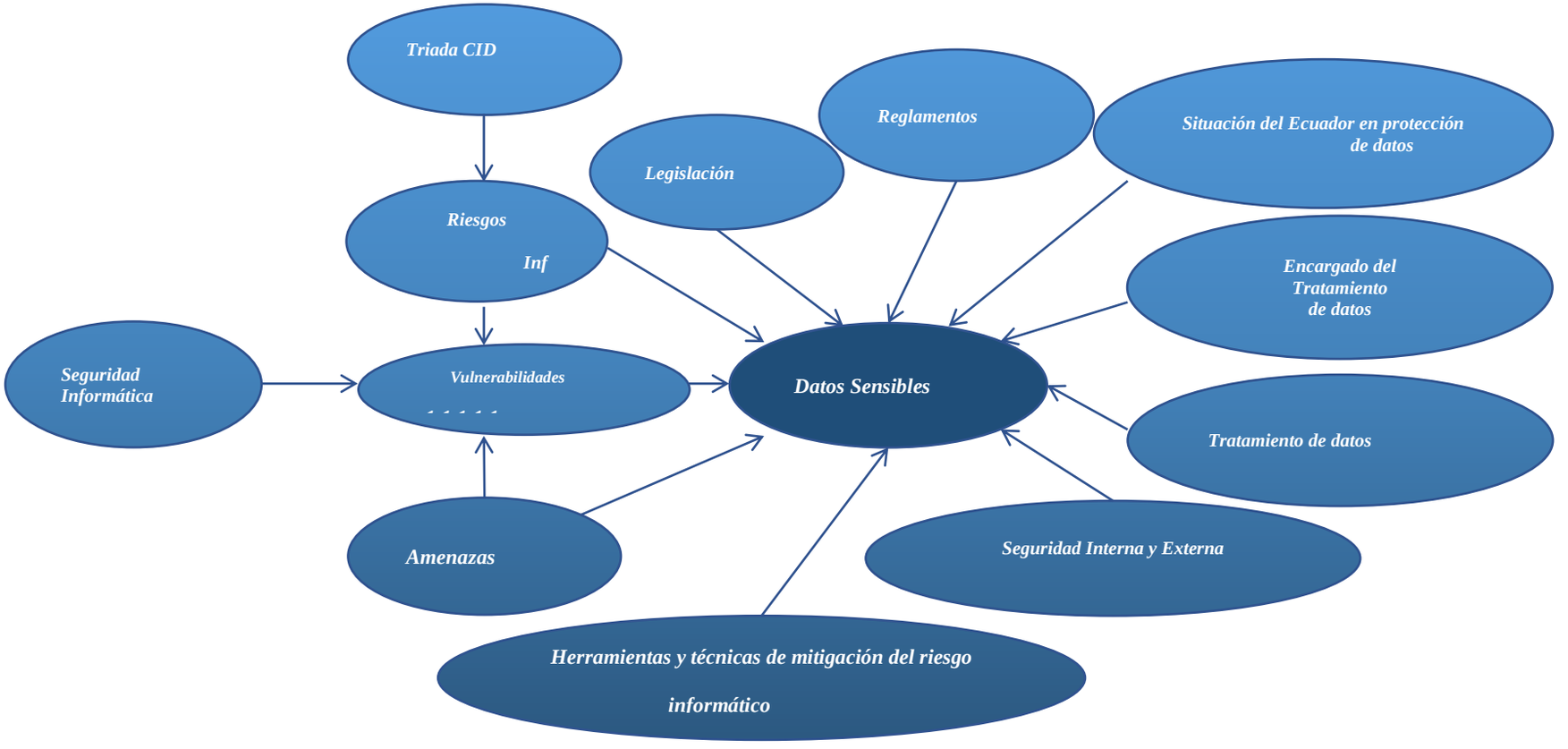


Figura 4 Constelación de Ideas de la Variable Independiente

Elaborado por: ***Vaca, P (2018)***

2.4.1 Marco Conceptual Variable Independiente:

2.4.1.1 Modelo

Para la Real Academia de la lengua española (RAE), un modelo constituye un arquetipo o punto de referencia para imitarlo o reproducirlo. En empresas el termino es usado en aposición para indicar que ha sido creado como ejemplar o puede serlo. Sin embargo, un modelo es un ente que representa de forma precisa algo que será realizado o ya existe, considerado como una representación simplificada de la realidad en la que aparecen algunas propiedades (CHIAPAS & MARTÍNEZ, 2009). En relación a los conceptos expuestos, un modelo representa una plantilla en la que se hace constar los pasos a seguir en la resolución de un problema, que se encuentra ya realizado, comprobado y autorizado.

2.4.1.2 Modelo de Seguridad Informática

Desde la perspectiva de la seguridad informática, en su publicación Aguilera afirma que un modelo de seguridad es la expresión formal (redactados fundamentalmente en términos técnicos y matemáticos) de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información (Aguilera, 2010).

Bajo el mismo concepto Gómez menciona, que un modelo de seguridad AAA (Autenticación, Autorización y Registro), se utiliza para poder identificar a los usuarios y controlar su acceso a los distintitos recursos de un sistema informático registrando además cómo se utiliza dichos recursos (Gómez, 2011).

De este modo, un modelo de gestión de seguridad informática se considera como un esquema o marco de trabajo en el que se incorpora un conjunto de características, atributos, indicadores o patrones, que proporciona un punto de referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos con los cuales se puedan cumplir con objetivos y prioridades.

Aunque un modelo de seguridad informática contribuye de manera positiva en la protección de la información de una organización, es importante que para que los objetivos estratégicos de una organización se cumplan se debería llevar a una organización hacia una arquitectura empresarial.

2.4.1.3 Arquitectura Empresarial

La arquitectura empresarial (AE), es una organización lógica de los procesos de negocio e infraestructura de tecnologías de la información (TI), reflejando la integración y estandarización de los requerimientos del modelo operativo de la empresa. Por medio de esta arquitectura una organización puede modelar la organización de TI, ya que esta forma se consiga que la entidad se desarrolle a partir de las necesidades desde una perspectiva de negocio en el cual todos los esfuerzos e inversiones realizados en materia de seguridad sea vista como una inversión y no como un gasto (Santiago, 2013).

En tal virtud una AE, se la considera como la organización de procesos de negocios e infraestructura de TI, en las que se ve a las adquisiciones en temas de seguridad como una inversión debido a la tasa interna de retorno TIR que esta ofrece y no como un gasto innecesario.

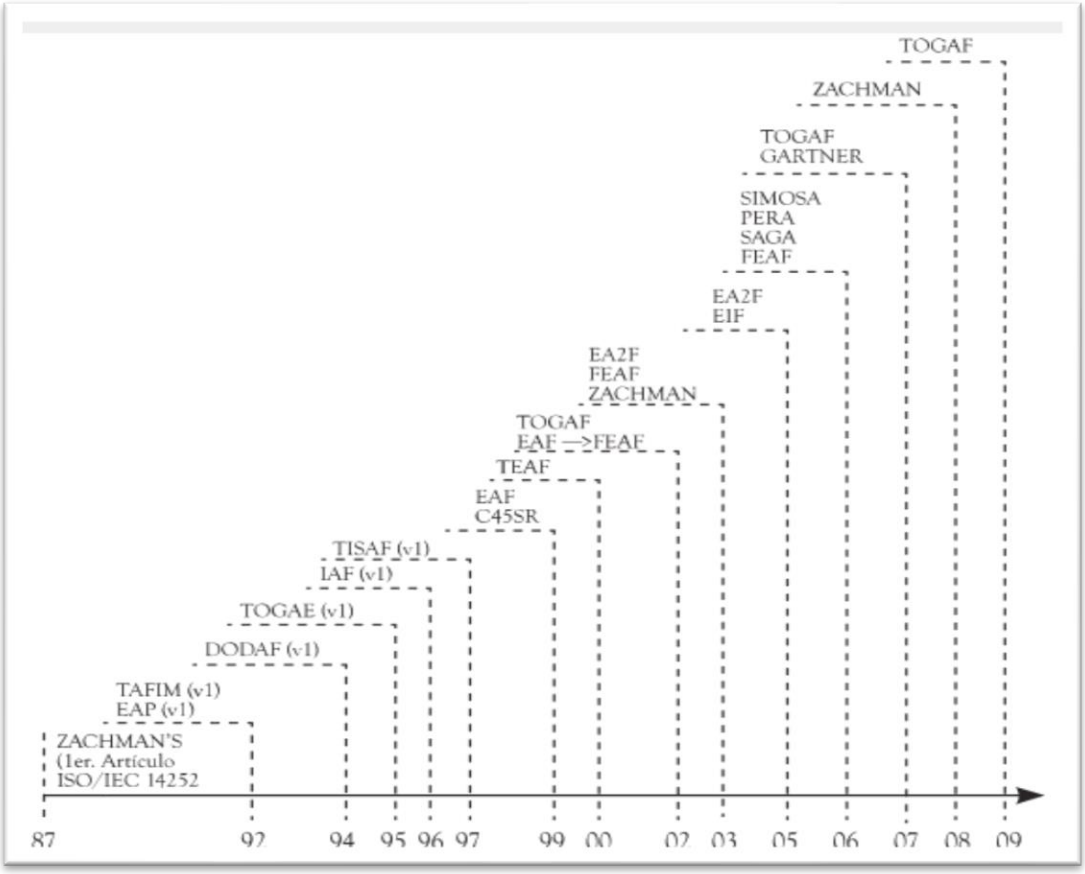


Figura 5 Evolución cronológica de los Frameworks de AE

Fuente: (Arango et al., 2010)

2.4.1.4 Marcos de Trabajo de una Arquitectura Empresarial.

Arango et al en su publicación menciona la evolución cronológica de los principales marcos de trabajo que se utilizan en la AE, cuyo concepto nace en 1987 con la publicación de J. Zanchman en el diario de IBM Systems, titulado "Un marco para la arquitectura de sistemas de información" de los cuales se destacan los Frameworks Zanchman y Togaf (Arango, Londoño, & Zapata, 2010).

De esta manera Jaramillo & Cabrera & Abad & Verdúm (2015) dan a conocer que Zanchman Framework se lo utiliza para realizar representaciones descriptivas o modelos de una empresa, y Togaf proporciona los métodos y herramientas para ayudar en la aceptación, producción, uso y mantenimiento de una AE, se basa en un modelo de procesos iterativo, el apoyo de las mejores prácticas y un conjunto reutilizable de activos existentes.

Marcos de trabajo / Componentes	TOGAF	Zachman Framework
Aporta beneficios de TI	x	x
Basado en entregables	x	x
Adaptable a las necesidades de una empresa	x	x
Gestión de infraestructura	x	x
Centrado en las actividades del negocio	x	
Organización y clasificación de artefactos	x	x
Gestión de requerimientos	x	
Gestión de alcance	x	x
Gestión de cambios	x	x

Figura 6 Cuadro comparativo entre Zanchman y Togaf

Fuente: (Jaramillo et al., 2015)

Para el autor Santiago (2013) los principales Frameworks existentes y analizados en su estudio para la propuesta de una AE las principales razones de utilizar Togaf son las siguientes:

- Framework de uso libre.
- Brinda documentación y guías de apoyo.
- Es reconocido internacionalmente como apoyo del desarrollo de una AE.
- Framework neutro lo cual permite integrarse con otros marcos de referencia y en este caso con marcos de referencia de seguridad informática.

2.4.1.5 Las Buenas Prácticas (Marcos de trabajo en seguridad informática)

Las buenas prácticas se han constituido como la esencia de construcción de nuevos procesos organizacionales, llevándolas desde una experiencia exitosa, pasando por una práctica prometedora, hasta conseguir una buena práctica. Por tal razón la mejor manera de conseguirlas es comparándose o realizando benchmarking con instituciones y estándares similares. Para ello en la Tabla 3 se detallan marcos de trabajo utilizados en seguridad informática (Baud, 2017):

Tabla 2 Marcos de Trabajo

MARCOS DE TRABAJO	DESCRIPCIÓN
Cobit	(Control Objectives for Information and releated Technologies) permite auditar y evaluar los servicios informáticos de una empresa para valorar la robustez en términos de seguridad y conformidad.
El Modelo Cmmi	Concreta los procesos que van a permitir alcanzar el nivel cinco de madurez (capacidad de conocer, capacidad de actuar).
Las Normas	Son documentos que definen las exigencias, y establecen directivas y características a utilizar. Entre las principales normas que interesan en informática son ISO, y AENOR.
Itil	Colección de libros que tratan acerca de la infraestructura de las tecnologías de la información. El enfoque de ITIL se basa en la experiencia o en las buenas prácticas, es abierto, no propietario y público.

Elaborado por: ***Vaca, P. (2018)***

2.4.1.6 Metodologías de Análisis de Riesgos

RAE, define a una metodología como el conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal. A pesar de ello Cairo et al, indican que una metodología es una secuencia sistémica de etapas una de las cuales incluye acciones o procesos dependientes entre sí y que permiten el logro de determinados objetivos. En seguridad informática esta definición no cambia solo que se amplía en relación a su contexto (Cairo, Puga, Mallea, Cobas, & Sánchez, 2016).

A continuación, se detallan las metodologías empleadas en cuestión de seguridad (Baca, 2016):

Tabla 3 Metodologías empleadas en seguridad informática.

METODOLOGÍA	DESCRIPCIÓN
CITICUS ONE	Software comercial que implementa el método FIRM del Foro de Seguridad de la información.
CRAMM	Originalmente desarrollado para uso del gobierno de Reino Unido.
ISO TR 13335	Precursor de la ISO/IEC 27005.
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información alineada a la ISO/IEC 27005 y otras metodologías internacionales.
ISO 27000 ISO 27001 ISO 27032	Presenta los requerimientos para una adecuada gestión de la seguridad de la información.

Fuente: (Baca, 2016)

2.4.1.7 Normas ISO en Seguridad Informática

Una norma es un documento cuyo uso es voluntario, que es fruto del consenso de las partes interesadas y que deben aprobarse por un organismo de Normalización reconocido. Entre los que se pueden mencionar la Organización Internacional para la Estandarización ISO (García, Cervigón, & Alegre Ramos, 2011).

Dentro de las normas ISO en cuanto a seguridad se refiere se dan a conocer las siguientes:

Tabla 4 Normas de la Familia ISO 27000 para la gestión de seguridad de la información.

NORMA	DESCRIPCION
ISO 27000	Contiene una visión general de las normas relacionada con la seguridad informática.
ISO 27001	Sustituye a la ISO 17799-1, basada en la norma BS 7799-2 de British Estándar y se fundamenta principalmente en preservar la información desde la confidencialidad, integridad y disponibilidad.
ISO 27002	Describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendables relacionados con la seguridad.
ISO 27003	Contiene una guía para la implementación de la norma.
ISO 27004	Implementa estándares para poder evaluar el sistema de gestión de la seguridad de la información.
ISO 27005	Recoge el estándar para la gestión del riesgo de la seguridad de la información.
ISO 27006	Indica los requisitos a cumplir por las organizaciones encargadas para emitir certificaciones ISO 27001.

Fuente: (García, Cervigón, & Alegre Ramos, 2011)

2.4.1.8 Integración de ADM-TOGAF Y SABSA

Jaramillo et al (2016) definen a SABSA (Sherwood Applied Business Security Architecture o Arquitectura de Seguridad de información en la empresa de Sherwood) como una metodología enfocada en el desarrollo de arquitecturas de seguridad empresarial. El integrar ambos Frameworks brinda soporte a los arquitectos empresariales, para tomar en cuenta la gestión del riesgo operacional proporcionando orientación que describe como TOGAF y SABSA se pueden combinar, en la Figura 7 se da a conocer el ciclo de vida de SABSA relacionado con ADM-TOGAF en la que cada iteración realiza un trabajo específico.

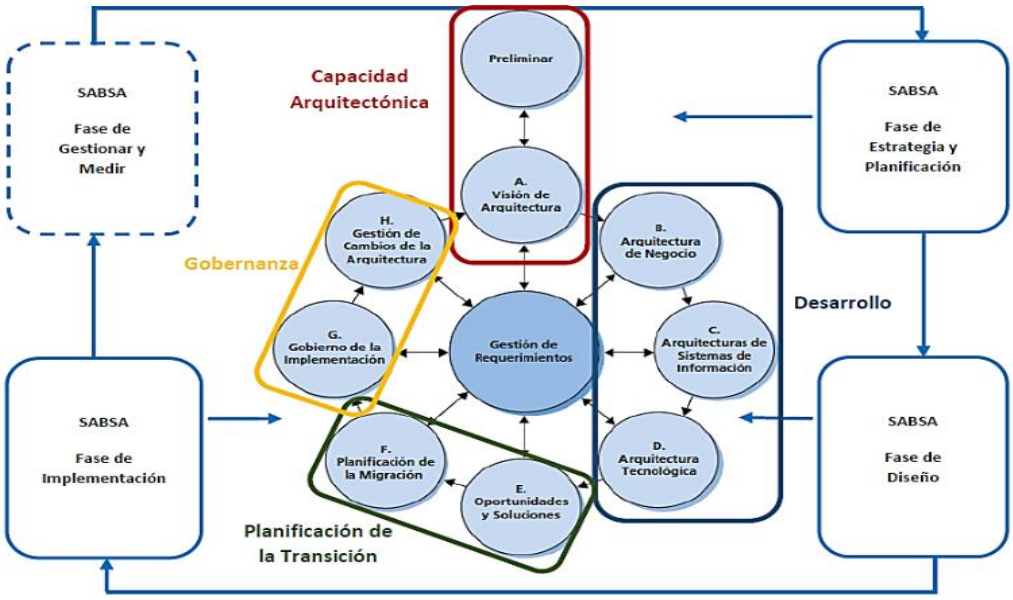


Figura 7 Integración de ADM-TOGAF con SABSA

Fuente: Jaramillo et al (2016)

Además, la integración de ADM de TOGAF y SABSA orientada a la seguridad informática, en la que se puede aprovechar una AE ya implementada junto a sus elementos desarrollados, con los que se determinan los controles y procedimientos que se acoplen en la arquitectura. Los lineamientos de la sirven de base para la elaboración de un modelo de seguridad informática para una AE, mediante la integración de ADM de TOGAF y SABSA (Jaramillo et al., 2015).

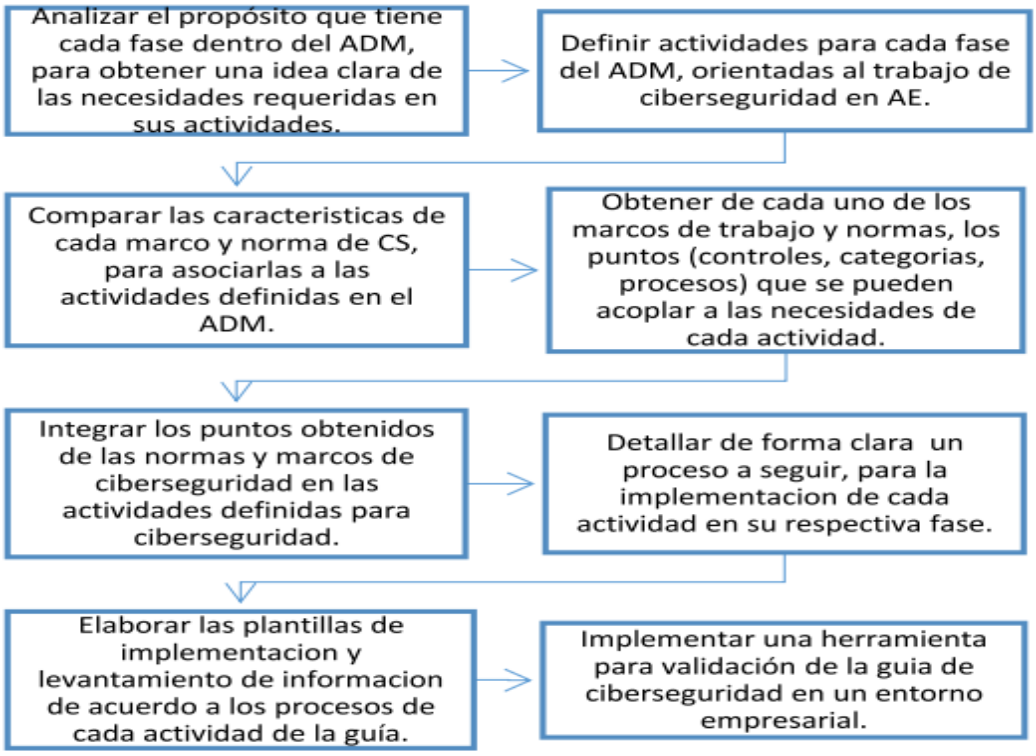


Figura 8 Pasos a seguir para la elaboración de un modelo de seguridad para AE.

Fuente: (Jaramillo et al., 2015)

2.4.1.9 Rueda de Deming

Coincidiendo con Ríos, La rueda Deming, es la mejora continua del servicio, o ciclo PHCA(Planificar, Hacer, Comprobar y actuar) surge con el objetivo de la mejora de los procesos industriales, en los cuales se pretendía optimizar la producción reducir los costes para ofrecer un producto más económico pero sin dejar a un lado la calidad del mismo, cuya filosofía principal es analizar, planificar y actuar sobre la información obtenida con el objetivo de ir realizando mejoras que aporten en soluciones de gestión (Ríos, 2014) .

Cabe mencionar la definición de Carpentier (2016) la rueda de Deming o PDCA (Plan, Do, Check, Act) propone controlar y mejorar un proceso mediante el uso de un ciclo continuo de cuatro etapas para que mediante la ejecución de este ciclo se logre reducir la necesidad de correcciones.

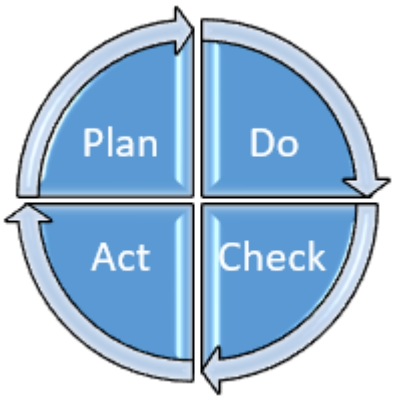


Figura 9 Rueda de Deming

Fuente: (Carpentier, 2016)

Bajo estas definiciones se determina que la rueda Deming se enfoca en cuatro procesos significativos y que persiguen la mejora continua de los procesos de una organización. En seguridad informática este concepto se mantiene debido a que se debe planificar políticas de seguridad (Plan), que se basen en los principios y objetivos mediante el análisis de la situación actual de la organización. Acto seguido se procede con la ejecución (Do) de los planes analizados y establecidos para después evaluar (Check) los resultados obtenidos para que de esta manera se evidencie si los objetivos planteados en el plan han sido conseguidos. Como este ciclo persigue la mejora continua (Act) se realizan las modificaciones pertinentes para que los objetivos sean cumplidos.

Amutio et al (2012) da a conocer una versión más detallada de la rueda Deming en la siguiente Figura:

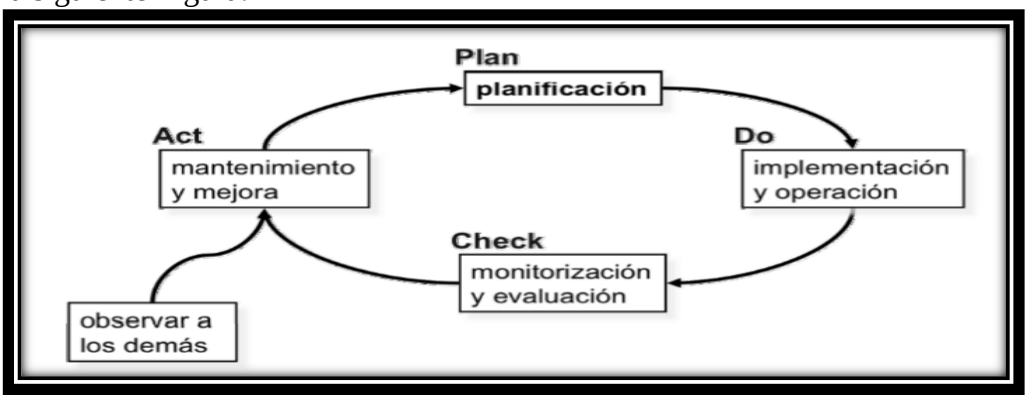


Figura 10 Ciclo PDCA de Deming

Fuente: (Amutio et al., 2012)

2.4.1.10 Políticas de Seguridad Genéricas

Para Areitio, la política de seguridad puede formularse de la siguiente forma: la información no puede darse, ni puede permitirse el acceso a ella, ni se puede permitir que sea inferida, ni se puede utilizar ningún recurso por parte de personas que no estén autorizadas de forma apropiada (Areitio, 2008).

A su vez Castro menciona que una política de seguridad puede definirse como una serie de normas que deben cumplir todas las personas que tengan acceso a cualquier información y/o tecnología de una organización (Castro, Díaz, Ignacio, & Elio, 2014).

Estas afirmaciones tienen sentido debido a que una política de seguridad debe ser cumplida por todo el personal interno y externo de una organización, además de estar alineada a las estrategias y políticas de gobierno para que los principios de la seguridad informática no se vean afectados.

2.4.1.11 Plan de Seguridad

Conjunto de tareas y procedimientos encaminados a la correcta y adecuada gestión de incidentes de seguridad junto con las personas designadas para llevar a cabo todas y cada una de estas tareas (Chicano, 2014).

En su sitio web la Universidad Internacional de Valencia indica que, un plan de seguridad permite aclarar inquietudes que se presenten acerca de las vulnerabilidades detectadas en los sistemas de información cuya meta principal es que una vez detectadas estas vulnerabilidades permita tomar las medidas necesarias en la prevención de problemas, además este plan debe contribuir en la protección de los datos de los sistemas críticos de una organización, mismo que debe estar basado en la ley de protección de datos (Universidadviu, 2018).

2.4.1.12 Procedimiento de Seguridad

Según Gómez (2011) un procedimiento de seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinada.

Figura 11 Jerarquía de políticas, planes y procedimientos de Seguridad Informática

Fuente: (Gómez, 2011)
Elaborado por: *Vaca P. (2018)*

De tal manera en la Figura 11 se ubica en la parte superior los objetivos esenciales que persigue la seguridad informática como es la Triada CID, es decir, garantizar la Confidencialidad, Integridad y Disponibilidad de la información. Luego de que los objetivos se encuentren definidos es de vital importancia definir las políticas, planes y procedimientos de Seguridad que se implementarán en la organización.

Así mismo los procedimientos de se desglosan en tareas y operaciones especificas mismos que pueden generar registros y evidencias que aportan en el seguimiento, control y supervisión del funcionamiento de un Sistema de Gestión de Seguridad de la Información SGSI (Gómez, 2011).

2.4.1.13 Mecanismos de Seguridad

Los mecanismos de seguridad son herramientas técnicas y métodos técnicos que se utilizan para implementar los servicios de seguridad, entre los más comunes se tienen: cifrado, resúmenes de mensajes y firmas digitales, certificados digitales, infraestructura de claves públicas (PKI) (IBM, 2016).

De acuerdo con Areitio (2008), los mecanismos de seguridad proporcionan y brindan soporte a los servicios de seguridad los cuales se dividen en dos clases:

Mecanismos de seguridad específicos, son utilizados para salvaguardar la confidencialidad, integridad, autenticación. Entre los mecanismos de seguridad específicos se dan a conocer los siguientes:

- Cifrado de clave pública.

- Firma digital.
- Mecanismos de control de Acceso
- Mecanismos de Integridad de datos como los MAC, hash o firma digital.
- Intercambios de autenticación.
- Relleno de tráfico.
- Control de encaminamiento.
- Notarización, con notarios o fedatarios electrónicos.

Mecanismos de seguridad generalizados, considerados como no específicos para servicios específicos, tales como: responsabilidad-auditoría, recuperación de la seguridad.

2.4.2 Marco Conceptual Variable Dependiente: Seguridad Lógica

2.4.2.1 Informática

La informática es una ciencia encargada del estudio y desarrollo de máquinas para tratar y transmitir información, así como, de los métodos para procesarla. En un concepto más sencillo la informática es el conjunto de ciencias y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras (De Pablos & Otros, 2004).

2.4.2.2 Tecnologías de la información TI

Se entiende como conjunto tecnologías y recursos asociados a los sistemas de información y comunicación, siendo TI un conjunto de tecnologías que aseguran la gestión eficiente de la información que se genera en una empresa (Seaone, 2005).

2.4.2.3 Gestión de TI

La gestión de los servicios de tecnologías de la información, es considerado como un conjunto de capacidades organizacionales especializadas en proporcionar valor a los clientes en forma de servicios. Estas capacidades organizacionales permite gestionar de forma eficaz los servicios ofrecidos a lo largo de su ciclo de vida en la cual resulta sumamente importante adoptar un conjunto de buenas prácticas (Mesquida, Mas, & Amengual, 2009)**.**

2.4.2.4 Seguridad Informática

La Seguridad Informática (SI) es el conjunto de actividades centradas en mecanismos defensivos y ofensivos empleados tanto para proteger el ciberespacio contra el uso indebido del mismo, defender su infraestructura tecnológica, los servicios que prestan y la información que manejan. La meta final de la SI va acorde con los objetivos que la seguridad informática persigue tales como: Confidencialidad, Integridad y Disponibilidad de la información (Jaramillo et al., 2016).

Por su parte Diaz & Muñoz (2018) afirman que, la SI hace referencia al empleo de modelos, normas, marcos de trabajo, estándares, metodologías, técnicas, herramientas y estructuras organizaciones enfocadas a salvaguardar la información en sus diferentes formas y estados**.**

Estas afirmaciones van de la mano en cuanto a SI se refiere, debido a que sin el empleo de metodologías, técnicas y modelos el mitigar o protegerse de ataques sería un esfuerzo que no tendría mucho éxito.

2.4.2.5 Servicios de la Seguridad Informática

Confidencialidad

La confidencialidad, es un principio de la seguridad informática en el cual la información sólo debe ser accesible para aquellos clientes y/o usuarios a lo que está dirigida (Ríos, 2014).

Guillen & Ramírez & Cifuentes (2017) afirman que, la confidencialidad busca garantizar que la información del usuario sólo sea conocida por él y por los usuarios a los cuales él autorice. Es así que la confidencialidad es un principio de la seguridad informática con el cual la información solo debe ser vista por el usuario o por las personas que dio la autorización para ser manipulada.

Integridad

Desde el punto de vista de la SI Caballero (2017) la integridad hace referencia al mantenimiento de la exactitud y complejidad de la información y los métodos de proceso.

Además, Romero et al (2014) indican que la integridad de la información significa que no debe ser posible que sea alterado en caso que sea interceptada la

información. Para que la información sea única, es decir, original este principio de la seguridad de la información garantiza que en ninguno de los casos los datos se hayan expuesto y manipulado por terceros.

Disponibilidad

Con el servicio de disponibilidad lo que se requiere es garantizar que la información se encuentre lista a ser accedida cuando se necesite (CHIAPAS & MARTÍNEZ, 2009).

Para Amutio et al (2012) definen disponibilidad como la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones. Aunque suene contraproducente es importante que se garantice la confidencialidad y la integridad de la información usando métodos y técnicas propias de cada servicio, pero si en esta actividad se ve afectada la disponibilidad que es garantizar el 99.9% cuando se la requiera, afectaría de manera directa a este principio de la seguridad informática.

Autenticación

Según Aguilera (2010) debe conocerse en todo momento que persona realiza las operaciones, para que tenga las mismas garantías que si las realizará personalmente en la empresa.

En concordancia con Gómez, la autenticación garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, destinatario de un mensaje podrá estar seguro que su creador es la persona que figura como remitente de dicho mensaje La autenticación hace referencia al proceso de verificación de las credenciales de un usuario, que mediante un sistema de logs o registros se garantiza que una persona realizó un proceso en un sistema de información (Gómez, 2011).

No repudio

El no repudio, es un servicio de la seguridad informática que pudiera ser emitido por un mecanismo como la firma digital, la integridad de los datos o su registro (Carpentier, 2016).

Por su parte Stallings menciona, que el no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje (Stallings, 2004).

Es de gran importancia garantizar que se cumpla con este servicio, ya que con esto se certifica que tanto el emisor como el receptor fueron participes en el envío y recepción de un mensaje.

2.4.2.6 Principio de "Defensa en Profundidad"

Jara y Pacheco (2013). señalan, en el área militar se utiliza el termino defensa en profundidad para denotar el uso de varias líneas de defensa consecutivas, cada una de ellas con un nivel de protección creciente, en vez de una única barrera muy fuerte.

Además, Gómez (2011) menciona, este principio consiste en el diseño de varios niveles de seguridad dentro del sistema informático de la organización. De este modo, si una de las barreras es franqueada por los atacantes, conviene en disponer de medidas de seguridad adicionales que dificulten y retrasen su acceso a información confidencial o el control por su parte de recursos críticos del sistema.

Figura 12 Principio de Defensa en profundidad.

Fuente: (Gómez, 2011)

En tal virtud el principio de Defensa en profundidad hace referencia que en el proceso de garantizar el resguardo de la información se implementen nuevas barreras en las que en la última capa se encuentren de manera encriptada los datos sensibles de una organización, con esto se consigue que un atacante al pasar por varias barreras de seguridad se tome más tiempo de lo que le tomaría romper una sola barrera robusta.

2.4.2.7 Sistema de Gestión de Seguridad de la información

Un Sistema de Gestión de Seguridad de la información (SGSI), ayuda a establecer políticas y procedimientos en relación a los objetivos de negocios de la organización, con el propósito de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decido asumir (Neira & Spohr, 2010).

Por su parte Baud afirma que, el SGSI contiene toda la información relativa a la seguridad del sistema de información. Este sistema se estructura alrededor de cuatro ejes (Baud, 2017):

- La información sobre la seguridad de la empresa,
- Las normas,
- Los estándares y
- La legislación que se aplican a la seguridad del sistema de información, los procedimientos de gestión y las directivas e instrucciones.

Bajo estos conceptos un SGSI contribuye en el establecimiento de políticas y procedimientos en relación a los objetivos institucionales de una organización. Además, el SGSI contiene las normas, estándares y la legislación referente a la seguridad de la información.

2.4.2.8 Riesgos Informáticos

Se considera a un riesgo informático como un evento o conjunto de eventos que puede poner en peligro un proyecto de la organización o que puede impedir su éxito (Chicano, 2014).

De igual manera Carpentier (2016) considera al riesgo como la probabilidad que un acontecimiento critico se presente en una organización. De esta forma un riesgo se lo clasifica según sus orígenes los cuales pueden ser: externos o internos.

Dadas estas afirmaciones un riesgo informático, se lo considera como un atentado que afecta de manera negativa a una organización interrumpiendo principalmente los servicios que la SI identificados en la triada CID.

2.4.2.9 Vulnerabilidad

A la vulnerabilidad se la define como una debilidad y por lo tanto es cualquier acción o elemento que no se haya protegido contra una posible amenaza (Rubio, Gómez, & Letón , 2017).

Caballero (2017) menciona como vulnerabilidad a cualquier factor de riesgo interno que representa las falencias o el grado de exposición de los activos informáticos de la organización, lo cual influye en la facilidad que un ciberdelincuente realice un ataque. Así mismo, en informática, una vulnerabilidad es cuando la información tiende a ser de fácil acceso ante una amenaza.

Se puede definir a una vulnerabilidad como, una puerta de acceso hacia un sistema de información, la cual no se encuentra debidamente protegida por algún mecanismo de seguridad, debido a que permite que una amenaza (malware, exploit, entre otros) se incruste en un sistema.

2.4.2.10 Acceso a los Sistemas y los Datos

La protección del acceso al sistema y a los datos es la parte más importante de la estrategia global de la seguridad. Esta comprende varias dimensiones y trata de elementos físicos y lógicos (Carpentier, 2016).

De acuerdo con Areitio, el acceso a los sistemas de información debe estar disponible solo para quienes lo necesitan y se encuentran autorizados para el descargo de la información (Areitio, 2008).

Al enfatizar estos conceptos, el acceso a los SI se contempla desde dos perspectivas: tanto lo físico como lo lógico. Es así, que este acceso se debe de garantizar que esté disponible para aquellos usuarios que se encuentran previamente autorizados y cuente con los privilegios necesarios para la recuperación de la información.

Seguridad Física.

La seguridad física de los centros de datos tiende a ser vulnerables si una persona con malas intenciones logra acceder físicamente a los servidores o si se produce una catástrofe natural (Rault, Laurent, ACISSI, & Agé, 2015).

Según Calle (1997), la seguridad física hace referencia a los mecanismos que una organización tiene que adoptar para salvaguardar al personal, equipos e instalaciones relacionados con las TI, de los riesgos y amenazas que puedan ser causados por catástrofes naturales o por actos agresivos causados por el personal externo o interno de una entidad.

Es así que, se considera como seguridad física a todo proceso, mecanismo o medida que una organización debe adoptar para resguardar su infraestructura tecnológica de cualquier amenaza sea esta de índole natural o provocada por algún usuario malintencionado.

Seguridad Lógica

La seguridad lógica es toda aquella relacionada con la protección directa de los datos y de la información, de tal forma que a mayor envergadura de la organización la información está mucho más comprometida, debido a que comprende no solo la economía, los bienes y servicios, sino también la información relativa a personas que mantienen contacto con la empresa: personal, clientes, proveedores, entre otros (Aguilera, 2010).

La seguridad lógica enmarca el conjunto de técnicas y lineamientos orientadas a la protección de la información contra la destrucción, perdida de la integridad, confidencialidad y disponibilidad de una organización (Desongles, Martos , Santos, & González , 2004).

Seguridad de la Información Personal.

Mendoza señala que los datos personales se refieren a la información del individuo, quien permite identificarlo a través de su descripción, origen, lugar de residencia, trayectoria académica, laboral entre otros. De otro modo Mendoza indica que, los datos personales también pueden ser sensibles, al describir aspectos sobre el individuo, como su forma de pensar, el estado de salud, las características físicas, ideología, vida sexual, entre otros (Mendoza Enríquez, 2018).

Por su parte Gómez (2011) da a conocer que el derecho a la intimidad y a la privacidad hace referencia al derecho que poseen las personas de poder excluir a terceros del conocimiento de su vida personal, es decir, de sus sentimientos, emociones, sus datos biométricos y personales y su propia imagen.

Es así que la seguridad de la información personal garantiza que todo individuo tiene derecho a mantener excluida su información a terceras personas siendo este quien autorice quien y que puede conocer su información sensible.

2.4.2.11 Declaración Universal de Derechos del Hombre

El primer acercamiento de la vida privada de una persona se dan a finales del siglo XIX, pero para la mitad del siglo XX este derecho adquiere mayor relevancia (Enríquez Álvarez, 2017).

El Articulo 12 menciona: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación". Termina indicando "Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"(Naciones Unidas, 1948).

Las Naciones Unidas vela por la protección de datos personales en los que se vean expuesto su honra e intimidad, y garantiza que este derecho se cumpla en cualquiera de las instancias.

2.4.2.12 Constitución Ecuatoriana sobre Protección de Datos Personales

La constitución del 2008 de Ecuador en el Articulo. 66 numeral 19 cuyo capítulo habla sobre los Derechos a la libertad instituye la protección de datos personales dando a conocer: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"(Asamblea Nacional, 2008).

2.4.2.13 Legislación Ecuatoriana sobre Privacidad

Según Estrada et al (2015), la privacidad es considerada como el derecho universal declarado en los derechos humanos de las naciones unidas.

Ecuador ha tenido un avance pausado en la legislación de la protección de los datos personales. Aunque desde 1998, la constitución política hacia una leve referencia del derecho a la intimidad y al secreto de la correspondencia. En el 2002 se da a conocer la ley que entre sus líneas constaban acciones sobre el comercio electrónico, firmas digitales y mensajes electrónicos. En este mismo año, el Articulo 9 de la constitución política menciona la protección de los datos, pero se concreta con datos que tendrán libre circulación únicamente con consentimiento del titular o con orden de autoridad competente. Ya para el año 2008, se da a conocer la acción jurisdiccional de Habeas Data considerado en el Artículo 92, derecho que permite a una persona u organización estar al tanto, autorizar y rectificar datos que la describan y reposen en bases de datos tanto públicas como privadas. Avanzando en el tiempo, para el 2010, se expide la Ley del Sistema Nacional de Registro Público (LSNRDP), que se encargaba de regular la manera que se almacena y accede a los datos públicos con el objetivo de transparentar y organizar el acceso a las fuentes de datos que las organizaciones poseen de una persona determinada.

2.4.2.14 Principio de "HABEAS DATA"

En su publicación Gil define al Habeas Data (HD) como una acción jurisdiccional que: brinda la potestad al concernido de los datos personales de reivindicar a los administradores de datos personales la recuperación, la inclusión, exclusión, edición, adición, actualización , y certificación de los datos, como también de las restricciones y controles que existen en temas de: divulgación, publicación o cesión de estos, en relación a los principios detallados en la administración de bases de datos personales (Gil, 2017).

Para los Autores Gordillo & Restrepo (2005) existen múltiples ideas y definiciones acerca del HD, mismas que dan a conocer sobre su naturaleza jurídica en las que se denotan su configuración como derecho esencial o como garantía específica de estos. Al ser considerado como derecho, se fundamenta en aquel que asiste a toda persona identificada o identificable a solicitar judicialmente la exhibición de los registros públicos o privados en los que se incluyen sus datos personales o los de su entorno familiar, para tomar conocimiento de su exactitud o solicitar su rectificación, la eliminación de datos que han perdido su integridad o que con el pasar del tiempo se han convertido en obsoletos o a su vez, que sean objeto de

discriminación o mal uso. Por otra parte, al considerarlos como garantía, cumple dos fases: la primera que todos los ciudadanos tengan acceso a las constancias de sus archivos, ya que con esto se tiende a controlar su veracidad. La segunda parte vela por la modificación del registro cuando sus datos son erróneos o requieren de alguna actualización.

El termino Habeas Data (HD) significa "tienes tus datos". Concepto que ofrece una garantía constitucional que permite a las personas pedir explicaciones a las organizaciones gubernamentales como privadas que poseen sus datos o información concreta, la forma como han sido almacenadas y cuál es el objeto de su registro y uso (Outomuro & Mirabile, 2015).

De otro modo Bazán (2012) da a conocer el manejo del habeas data en Ecuador mencionando que la constitución de 1998, ahora ya sustituida, regulaba el HD en el artículo 94, resaltando el derecho de acceder a los documentos, bases de datos e informes sobre si misma o de sus bienes, que reposen en entidades públicas o privadas, así como de permitirle saber el uso que se hicieran de ellos y de su propósito. El titular de los datos o concernido tendrá el control total el cual tendrá el derecho de solicitar al administrador de los datos sin costo alguno el acceso, la actualización, su rectificación y el derecho al olvido, eliminación o anulación. Al hablar de HD referente a datos sensibles, este archivo deberá estar autorizado por la ley o por el titular, en las que se deberán adoptar y exigir todas las medidas de seguridad necesarias; si es que estas medidas de seguridad no se atienden, el titular podrá acudir donde un juez y demandar por los daños ocasionados.

Con los conceptos antes expuestos se entiende por habeas data como aquel derecho que otorga al propietario de los datos personales, de solicitar a los administradores de base de datos el acceso, la inclusión, exclusión, edición, adición, actualización y certificación de los mismos. En el caso de datos sensibles dichos bancos de datos deberán estar autorizados por la ley o por la persona titular en las que se exigirá las medidas de protección necesarias.

2.4.2.15 Situación Actual del Ecuador en Protección de los Datos en Relación a otros Países

En el presente epígrafe se analizará la situación del Ecuador frente a otros Países en la protección de datos personales.

Unión Europea.

La Unión Europea (UE) cuenta con el Reglamento General de Protección de Datos RGPD que entró en vigor el 25 de mayo del 2016 que es relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Cabe recalcar que este reglamento es aplicable según el Artículo. 99 desde el 25 de mayo del 2018 (General Data Protection Regulation, 2016).

Alemania

En concordancia con García (2012), Alemania cuenta con las leyes de protección de datos más severas de todo el mundo, en el que cada titular de la información brinda y autoriza que datos estará dispuesto a quien suministrarlos; cabe recalcar que por esta ley las empresas no se encuentran obligadas a proporcionar información de sus bases de datos a ninguna institución gubernamental.

Argentina

Argentina se encuentra analizando la reforma de la Ley 25.326 debido a que en Europa entro en vigor el RGPD. Entre los principales aspectos de esta ley se basa en que coloca total responsabilidad al prestador de servicios de tratamiento de datos, siendo este obligado a adoptar las medidas necesarias para que la Ley sea cumplida(Becerra, Zarate, & Gomez, 2017).

Colombia

En Colombia se considera la protección de datos como un derecho fundamental con lo cual él es importante que el estado garantice su vigilancia tanto en el sector público como privado. Además, menciona que la finalidad de lo expreso en la ley 1581 de 2012 es proteger al ciudadano como individuos, y velar por el derecho a conocer y autorizar que tipo información personal se encuentra alojada en determinada base de datos(García, 2012).

Ecuador

En el 2016 se da conocer el Proyecto de Ley de Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los datos personales de los cuales se da a conocer lo siguiente:

Artículo 1.- La presente Ley La presente tiene por objeto proteger y garantizar el derecho de todas las personas a la intimidad y privacidad en el tratamiento de los datos personales que se encuentren en base de datos o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas. Por otra parte, en el Artículo. 4 literal 6 de la Protección de los datos se indica que es la facultad que otorga Ley para que el dueño de los datos personales, decida a quién, proporciona su información, cómo y para qué. Este derecho permite acceder, rectificar, cancelar y oponerse al tratamiento de su información personal. Cabe recalcar que en el Artículo 7.- Derechos de las niñas, niños y adolescentes. Se asegurará el respeto al derecho a la intimidad de las niñas, niños y adolescentes, por lo que se prohíbe el tratamiento de sus datos personales, salvo aquellos que sean de naturaleza pública. Es deber del estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes respecto del tratamiento indebido de sus datos personales; y, proveer de conocimiento acerca del uso responsable y seguro por parte de niñas, niños y adolescentes de sus datos personales, su derecho a la intimidad y protección de su información personal a la de los demás(Asamblea Nacional del Ecuador, 2016a).

Aunque en el Ecuador la protección de los datos no ha cumplido con la madurez que debería tener, desde 1998 hasta la presente, se ha implementado derechos y obligaciones sobre el cumplimiento en el tratamiento de la información.

2.4.2.16 Definiciones de lo tratado en la Ley y RGPD

Datos Personales

En el RGPD de la Unión Europea, se define a datos personales como: "Toda información sobre una persona física identificada o inidentificable" siendo estos, por ejemplo: "un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genérica, psíquica, económica, cultural o social de dicha persona"(General Data Protection Regulation, 2016).

El Articulo 3 de la ley 1581 de octubre del 2012 de Colombia define a personal como "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales o determinables"(Colombia, 2012).

La Asamblea Nacional del Ecuador no se aleja mucho de estas definiciones debido a que trata a un dato personal como: “cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables” aquí mismo se hace constar como dato personal: “nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico , número de teléfono, numero de cedula, matricula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular”(Asamblea Nacional del Ecuador, 2016).

Datos Sensibles

Los datos sensibles son aquellos que tienen una inmediata incidencia en la privacidad o un riesgo para prácticas discriminatorias. También se considera como tales aquellas informaciones que hacen referencia a convicciones personales, así como las referentes al resto de las libertades (Sánchez, 1998).

Por su parte Drummond (2004) afirma que: los datos sensibles, son los datos relacionados con la situación patrimonial y financiera, sea del propio o de su entorno familiar, estado de salud, convicciones filosóficas o políticas, afiliación partidaria o sindical, fe religiosa, vida privada y origen racial o étnica, bien como el tratamiento de datos relativos a la vida sexual, incluyendo los datos genéticos.

Muchas aplicaciones web no protegen adecuadamente datos sensibles, tales como números de tarjetas de crédito, o credenciales de autenticación. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador (Nomura, Fukai, Hano, & Fujimoto, 1983).

Este tipo de datos requieren de un tratamiento especial para que no sean robados, secuestrados, modificados, o usados con el fin de llevar a cabo delitos informáticos. García y Stiward en el apartado VII señalan que, la debilidad más común es no cifrar los datos sensibles y cuando emplean cifrado es común detectar claves débiles, uso de algoritmos y técnicas de hash débiles. Las debilidades de los navegadores web son fáciles de descubrir por los atacantes, pero difíciles de explotar a gran escala (Garcia & Estiwar, 2013).

La Unión Europea en su Artículo 9 del RGPD menciona el tratamiento de categorías especiales de datos personales definiendo: “Quedan prohibidos el tratamiento de

datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, datos relativos a la salud o datos relativos a vida sexual o las orientaciones sexuales"(General Data Protection Regulation, 2016).

La Ley 1581 de 2012 del Gobierno de Colombia, se apega a la definición emitida por el RGPD de la UE indicando que los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede llevar a la discriminación del propietario de estos (Colombia, 2012).

En el Articulo 4.- Definiciones. Para los efectos de la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos personales se define a los datos sensibles como: todos los datos que hacen referencia a las características físicas de una persona que dan a conocer el origen racial y étnico, su ideología, filosóficas o morales, su postura frene a la política, su afinidad religiosa, datos genéticos, la información concerniente a la salud, vida sexual o cualquier dato relacionado a la información intima del titular(Asamblea Nacional del Ecuador, 2016).

De este modo se puede considera como dato sensible, a aquel que revele información que solo le pertenece a la persona o al que esta haya autorizado. Entre este conjunto de datos sensibles se pueden considerar: situación patrimonial y financiera, datos de salud, creencias religiosas, vida sexual, entre otros, que sean propios de la vida privada de las personas.

Encargado del Tratamiento de Datos

El RGPD de la UE identifica al Encargado del Tratamiento de datos como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (General Data Protection Regulation, 2016).

El encargado de los datos debe invertir en tecnologías para suministrar mecanismos de autorización, con lo que se brinde cierto tipo de garantía en cualquier momento al titular de los datos en el cual este pueda modificar y restringir el acceso de sus datos almacenados en los bancos de datos(García, 2012).

Enríquez (2017), en su publicación ejemplifica estos dos aspectos en cuanto a las funciones del encargado del tratamiento de datos: Escenario 1: si una persona decide aperturar una cuenta en una red social la cual puede ser Facebook, y Facebook los transfiere a Twitter, el segundo sería el encargado del tratamiento de datos, por otra parte, Escenario 2: si una persona A decide publicar algún contenido en Facebook datos personales de una persona B, en encargado del tratamiento viene a ser Facebook.

Tratamiento de Datos Sensibles

El proyecto de ley del Ecuador muestra una visión clara sobre el tratamiento de datos sensibles con los cuales nadie podrá a ser obligado a proporcionar datos sensibles que puedan afectar el derecho a la privacidad de las personas salvo en las siguientes circunstancias (Asamblea Nacional del Ecuador, 2016):

1. Cuando el propietario de los datos autoriza específicamente por escrito el tratamiento de su información sensible.
2. Siempre que se necesario proteger el interés vital del propietario de los datos en el caso de que este se encuentre física o jurídicamente incapacitado.
3. En el caso específico de que sus datos son de suma importancia para el reconocimiento, ejercicio o de defensa de un derecho en proceso judicial.
4. Si estos tienen una finalidad estadística, científica o académica, siempre y cuando se adopten medidas ara la supresión de la identidad de los titulares.

2.4.2.17 Sanciones tipificadas en el COIP sobre el tratamiento de datos sensibles

Aunque en el Ecuador no se encuentre en vigor la ley de protección de datos en el Código Orgánico Integral Penal (COIP) se mencionan sanciones en el caso de hacer mal uso de datos personales.

Art. 229 COIP

En la sección tercera del COIP que trata de los Delitos contra la seguridad de los activos de los sistemas de información y comunicación se detalla el artículo 229 que textualmente dice:

> "Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico,

informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermedia financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años"

En este artículo, aunque no se detalla específicamente un dato sensible se da a conocer aspectos como violación del secreto, la intimidad y la privacidad de las personas, la cual en el caso de ser una persona natural la sanción va de uno a tres años, pero en el caso de ser servidor público el que cometa este acto ilícito será sancionado con pena privativa de libertad de tres a cinco años.

2.5 Hipótesis

El modelo de gestión de la seguridad lógica de la información incide en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

2.6 Señalamiento de Variables

Variable Independiente: Modelo de seguridad lógica de la información.

Variable Dependiente: Protección de los datos sensibles de los Distritos de Educación del Ecuador.

CAPÍTULO III

METODOLOGÍA

El capítulo de metodología constituye un marco conceptual, lo cual es la clave del investigador para describir, interpretar, analizar el tema a tratar haciendo uso de los métodos idóneos con el objetivo de dar respuesta al planteamiento del problema.

3.1 Enfoque

Según Báez y Pérez el método cualitativo se adhiere a la corriente de pensamiento fenómeno-lógica cuya meta principal se basa en conocer las razones, cuestionamientos del porqué acontece lo que acontece. Por tal razón se fundamenta en lo que se observa y habla con los actores entre ellos empleados, clientes, consumidores, expertos, entre otros, de la realidad, para que con esto se explique lo que causa sus comportamientos, como se perciben los acontecimientos y que actitudes sustentan sus actos (Báez & Pérez , 2007).

El método cuantitativo se basa principalmente en la medición de las características de los fenómenos sociales, lo cual supone derivar un marco conceptual pertinente al problema analizado. Este método tiende a generalizar y normalizar resultados (Bernal Torres, 2006).

Además (Packer, 2013) da conocer la visión común de la investigación cualitativa y cuantitativa.

Tabla 5 Visión de la investigación cualitativa y cuantitativa

Investigación Cuantitativa	Investigación Cualitativa
Provee explicaciones	Provee solo descripciones
Es objetiva	Es subjetiva
Estudia las causas	Estudia experiencias
Puede poner a prueba la hipótesis	Puede solo generar la hipótesis

Fuente: (Packer, 2013).

Por tal razón el presente proyecto de investigación se basará en un enfoque cuali-cuantitativo porque se utilizarán parámetros de medición de la variable independiente en relación de la variable dependiente.

3.2 Modalidad básica de la investigación

3.2.1 Investigación Aplicada

La investigación aplicada es aquella que busca modificar una realidad presente con alguna finalidad práctica, es decir, tiende a la resolución de problemas o al desarrollo de ideas a corto o mediano plazo, dirigidas a conseguir innovaciones (Leiva, 2001).

Para Ibáñez la investigación aplicada o también llamada tecnológica depende de las nociones básicas cuyo objetivo se basa en la aplicación práctica de manera instantánea, lo que significa, que no se enfoca en desarrollar teorías o principios sino en solucionar problemas específicos (Ibáñez, 2015).

La razón por la cual se va a utilizar la investigación aplicada es porque se pretende innovar el proceso de gestión de la seguridad de la información mediante el estudio, análisis e implementación de un modelo de seguridad lógica de la información.

3.2.2 Investigación Bibliográfica

La investigación bibliográfica, es aquella que se fundamenta principalmente en datos obtenidos de distintas fuentes bibliográficas de información, entre estas figuran: libros, revistas, periódicos, entre otros documentos o escritos, que son debidamente analizados, interpretados y comentados (Aguilar, 1994).

Baena llama a este tipo de investigación como documental, la cual se basa en la búsqueda de una respuesta específica a partir de la indagación de documentos mismos que pueden ser: libros, publicaciones, impresos, folletos, sistemas de información, todo tipo de objetos entre otros (Baena, 2014).

Se utilizará la investigación bibliográfica, debido a que a este tipo de investigación se la considera como el inicio o punto de partida para realizar cualquier tipo de investigación científica. Por otra parte, la aplicación de este tipo de investigación servirá para la sustentación teórica del documento lo que lleva a obtener un conocimiento profundo de la literatura más relevante principalmente de fuentes como publicaciones de congresos, libros y revistas científicas.

3.2.3 Investigación de Campo

Es aquella que se planea, organiza y dirige para recopilar información de la realidad empírica que se estudia, utiliza sus propios procedimientos, técnicas e instrumentos

para la recolección de la información, dependiendo de las características del objeto de estudio, las hipótesis, objetivos, la disponibilidad de tiempo, personal y recursos económicos y materiales (Rojas, 2002).

En este tipo de investigación se recolecta la información fundamentándose en evidencias reales, aunque no sean útiles para validar una teoría científica, debido a que es totalmente dependiente de la subjetividad de las interpretaciones de sus actores (Landeau, 2007).

La aplicación de la investigación de campo será de gran importancia ya que su uso se basará primordialmente en recopilar información mediante el uso de instrumentos propios de este tipo de investigación aplicados en la institución que será objeto de estudio.

3.3 Nivel o tipo de investigación

3.3.1 Investigación Exploratoria

Este tipo de investigación tiene como objeto principal captar una perspectiva general de la problemática debido a que contribuye en la división de un problema macro desglosándolos en micro problemas, es decir, trata a los problemas como módulos más exactos hasta la manera como se trata la hipótesis. Sintetizando lo antes expuesto este tipo de investigación se lo suele usar para descifrar conceptos, los cuales pueden servir para: desarrollar estudios en los que intervengan algún tipo de hipótesis, instaurar características primordiales en el desarrollo de nuevas investigaciones, dejar en claro conceptos. (Namakforoosh, 2005).

Este tipo de investigación es el punto de partida en el que se define con mayor precisión el problema a analizar. El objetivo principal es suministrar al investigador lineamentos preliminares sobre la totalidad o una parte del problema (Merino, 2015).

La presente investigación se encontrará en el ámbito exploratorio debido a que se abordará los aspectos fundamentales de la problemática de un tema sin explorar, es decir, la incidencia de un modelo de seguridad lógica en la protección de los datos sensibles de los Distritos de Educación del Ecuador, para que con esto se determine los procedimientos adecuados en la investigación posterior.

3.3.2 Investigación Descriptiva

Coincidiendo con Namakforoosh, a este tipo de investigación se la considera como una manera de estudio para conocer quién, donde, cuándo, cómo y por qué del sujeto de estudio, es decir, toda la información obtenida en un estudio descriptivo, ademas este tipo de investigación da a conocer de una manera más clara a una organización: el consumidor, objetos, conceptos, y cuentas (Namakforoosh, 2005).

La investigacion descriptiva tiene como objetivo describir una situación presente considerada como un nivel basico de investigación, se guía por las preguntas de investigacion que el investigador formula cuando plantea su hipótesis y se basa en tecnicas e instrumentos como la encuesta, la entrevista, la observación y la revisión documental. Entre los principales temas de investigación que trata se tiene: Estudios de carácter diagnóstico, diseño de (guías, modelos, productos prototipos, etc), estudios de mercado, estudios de tiempos y movimientos (Bernal Torres, 2006).

La aplicación de la investigación descriptiva será de suma importancia debido a que se tendrá que utilizar el método del análisis para observar el tratamiento de la información y principalmente de los datos sensibles del Distrito de Educación en estudio, para que de esta manera ordenar, agrupar o sistematizar los objetos involucrados en la incidencia del modelo de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación.

3.3.3 Explicativa

Por medio de este tipo de investigación se plantean los orígenes del fenómeno físico o social que ha sido objeto de estudio. Su principal objetivo es determinar cómo suceden la mayor parte de sucesos, a través de la delimitación de las relaciones causales existes o de las condiciones que en ella se produce (Ospino, 2004).

En concordancia con García, la investigación explicativa se encarga de buscar el porqué de los causales de un fenómeno por medio del establecimiento de la relación que existe entre la casusa-efecto (García P. , 2006).

Valiéndose del método analítico sintético la investigación explicativa aportará al autor del presente documento de investigación ir de lo general a lo particular sea en objetos de estudio, fuentes bibliográficas y verificación de la hipótesis planteada.

3.3.4 Investigación Correlacional

Esta investigación es la que tiene mayor probabilidad de responder a preguntas que existen acerca de la relación que existe entre variables o sucesos. Dicho de otra forma, proporciona indicios de relación que pueden existir entre dos o más cosas, pero de ninguna manera implica que una es la causante de otra (Salkind, 1999).

Al aplicarse un estudio correlacional se llega a determinar si dos variables se encuentran correlacionadas o no. Lo que significa que se podría analizar si existe un aumento o disminución en una variable coincide con el aumento o disminución en otra variable (Siddharth Kalla, 2010).

Cumple con el propósito de establecer la relación existente entre las variables independiente y dependiente del presente estudio, es decir, la relación que se encuentra entre el modelo de seguridad lógica de la información y la protección de los datos sensibles.

3.4 Población y Muestra

3.4.1 Población

Para el desarrollo del presente proyecto de investigación se trabajará con la población conformada por los funcionarios de la institución especificados en la Tabla 6, debido a que serán los que serán objeto de estudio en el tratamiento de la información. La aplicación de la investigación se enfocará en los funcionarios del Distrito de Educación 23D01 de Santo Domingo de los Tsáchilas siendo estos los principales actores del objeto de estudio a los cuáles se les aplicará en distintas formas el uso del modelo de seguridad lógica de la información verificar su incidencia en la protección de los datos sensibles de los distritos de educación.

Tabla 6 Población de estudio

N°	SERVIDORES PÚBLICOS RESPONSABLES DE LAS UNIDADES DE LA DIRECCIÓN DISTRITAL 23D01EDUCACIÓN SANTO DOMINGO DE LOS TSÁCHILAS	CANT.
1	Director Distrital	1
2	Unidad Atención Ciudadana	1
3	Unidad de Apoyo Seguimiento y Regulación	1

4	UDAI	1
5	DECE	1
6	Unidad de Talento Humano	1
7	Unidad de Planificación	1
8	Unidad de Tecnología de la Información	1
9	Unidad de Administración Escolar	1
10	Unidad de Gestión de Riesgos	1
11	Unidad de Asesoría Jurídica	1
12	Unidad Administrativo Financiero	1
13	Unidad Financiera	1
	TOTAL:	**13**

Elaborado por: Vaca P. (2018)

3.4.2 Muestra

Debido a la población especificada en la Tabla 6 Población de estudio, de las personas responsables de cada una de las Unidades administrativas del Distrito de Educación 23D01 no se realizará un cálculo de la determinación de la muestra, ya que la información que se pretende recopilar es accesible al investigador.

3.5 Operacionalización de Variables

3.5.1 Variable Independiente:

Tabla 7 Variable Independiente: Modelo de gestión de seguridad lógica de la información.

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Un modelo de gestión de seguridad lógica de la información se considera como un esquema o marco de trabajo en el que se incorpora un conjunto de características, atributos, indicadores o patrones que proporciona un punto de referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos con los cuales se puedan cumplir con objetivos y prioridades.	Organización. Modelo de seguridad informática Capacidades referentes a la seguridad informática. Procesos. Métodos.	- Nivel de Confidencialidad - Nivel de Integridad - Nivel de Disponibilidad. - Aceptación.	- ¿Cuál de los modelos de seguridad informática es adaptable en los distritos de educación? - ¿Qué se está haciendo en cuanto a la protección de la seguridad lógica de la información? - ¿Tiene la organización buenas prácticas de seguridad de la información? - ¿Culturalmente es aceptado por parte de los funcionarios de la organización? - ¿Información accesible y veraz? - ¿Se ven reflejados los resultados con la implementación de un modelo de gestión de la seguridad información?	- Encuesta con Cuestionario - Entrevista con Cuestionario - Experimental

Elaborado por: Vaca P. (2018)

3.5.2 Variable Dependiente:

Tabla 8 Variable Dependiente: Protección de los datos sensibles de los Distritos de Educación del Ecuador.

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
La protección de datos hace referencia al proceso de salvaguardar la información tanto en la integridad y confiabilidad de los mismos, así como de garantizar la continuidad del negocio ante cualquier ataque sea este accidental o provocado, en las que se incluya a todo el personal que labora en una organización.	- Seguridad Informática. - Salvaguardar la información. - Continuidad de negocio. - Calidad de la información. - Nivel cultural y formativo del personal en temas de protección de datos	- Métricas de seguridad de la información. - Métricas de continuidad de negocio. - Métricas de la calidad de la información. - Porcentaje de Cultura organizacional.	- ¿Cuál es el proceso óptimo para la protección de los datos sensibles de la entidad? - Cambio de la cultura organizacional en Seguridad Informática. - Número de políticas implementadas para la protección de la información. - Tiempo de reposición ante un ataque informático.	Encuesta con Cuestionario Entrevista con guía Experimental

Elaborado por: Vaca P. (2018)

3.6 Recolección de Información

En el proceso de recolección de información se utilizará instrumentos tales como: fichas bibliográficas, fichas de trabajo, entrevistas y cuestionarios que serán elaborados con preguntas objetivas mediante el diseño de preguntas cerradas como se lo puede visualizar en la siguiente tabla:

Tabla 9 Recolección de la Información

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Funcionarios del Distrito de Educación.
¿Sobre qué aspectos?	Seguridad de la información. Datos Sensibles. Impacto del uso de un modelo de seguridad de la información.
¿Quién, Quiénes?	Investigador: Ing. Patricio Neptali Vaca Escobar.
¿Cuándo?	Cuarto trimestre del 2018 y primer trimestre del 2019
¿Dónde?	Distrito de Educación 23D01.
¿Cuántas veces?	Una para la recolección de información para la investigación.
¿Qué técnicas de recolección?	Encuesta Entrevista Datos Estadísticos
¿Con qué?	Cuestionario Cuestionario Inspecciones
¿En qué situación?	Dentro del horario de trabajo con profesionalismo investigativo y absoluta confidencialidad y reserva.

Elaborado por: Vaca P. (2018)

3.7 Procesamiento y Análisis

- Revisión crítica de la información recogida; es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente y otras fallas.
- Repetición de la recolección, en ciertos casos individuales para corregir errores de contestación.
- Tabulación o cuadros variables de la hipótesis y objetivos.
- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en los análisis).
- Estudio estadístico de datos para presentación de resultados.

3.7.1 Análisis de Resultados

- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados con apoyo del marco teórico en el aspecto pertinente.
- Comprobación de hipótesis para la verificación estadística.
- Establecimiento de conclusiones y recomendaciones.

CAPITULO IV

ANALISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de Resultados

En la actualidad los Distritos de Educación del Ecuador se ven vulnerados ante distintos ataques o delitos informáticos. Estos ataques pueden ser provocados directa e indirectamente por parte de los funcionarios por desconocimiento de mecanismos o técnicas básicas de mitigación de riesgos informáticos.

El análisis de resultados se lo dividió en dos etapas, la primera en la que se aplica pruebas de pentesting, auditoria informática, recogida de información a través de técnicas de hacking ético y la segunda etapa consiste en la aplicación de una encuesta dirigida a los servidores públicos con cargo de jefe de cada una de las unidades administrativas de la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo.

4.1.1 Primera etapa de recolección de datos.

En esta primera etapa se realizaron pruebas de pentisting utilizando una máquina virtual corriendo el sistema operativo Kali Linux de las siguientes pruebas de hacking ético:

- **Ataque de Phishing**: Identificación de usuarios que acceden a sitios web sin verificación alguna.
- **Ataque crimeware:** Identificación de usuarios que instalan aplicaciones sin comprobar y que pueden tener dentro de su estructura código malicioso tal como: keyloggers.

4.1.1.1 Primer Ataque: Identificación de como los funcionarios actúan ante un ataque de phishing sitio web clonado MOGAC (Módulo de atención ciudadana).

Esta prueba se lo realizó utilizando la herramienta SET (The Social-Enginner Toolkit), la cual se la configuró de la siguiente manera:

- ✓ Se accede por medio del comando **setoolkit** la terminal de Kali.
- ✓ Se selecciona las opciones 1) Social-Engineering Attaks, 2) Website Attak Vector, 3) Credential Harvester Attak Method.

- ✓ Al seleccionar este método de ataque, se procede a seleccionar la opción 2) Site Cloner.
- ✓ Acto seguido solicitará que se ingrese una dirección ip la cual será a donde regresen las credenciales de los funcionarios que caigan en este ataque.
- ✓ De la misma manera en el proceso de configuración, se le solicitará que se ingrese la dirección url del sitio al cual se pretende clonar que para este caso será: http://atencionciudadana.educacion.gob.ec/, como se observa en la siguiente figura .

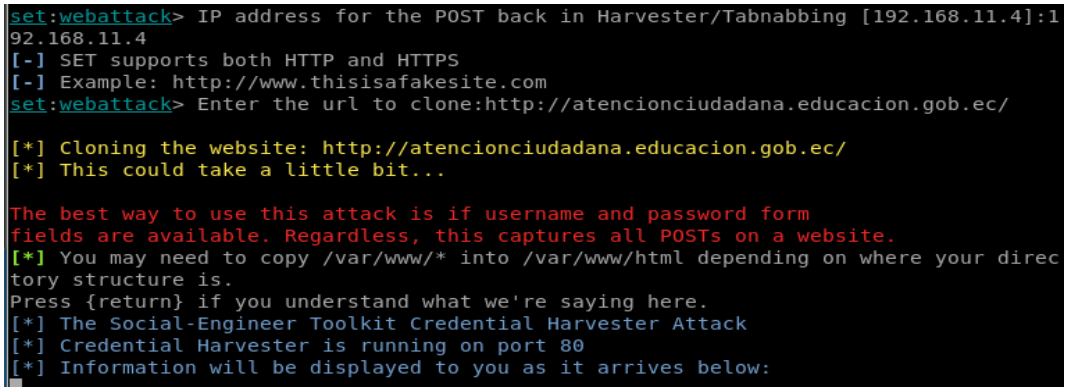


Figura 13 Configuración de la herramienta SET en la clonación del sitio web Mogac.

Elaborado por: Vaca P. (2019)

Una vez ya configurada la herramienta, se procederá a enviar a cada uno de los usuarios de estos servicios, misma que tendrá una interfaz como se la muestra en la siguiente figura:

Figura 14 Sitio web MOGAC clonado.

Elaborado por: Vaca P. (2019)

Como se observa en la figura anterior la interfaz gráfica del módulo de gestión ciudadana es similar al original, diferenciándose por un único e importante factor

que es la identificación de la dirección url, pese a que en la actualidad se realizan campañas de prevención ante ataques de phishing y clonando otros sitios utilizados por el personal operativo y administrativo se obtuvieron los siguientes resultados: Ante este primer ataque y como sustento a la verificación de la hipostesis surge la siguiente interrogante: ¿El personal de la DD23D01 Educación de la ciudad de Santo Domingo reconoce cuando está siendo atacado por una técnica de phishing?, en base a esta pregunta para los ataques fallidos se lo ha considerado que el funcionario "Si" sabe cómo identificarlo, además para los ataques satisfactorios denota que el servidor público "No" reconoce un ataque informático. En la siguiente tabla se muestran los resultados.

Tabla 10 ¿El personal de la DD23D01 Educación de la ciudad de Santo Domingo reconoce cuando está siendo atacado por una técnica de phishing?,

Respuesta	Frecuencia	Porcentaje
SI	2	15,38%
NO	11	84,62%
SUMAN	**13**	**100%**

Elaborado por: *Vaca, P (2019)*

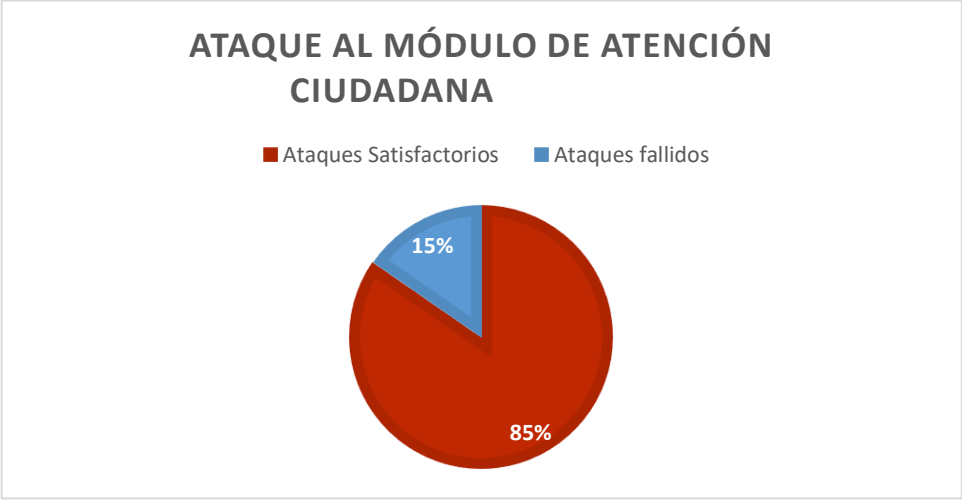


Figura 15 Ataque al módulo de atención ciudadana MOGAC.

Análisis de Resultados: Como se observa en la figura de los 13 ataques realizados a los funcionarios 11 de ellos que corresponden al 84,62% fueron satisfactorios y tan solo 2 de ellos representando el 15,38% fueron fallidos.

Interpretación: En la gráfica se observa que el 85% de los jefes de unidad administrativa no conocen como actuar ante un ataque de phishing, es decir, que acceden a cualquier url sin previa verificación, cabe recalcar que en la actualidad existen técnicas en las cuales se logra clonar sitios web ocultando las direcciones ip y cambiándolas por dominios similares al de sitio web del que ha sido clonado. Esto también da a conocer la falta de cultura de seguridad informática de los usuarios, que por un simple error de validación de urls, puede dejar expuestos datos de carácter sensible de cualquier organización.

4.1.1.2 Segundo ataque: Identificación de usuarios que instalan aplicaciones sin comprobar y que pueden tener dentro de su estructura código malicioso tal como: keyloggers.

Los crimeware por lo general instalan keylogger dentro de las maquinas victimas con el objetivo de substraerse credenciales de logueo, con lo cual los atacantes pueden hacerse de los sistemas de información desencadenando en la vulneración de datos personales y entro ellos los de carácter sensible.

Para este segundo ataque se creará un keylogger en Kali Linux y se lo enviará a los jefes de unidad para comprobar el comportamiento que tienen ante este tipo de ficheros.

Se utilizará la herramienta **sAINT** para crear el malware que será enviado vía correo electrónico aplicando técnicas de ingeniería social, para que la persona a la cual le llegue el mensaje no le quede espacio a la duda. Para configurarlo se detallan los siguientes pasos:

- ✓ El programa sAINT necesita de dependencias como Maven y JDK8 para ser instalado.

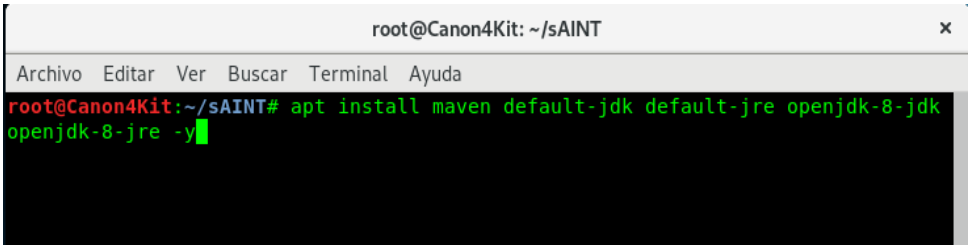


Figura 16 Instalación de dependencias maven y jdk8 para Saint

Elaborado por: Vaca P. (2019)

- ✓ Aunque el aplicativo por naturaleza deja un archivo .jar lo cual permite ejecutar en la mayoría de computadores de la Dirección Distrital, se instalará las siguientes dependencias con lo que permitirá generar ficheros .EXE.

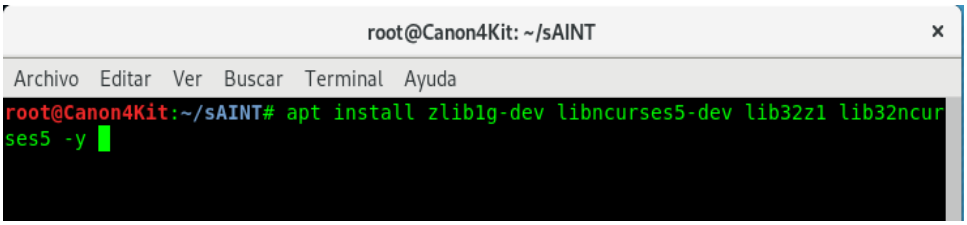


Figura 17 Dependencias zliblg-dev libncurses5-dev lib32zl lib32ncurses -y para la generación de ficheros .EXE

Elaborado por: Vaca P. (2019)

- ✓ El proyecto se encuentra alojado en GIT y por esta razón basta con ejecutar el comando git clone con la dirección de alojamiento para proceder a la descarga.

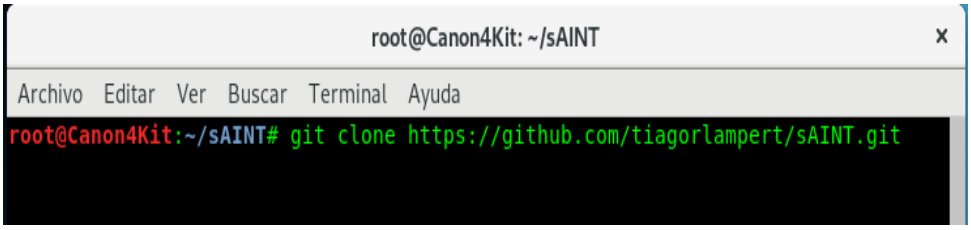


Figura 18 Proceso de clonación del proyecto sAINT

Elaborado por: Vaca P. (2019)

- ✓ Una vez clonado el directorio sAINT se le da permisos de ejecución al fichero configure.sh para la configuración de librerias.

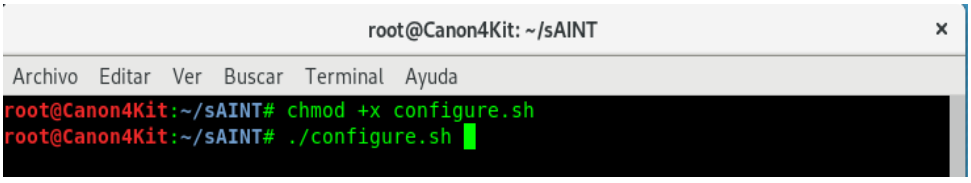


Figura 19 Permisos de ejecución y configuración del fichero configure.sh de sAINT

Elaborado por: Vaca P. (2019)

- ✓ Para ejecutar el software se lo hace mediante el comando java -jar sAINT.jar

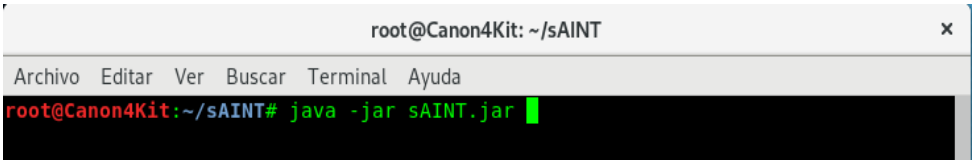


Figura 20 Ejecución del lanzador de sAINT.

Elaborado por: Vaca P. (2019)

✓ El siguiente paso a realizar es configurar el malware con las credenciales del usuario atacante como se muestra en la siguiente ilustración

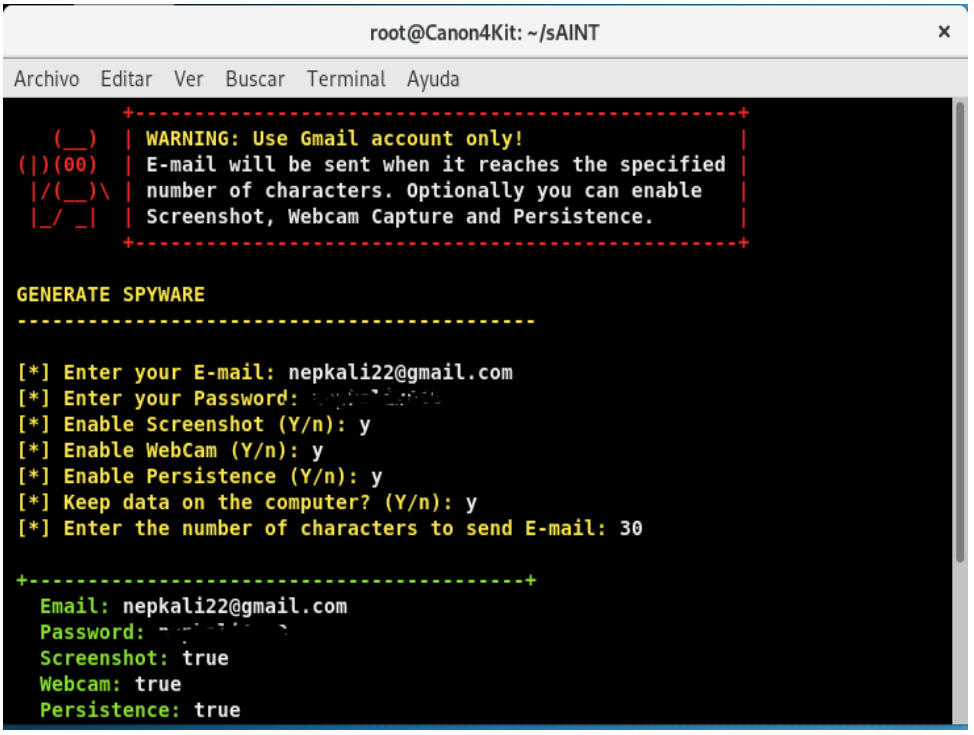


Figura 21 Configuración de las credenciales y parámetros básicos del malware.

Elaborado por: Vaca P. (2019)

✓ El software enviara una notificación en la que debe permitir el acceso de apps menos seguras en el correo electrónico Gmail.

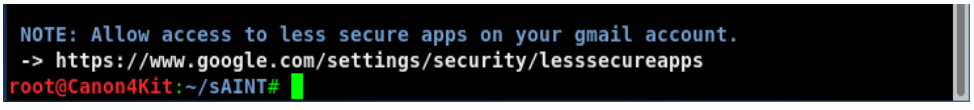


Figura 22 Notificación para habilitar el acceso de apps menos seguras en Gmail

Elaborado por: Vaca P. (2019)

- ✓ El aplicativo generará dos archivos dentro del subdirectorio target de sAINT con extensiones .exe y jar

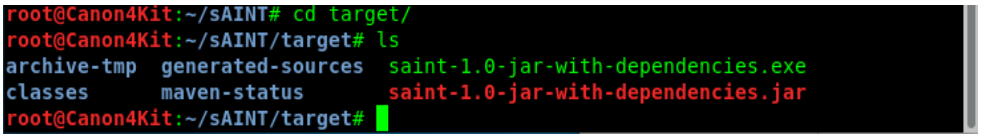


Figura 23 Ficheros generados por sAINT

Elaborado por: Vaca P. (2019)

- ✓ Se realizará el proceso de empaquetado en zip y estructura de uno de los sistemas de gestión escolar utilizado por la Dirección Distrital Educación 23D01, como se detalla en la siguiente ilustración:

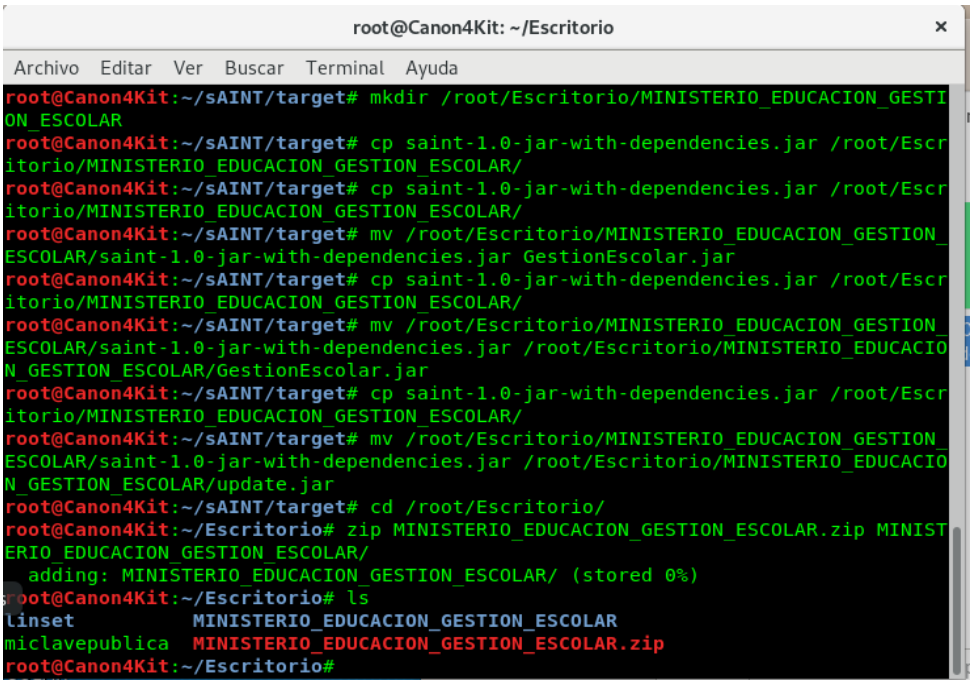


Figura 24 Empaquetado zip de los ficheros con contenido malware.

Elaborado por: Vaca P. (2019)

- ✓ Una vez descargado el fichero .zip por la victima basta con solo ejecutarlo para que se empiecen a recopilar un conjunto de 50 palabras mismas que serán enviadas al correo configurado para este caso. Cabe recalcar que el keylogger tiene la propiedad de capturar screenshot, capturar imágenes de la webcam y por supuesto enviar cada movimiento realizado en teclado.

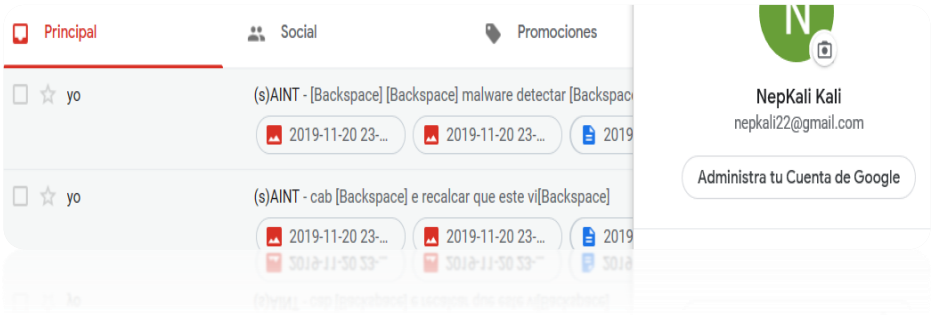


Figura 25 Ficheros que llegan al correo configurado desde los computadores infectados.

Elaborado por: Vaca P. (2019)

✓ Es destacable que este tipo de malware a la fecha de este documento de investigación es prácticamente indetectable por los antimalware. Aunque se recomienda si es el caso, de que un computador se vea comprometido por este tipo de malware borrar el directorio que se crea dentro de %appdata% llamado saint.

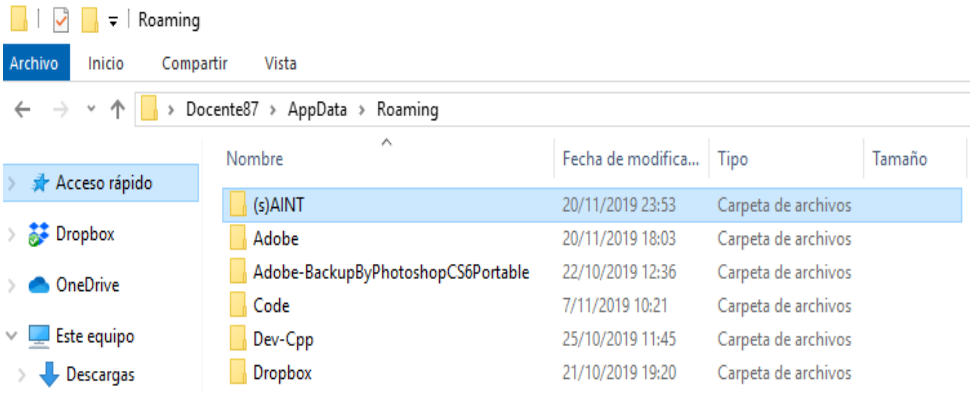


Figura 26 Fichero a eliminar generado por el virus Saint

Elaborado por: Vaca P. (2019)

✓ Es recomendable también verificar si es que algún tipo de archivo con extensión .jar contiene código malicioso, una de las soluciones es pasar el fichero en https://www.virustotal.com que se encarga de analizar las ingenieras malware inmersas en el fichero.

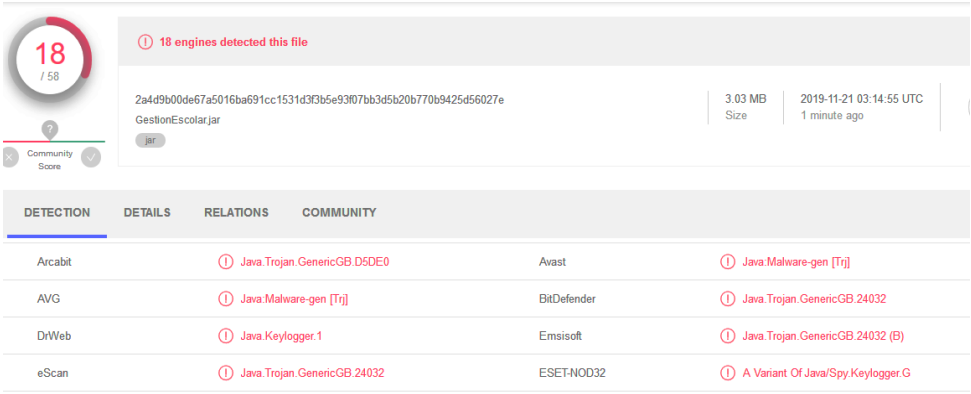


Figura 27 Análisis del fichero infectado en el sitio web de virus total

Elaborado por: Vaca P. (2019)

- ✓ En el caso de que un fichero no se encuentre con código malicioso, virus total emitirá un reporte de fichero totalmente libre de malware.

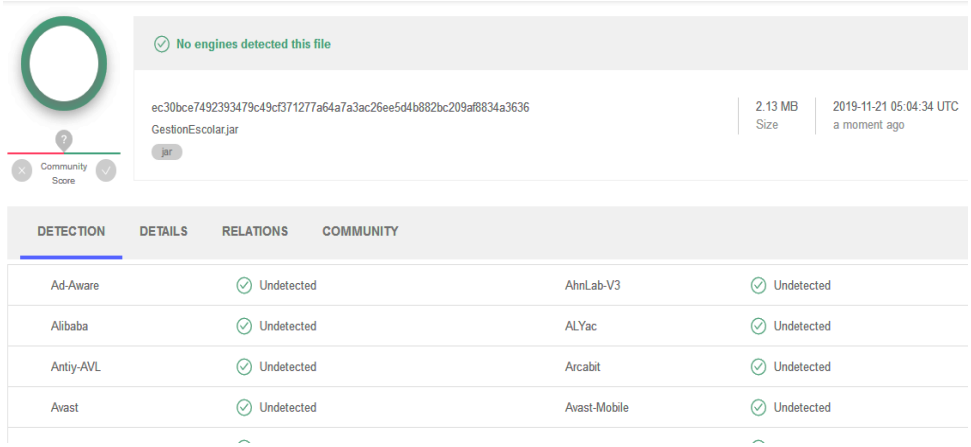


Figura 28 Análisis del fichero original y sin malware.

Elaborado por: Vaca P. (2019)

De la misma manera que en la pregunta anterior ante esta prueba de pentesting surge la siguiente interrogante: ¿El funcionario de la DD23D01 Educación de la ciudad de Santo Domingo identifica si un fichero contiene código malicioso antes de proceder a instalarlo?

En este segundo ataque se envió el contenido del archivo MINISTERIO_EDUCACION_GESTION_ESCOLAR.zip obteniendo los siguientes resultados:

Tabla 11 ¿El funcionario de la DD23D01 Educación de la ciudad de Santo Domingo identifica si un fichero contiene código malicioso antes de proceder a instalarlo?

Respuesta	Frecuencia	Porcentaje
SI	1	7,69%
NO	12	92,31%
SUMAN	**13**	**100%**

Elaborado por: *Vaca, P (2019)*

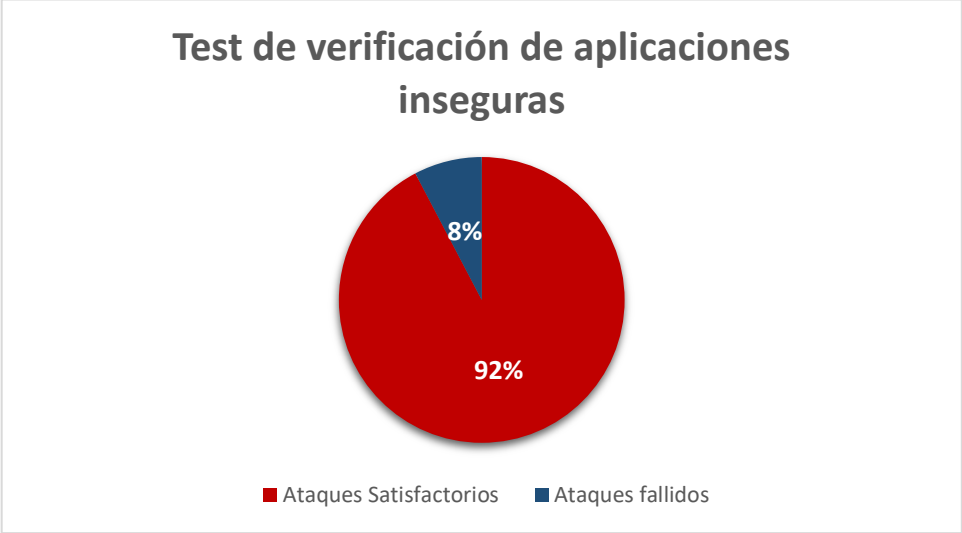


Figura 29 Test de verificación de instalación de aplicaciones seguras.

Elaborado por: *Vaca, P (2019)*

Análisis de resultados: De los 13 funcionarios a los que se les envió el archivo 12 de ellos correspondiente al 92,31% ejecutaron el aplicativo sin ninguna restricción y tan solo uno de ellos que corresponde al 7,69% se negó a ejecutarlo en el computador al que es custodio.

Interpretación: Este ataque se lo realizó aplicando ingeniería social a los jefes de unidad indicándoles que es un programa de actualización del aplicativo de Gestión Escolar, y del cuál tenían que realizar este proceso para el correcto funcionamiento de los sistemas de información. Con estos datos obtenidos se ve reflejado que los funcionarios ejecutan cualquier aplicativo en sus computadores, sin antes realizar una validación de los mismos comprobando si es que tienen algún tipo de malware.

4.1.1.3 Identificación de riesgos sobre respuestas técnicas de los jefes de unidad de los departamentos ante ataques informáticos.

Luego de haber realizado las dos pruebas de pentesting a los jefes de unidad para saber cómo responden técnicamente ante estos tipos de ataques en los cuales los delincuentes informáticos buscan obtener credenciales de acceso para hacerse de la información de una organización, se aplicará una metodología de análisis y gestión de riesgos de tecnologías de la información (MAGERIT).

MAGERIT, se la define como una metodología que abarca una de las fases fundamentales en un sistema de gestión de seguridad de la información basándose en el análisis de gestión de riesgos (Moliner, 2005).

Por su parte esta metodología detalla una escala de impacto según el riesgo que pueda producir una amenaza en la organización:

Tabla 12 Nivel de impacto MAGERIT

Nivel de impacto	Porcentaje
Bajo	0% - 25%
Intermedio	26% - 50%
Alto	51% - 75%
Muy Alto	>76%

Elaborado por: *Vaca, P (2019)*
Fuente: (Hurtado, 2017)

En el presente documento de investigación y específicamente para el análisis de los riesgos encontrados a partir de las técnicas de pentesting que resultaron como satisfactorios en las pruebas de respuesta técnicas aplicadas se tiene:

- Vulnerabilidad = Porcentaje de usuarios afectados en técnicas de phishing.
- Vulnerabilidad = Porcentaje de usuarios que instalan aplicaciones con código malicioso, sin validación y autorización.

Tabla 13 Interpretación según MAGERIT de ataques phishing

Ataque	% de usuarios afectados	Vulnerabilidad
Phishing	84,62%	84,62%

Elaborado por: *Vaca, P (2019)*

Tabla 14 Cálculo de usuarios que instalan aplicaciones con código malicioso, sin validación y autorización.

Ataque	% de usuarios afectados	Vulnerabilidad
Keylogger	92,31%	92,31%

Elaborado por: *Vaca, P (2019)*

La metodología aplicada para el análisis de riesgos en la presente investigación, proporciona ponderaciones con escalas que van desde la visualización de información, pasando por la recopilación de información, hasta llegar a la desactivación de servicios.

Tabla 15 Ponderación de amenazas informáticas según MAGERIT

Amenaza	Porcentaje
View Information (VI)	0.33
Information Gathering (IG)	0.66
Disable Services (DS)	0.99

Elaborado por: *Vaca, P (2019)*
Fuente: (Hurtado, 2017)

Por su parte MAGERIT, indica las dimensiones de afectación en aspectos de seguridad de la información basándose en la triada CID.

Tabla 16 Dimensiones de afectación de la seguridad de la información

Ataque	Dimensión		
	Integridad	Confidencialidad	Disponibilidad
Phishing	x	x	x
Keylogger	x	x	x

Elaborado por: *Vaca, P (2019)*

Una vez obtenido los datos de usuarios afectados en ataques de phishing y keyloggers satisfactorios y contando con las ponderaciones y dimensiones en

aspectos de seguridad informática se procederá calcular el riesgo que estos ataques implican para la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo mediante la siguiente formula:

$$Riesgo = Amenaza\ x\ Vulenerabilidad$$

Tabla 17 Cálculo del riesgo

Amenaza	Escala amenaza	Vulnerabilidad	Impacto	Riesgo
Phishing	VI 0.33	84,62%	Alto	27,9%
Phishing	IG 0.66	84,62%	Alto	55,84%
Phishing	DS 0.99	84,62%	Alto	83,77%
Keyloggers	VI 0.33	92,31%	Alto	30,46%
Keyloggers	IG 0.66	92,31%	Alto	60,92%
Keyloggers	DS 0.99	92,31%	Alto	91,39%

Elaborado por: *Vaca, P (2019)*

4.1.2 Segunda etapa de recolección de datos aplicación de encuesta.

El objetivo de esta etapa es recolectar datos que permitan al investigador del presente documento tener una visión más clara de cuál es la situación actual de los funcionarios en cuanto a su cultura informática, manejo y administración de datos sensibles, y la manera en cómo se los están protegiendo desde lo estipulado en la constitución de la República del Ecuador, así como del anteproyecto de manejo de datos sensibles presentado por la DINARDAP. La presente encuesta consta de un total de 24 preguntas que fueron realizadas a los jefes de los distintos departamentos de la Dirección Distrital Educación 23D01.

Pregunta 1: ¿Conoce cuáles son los Datos Sensibles que se manejan en la Institución?

Tabla 18 Manejo de datos Sensibles

RESPUESTA	FRECUENCIA	PORCENTAJE
SÍ	6	46,2%
NO	7	53,8%
SUMAN	**13**	**100%**

Elaborado por: *Vaca, P (2019)*

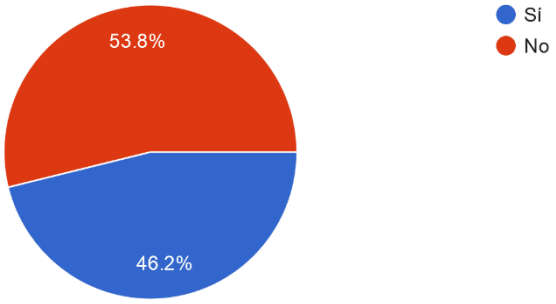


Figura 30 Manejo de datos Sensibles

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: La gran parte de los jefes de unidades encuestados manifestaron no conocer cuáles son los datos sensibles que se manejan en la institución lo que corresponde al 53,8%, no obstante, el 46,2% respondieron que si los conocen.

Interpretación: De un total de 13 personas encuestadas, 6 respondieron que si conocen sobre el manejo de datos sensibles y 7 que desconocen sobre el tratamiento de datos sensibles del Distrito de Educación 23D01. Al existir una brecha tan pequeña se puede concluir que quizá conocen cuales son los datos sensibles, pero de una manera genérica.

2. ¿Existen políticas institucionales de seguridad establecidas para el manejo de datos sensibles?

Tabla 19 Políticas de seguridad en el manejo de datos sensibles

RESPUESTA	FRECUENCIA	PORCENTAJE
SÍ	7	53,8%
NO	6	46,2%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

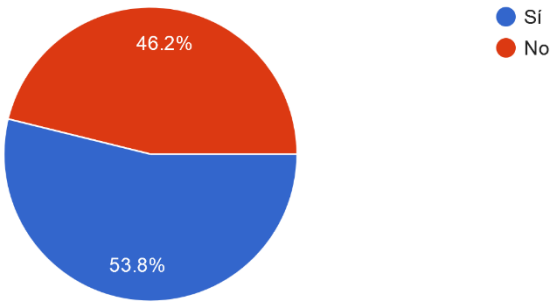


Figura 31 Políticas de seguridad en el manejo de datos sensibles

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Como se observa en la figura anterior, el 53,2% afirma que existen políticas de seguridad en el manejo de datos sensibles, de otro modo el 46,2% menciona que no existen dichas políticas.

Interpretación: De un total de 13 personas encuestadas, 7 de ellas respondieron que si existen políticas de seguridad para el manejo de datos sensibles y los 6 restantes mencionaron que no existen estas políticas, es decir, que estas políticas pueden ser aplicadas o cumplidas por ciertos departamentos o unidades funcionales y el resto no las aplican.

3. ¿La institución cuenta con procedimientos estandarizados sobre los lineamientos en el manejo de datos sensibles?

Tabla 20 Lineamientos en el manejo de datos sensibles

RESPUESTA	FRECUENCIA	PORCENTAJE
SÍ	6	46,2%
NO	7	53,8%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

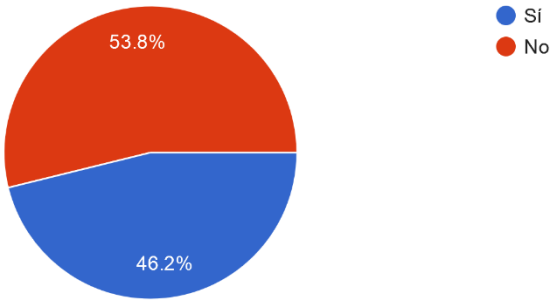


Figura 32 Lineamientos en el manejo de datos sensibles

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: La mayoría de los funcionarios encuestados aseguraron no conocer sobre lineamientos en el manejo de datos sensibles lo que corresponden a un 53,8% a diferencia del 46,2% que afirmaron si conocer.

Interpretación: Del total de responsables de departamento encuestados, 7 de ellos respondieron que la institución no cuenta con lineamientos estandarizados para el manejo de datos sensibles, lo que puede ocasionar que en uno o varios de los departamentos exista fuga de información, en los que se puedan ver afectados datos personales tanto de los funcionarios, estudiantes, de los mismos padres de familia, entre otros.

4. ¿Conoce si en la institución manejan un modelo para el tratamiento de datos sensibles?

Tabla 21 Resultados Manejo de modelo en el Distrito de Educación 23D01

RESPUESTA	FRECUENCIA	PORCENTAJE
SÍ	3	23,1%
NO	10	76,9%
SUMAN	**13**	**100%**

Elaborado por: *Vaca, P (2019)*

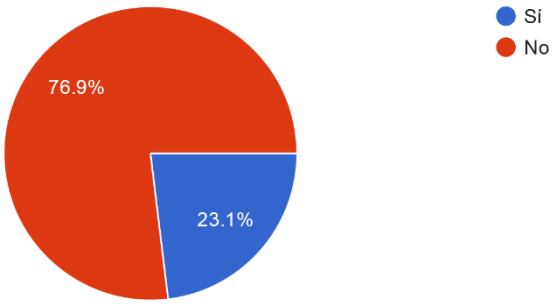


Figura 33 Resultados Manejo de modelo en el Distrito de Educación 23D01

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Del grupo de servidores públicos encuestados mediante la aplicación de esta pregunta el 76,9% dieron a conocer que el Distrito de Educación 23D01 no manejan un modelo a seguir para el tratamiento de datos sensibles.

Interpretación: La aplicación de esta pregunta permite observar que 10 de los 13 jefes departamentales no cuentan con un modelo a seguir para el manejo de datos sensibles, por tal razón la información confidencial se encuentra expuesta y puede ser interceptada para el uso con fines maliciosos.

5. ¿Al enviar datos sensibles a través del navegador, revisa si la dirección URL tiene una conexión segura, talvez usa un protocolo seguro como https?

Tabla 22 Resultados: Verificación conexión segura

RESPUESTA	FRECUENCIA	PORCENTAJE
SÍ	2	15,40%
NO	11	84,60%
SUMAN	**13**	**100%**

Elaborado por: *Vaca, P (2019)*

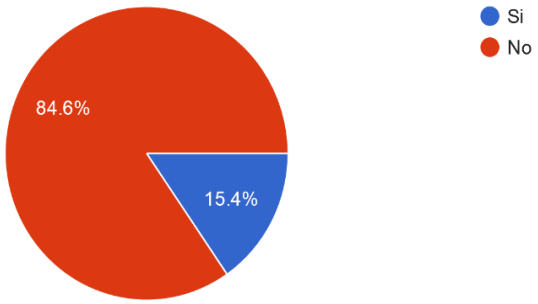


Figura 34 Resultados: Verificación conexión segura

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: El gráfico anterior de los resultados de si los usuarios de DD23D01 Educación realizan una validación si una conexión es segura, evidencia que tan solo el 15,4% revisan si la dirección URL tiene una conexión segura en el envío de información, frente al 84,6% que no lo hace.

Interpretación: El mayor porcentaje de responsables de departamentos no le toman mucha atención al uso de protocolos de comunicación seguros tales como https, sino que exponen la información entre ella los datos sensibles.

6. ¿En la institución hacen uso de herramientas seguras para subir, transmitir y generar información en los que intervengan datos sensibles?

Tabla 23 Resultados: Uso de Herramientas seguras.

RESPUESTA	FRECUENCIA	PORCENTAJE
SÍ	3	23,10%
NO	10	76,90%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

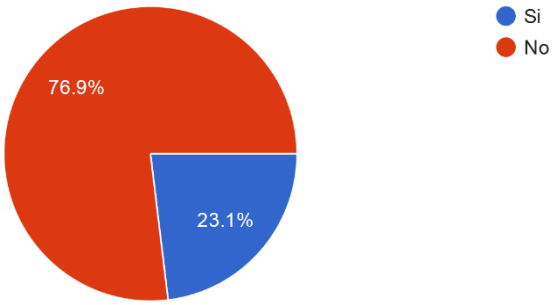


Figura 35 Resultados: Uso de Herramientas seguras.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Del total de los encuestados, el 76,9% indican que no utilizan herramientas seguras, mientras que el 23,1% que aseguran si utilizarlas.

Interpretación: Los resultados de esta encuesta demuestran que no existen herramientas estandarizadas para la transmisión, carga, y generación de información en los que intervengan datos sensibles.

7. ¿Conoce quién es el responsable del tratamiento de los datos sensibles en el Distrito de Educación 23D01?

Tabla 24 Resultados: responsable del tratamiento de los datos sensibles

RESPUESTA	FRECUENCIA	PORCENTAJE
Director de Sistemas	4	30,8%
Director de RRHH	0	0%
Oficial de la seguridad de la información	2	15,3%
No existe responsable	4	30,8%
No sé	3	23,1%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

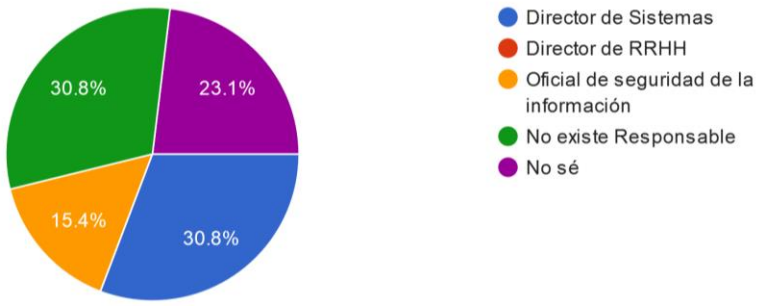


Figura 36 Responsable del tratamiento de los datos sensibles

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Se preguntó a los encuestados acerca del responsable del tratamiento de los datos sensibles, los resultados obtenidos estuvieron divididos con un 30.8% para el "Director de Sistemas", con la misma escala porcentual manifestaron que "No existe responsable", de otro modo el 23,1% mencionaron "No saber" y el 15,4% que corresponde a un total de 2 jefes departamentales indicaron que esta responsabilidad recae sobre un "oficial de seguridad de la información".

Interpretación: Con la aplicación de esta pregunta se nota claramente que no existe un oficial de la seguridad de la información, debido a que existe dispersión en las respuestas obtenidas.

8. ¿El responsable de la protección de datos está dedicado a tiempo completo?

Tabla 25 Resultados: Tiempo que dedica el responsable de la protección de datos.

RESPUESTA	FRECUENCIA	PORCENTAJE
No	3	23,1%
Sí	1	7,7%
No sé	4	30,8%
No existe responsable	5	38,5%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

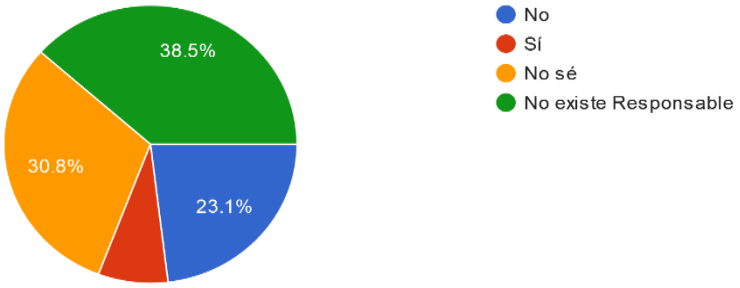


Figura 37 Tiempo que dedica el responsable de la protección de datos.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Con base al gráfico anterior el 38,5% respondieron que "No existe responsable, el 30,8% "No sé", por su parte el 23.1% indicaron que "No" existe responsable a tiempo completo y el 7,7% que corresponde a un responsable de departamento respondió que "Si".

Interpretación: Según los resultados obtenidos en esta pregunta demuestran que en los Distritos de Educación no existe un responsable de la protección de los datos debido a la correlación de las opciones.

9. ¿En la actualidad, El Distrito de Educación 23D01 cuenta con una medida o plan para la protección de datos sensibles?

Tabla 26 Resultados: Medida o plan de protección de datos sensibles.

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	4	30,8%
No, pero estamos en proceso	1	7,7%
No	3	23,1%
No sé	5	38,5%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

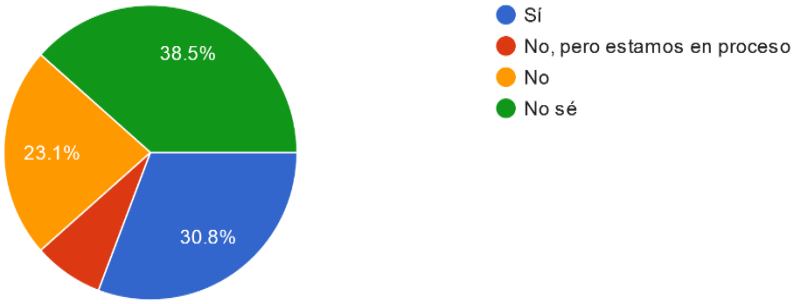


Figura 38 Medida o plan de protección de datos sensibles.

Elaborado por: *Vaca, P (2019)*

Análisis de Resultados: Tomando como referencia la figura 38, el 38,5% de los encuestados han manifestado que no saben de la existencia de un plan o medida de datos sensibles, sin embargo el 30,8% indican que "Si" cuentan con este plan, pero el 23,1% responden que "No" y el 7,7% responden que "No, pero estamos en proceso".

Interpretación: Mediante la aplicación de esta encuesta se logra determinar que el Distrito de Educación no cuenta con una medida o plan de protección de los datos sensibles.

10. ¿El Distrito de Educación 23D01 cuenta con información clasificada en datos personales, sensibles, financieros/patrimoniales?

Tabla 27 Información clasificada de datos personales, sensibles, financieros/patrimoniales

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	4	30,8%
No, pero estamos en proceso	0	0%
No	3	23,1%
No sé	6	46,2%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

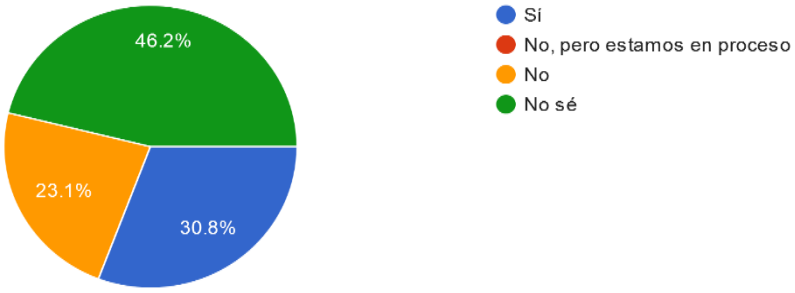


Figura 39 Información clasificada de datos personales, sensibles, financieros/patrimoniales

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: De acuerdo a la figura anterior, de los 13 funcionarios encuestados el 46,2% indicaron No saber si en el Distrito de Educación cuenta con información clasificada de datos personales, sensibles, financieros/patrimoniales. De otro modo el 30,8% respondieron que Sí cuenta con esta clasificación de información. Sin embargo, el 23,1% respondieron que No existe información clasificada.

Interpretación: La aplicación de esta pregunta demuestra que en el Distrito de Educación no existe la información clasificada, es decir, que se trata a cualquier tipo de información entre ella los datos sensibles de la misma manera que cualquier dato de carácter público.

11. ¿En qué departamento del Distrito de Educación 23D01 cree usted que existe mayor relevancia respecto a los datos sensibles?

Tabla 28 Departamento con mayor relevancia de datos sensibles

RESPUESTA	FRECUENCIA	PORCENTAJE
Unidad Financiera	1	7,7%
Unidad de Planificación	1	7,7%
Dece	5	38,5%
Unidad de Talento Humano	0	0%
Asesoría Jurídica	6	46,2%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

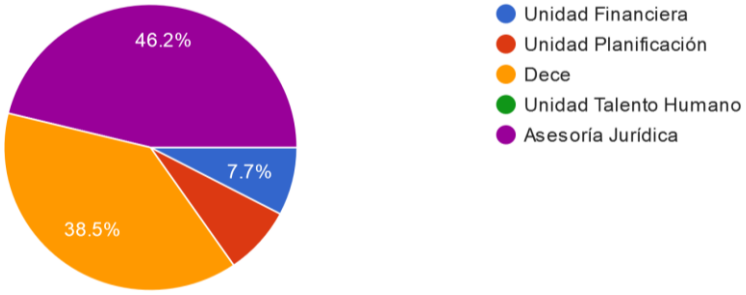


Figura 40 Departamento con mayor relevancia de datos sensibles

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Se preguntó a la población en cual departamento se manejan más datos sensibles dando como resultado que el 46,2% de los datos se encuentran en la unidad de Asesoría Jurídica, seguido del Departamento de Consejería Estudiantil (DECE) con el 38,5% y por último con el 7,7% las Unidades Financiera y Planificación.

Interpretación: Según la encuesta se refleja que en las unidades departamentales de Asesoría Jurídica y Dece existe mayor circulación de datos sensibles lo que se convierte en una alerta como objeto de estudio dichos departamentos.

12. ¿Utiliza métodos de encriptación para él envió de información sensible que lo realiza vía correo electrónico?

Tabla 29 Resultados: Uso de métodos de encriptación para el envío de información sensible.

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	0	0%
Casi Siempre	1	7,7%
A veces	3	23,1%
Casi Nunca	4	30,8%
Nunca	5	38,5%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

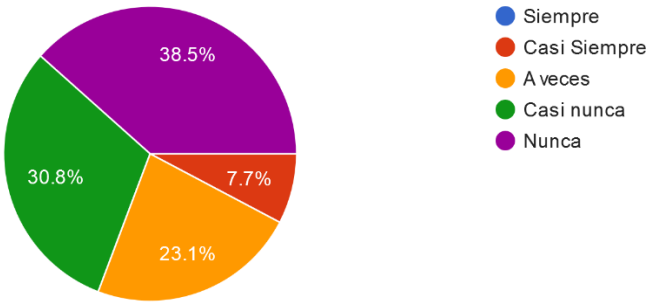


Figura 41 Resultados: Uso de métodos de encriptación para el envío de información sensible.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: El 38.5% de los encuestados respondieron que "Nunca" hacen uso de métodos de encriptación para el envío de información sensible, en cambio, el 30,8% respondieron "Casi nunca", por su parte el 23,1% indica que "A veces" y por último el 7% menciona que casi siempre lo hace.

Interpretación: Aproximadamente el 92,2% no utilizan métodos de encriptación para el envío de información, lo que conlleva a que datos sensibles puedan ser vulnerables.

13. ¿El Distrito de Educación 23D01 le ha hecho firmar un acuerdo de confidencialidad de la información?

Tabla 30 Resultados: Acuerdo de Confidencialidad

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	1	7,7%
Casi Siempre	4	30,8%
A veces	1	7,7%
Casi Nunca	1	7,7%
Nunca	5	38,5%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

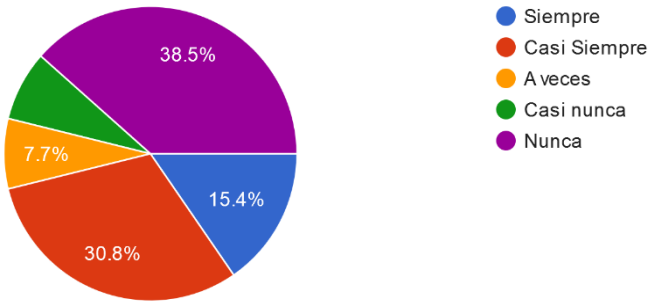


Figura 42 Resultados: Acuerdo de Confidencialidad

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Como lo describe en la figura de los resultados de Acuerdo de confidencialidad, del total de los encuestados en relación a si le han hecho firmar un acuerdo de confidencialidad respondieron: el 38,5% que nunca lo han hecho, así mismo el 30,8% dieron a conocer que casi siempre lo han hecho, además el 15,4% indicaron que siempre lo hacen y con el 7,7% manifestaron que a veces y casi nunca lo hacen.

Interpretación: El resultado de esta pregunta permite conocer que el 52,9% no firma o firmó un acuerdo de confidencialidad para el tratamiento de datos sensibles, lo que tiende a generar repudio al momento de que algún dato sensible sea expuesto como público.

14. ¿Sabe reconocer un correo electrónico sospechoso?

Tabla 31 Resultados: Reconoce un correo electrónico Sospechoso

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	2	15,4%
Casi Siempre	2	15,4%
A veces	5	38,5%
Casi Nunca	2	15,4%
Nunca	2	15,4%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

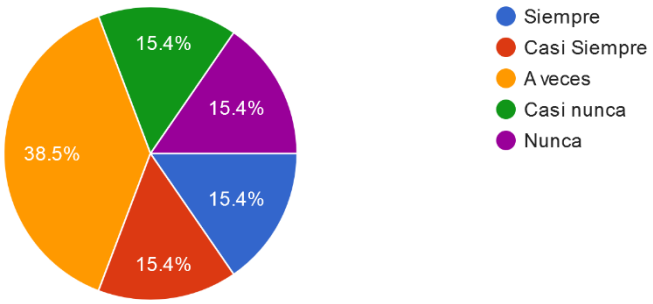


Figura 43 Resultados: Reconoce un correo electrónico Sospechoso

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Basándose en las respuestas, es posible deducir que tan solo 15,4% siempre y casi siempre reconocen un correo electrónico sospechoso, pero el 38,5% a veces lo hace, frente al 15,4% que casi nunca y nunca lo reconocen

Interpretación: Los resultados expuestos en esta pregunta arrojan datos alarmantes debido a que del total de los encuestados el 69,3% manifiestan no reconocer un correo electrónico sospechoso. Estos datos son preocupantes debido a que las Unidades del Distrito de Educación se pueden ver expuestas a ciberataques.

15. ¿Cuál es el nivel de riesgo que tiene el Distrito de Educación 23 D01 en las siguientes situaciones para el robo o el mal uso de los datos sensibles? Para sus respuestas utilizar la siguiente escala:1. Débil 2. Notable3. Muy Fuerte

Tabla 32 Resultados: Niveles de Riesgo en situaciones de robo o el mal uso de datos sensibles.

RESPUESTA	Ataques cibernéticos a través de internet a vía correo electrónico	PORCENTAJE	Ataques cibernéticos a través de red local (realizados por terceros)	PORCENTAJE	Robo de información vía dispositivos usb, discos duros, celulares, Tablet.	PORCENTAJE	Robo de laptops y/o Pcs.	PORCENTAJE
1	5	38,46 %	2	15,38 %	3	23,08 %	2	15,38 %
2	6	46,15 %	9	69,23 %	5	38,46 %	5	38,46 %
3	2	15,38 %	2	15,38 %	5	38,46 %	6	46,15 %
Suman	**13**	**100%**	**13**	**100%**	**13**	**100%**	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

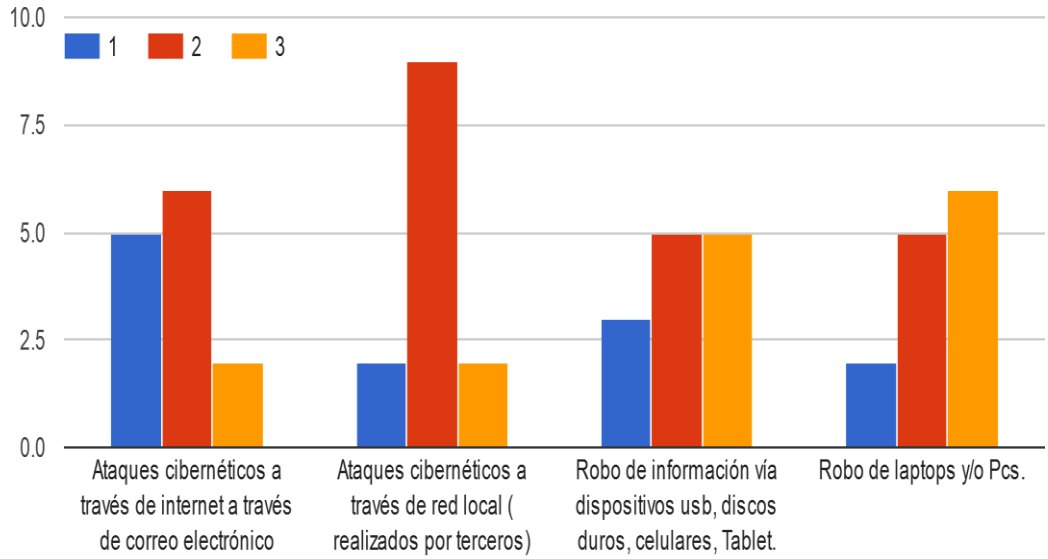


Figura 44 Resultados: Niveles de Riesgo en situaciones de robo o el mal uso de datos sensibles.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Mediante la aplicación de esta interrogante se determinó el nivel de riesgo que califica cada uno de los jefes departamentales en distintas situaciones que se puede ver expuesta información sensible del Distrito de Educación siendo las respuestas de la siguiente manera: referente a los ataques cibernéticos a través de internet vía correo electrónico el 46,15% lo consideran medianamente riesgoso, de otro modo los ataques a través de red local (ocasionados por terceros) es una vulnerabilidad notable debido que 69,23% de los interrogados lo consideran de esta manera, el robo de información vía (usb, disco duro, celulares, tablets) existió paridad en cuanto al notable y fuerte nivel de riesgo con el 38,46%, y por último 46,5% de los encuestados consideran un riesgo fuerte el robo de laptops y/o Pcs.

Interpretación: Las respuestas de los encuestados sirven como indicador para medir el nivel de riesgo y la conciencia que existe en cada uno de los jefes de unidad administrativa ante una eventualidad expuesta. De ellos mismos se ubican los riegos, respondiendo al nivel notable y fuerte con mayor frecuencia.

16. ¿Cuál sería el impacto principal que pueda ser provocado por la fuga de datos sensibles del Distrito de Educación 23D01?

Tabla 33 Impacto principal ante la fuga de datos sensibles

RESPUESTA	FRECUENCIA	PORCENTAJE
Legal	7	53,8%
Económico	1	7,7%
Imagen y Reputación	3	23,1%
Operativo	2	15,4%
Continuidad de negocio	0	0%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

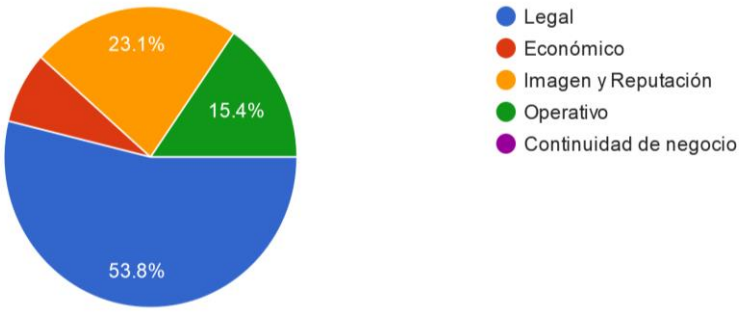


Figura 45 Impacto principal ante la fuga de datos sensibles

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Entre los principales tipos de impacto que el Distrito de Educación se puede ver afectado si existiera fuga de información entre ellos datos sensibles, la gran mayoría que corresponde al 53,8% respondió que se vería afectado por aspectos legales, seguido por el 23,1% que mencionan que la afectación sería en términos de imagen y reputación, por su parte, el 15,4% indican que tendría que ver con procesos operativos, y por último el 7,7% dan a conocer que el impacto significaría una sanción o pérdida económica.

Interpretación: Con los resultados obtenidos se concluye que la gran parte de los encuestados relacionan una sanción legal si es que hubiese algún tipo de fuga de información. En el caso del Distrito de Educación lo legal se relaciona estrechamente con la imagen y reputación lo que significaría que los usuarios

(funcionarios, docentes, estudiantes y padres de familia) realicen una demanda contra los responsables del tratamiento de la información.

17. ¿Referente al manejo de sistemas de información del Mineduc, utiliza contraseñas fuertes y una diferente para cada servicio?

Tabla 34 Manejo de contraseñas diferentes para cada servicio

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	4	30,8%
Casi Siempre	6	46,2%
A veces	2	15,4%
Casi Nunca	0	0%
Nunca	1	7,7%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

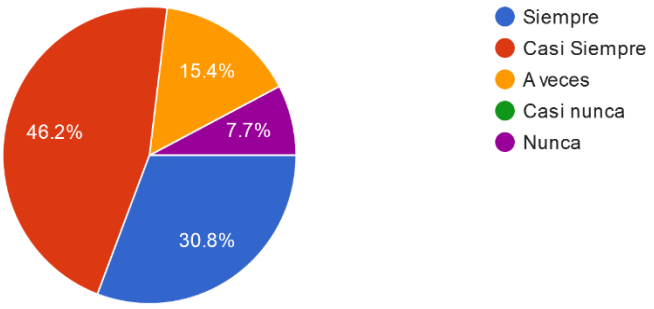


Figura 46 Manejo de contraseñas diferentes para cada servicio

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: De acuerdo con la pregunta N°17 realizada, se observa que el 46,2% de los encuestados mencionan que casi siempre usan contraseñas fuertes, por otro lado, el 30,8% dan a conocer que siempre hacen uso de claves robustas y diferentes para cada servicio y el 15,4% lo hace a veces.

Interpretación: Los funcionarios son conscientes de los riesgos que implican manejar los servicios que ofrecen los sistemas de información que ellos utilizan diariamente, por lo que se observa la preocupación de usar claves fuertes y diferentes para cada servicio.

18. ¿Culturalmente y como medida de prevención cambia con regularidad las contraseñas de los sistemas de información de Mineduc?

Tabla 35 Cambios de contraseñas con regularidad.

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	4	30,8%
Casi Siempre	3	23,1%
A veces	2	15,4%
Casi Nunca	4	30,8%
Nunca	0	0%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

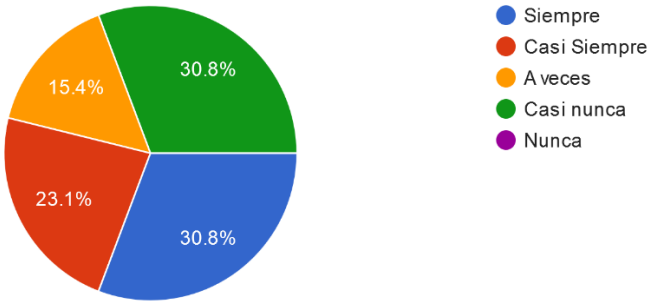


Figura 47 Cambios de contraseñas con regularidad.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Como se puede observar, tan solo el 30,8% de los encuestados siempre realizan cambios de contraseña con regularidad, el 23,1% lo realiza casi siempre, a diferencia del 15,4% que dieron a conocer que los cambios de clave lo hacen a veces, sin embargo, el 30,8% lo casi nunca lo hace.

Interpretación: Existe concordancia en cuanto a las respuestas de los jefes de unidad sobre los cambios de contraseña, lo que demuestra que en ciertos departamentos existe el conocimiento o la cultura de seguridad informática de lo importante que es mantener contraseñas actualizadas.

19. ¿Con frecuencia el departamento de TI realiza copias de seguridad de los sistemas de información de Mineduc?

Tabla 36 Frecuencia en Copias de Seguridad de los sistemas de información del Mineduc

RESPUESTA	FRECUENCIA	PORCENTAJE
Diariamente	0	0%
Semanalmente	1	7,7%
Mensualmente	10	76,9%
Anualmente	1	7,7%
Nunca	1	7,7%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

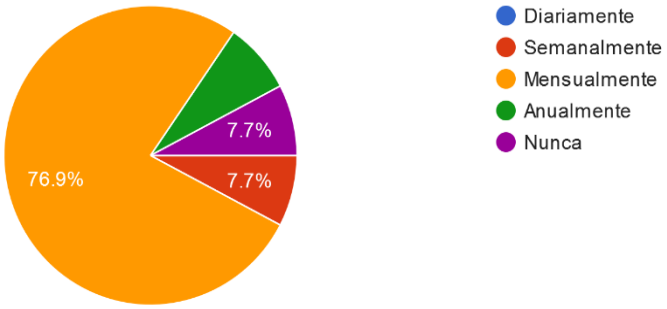


Figura 48 Frecuencia en Copias de Seguridad de los sistemas de información del Mineduc

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: De acuerdo a las respuestas, la mayoría de los encuestados que corresponde al 76,9% respondieron que las copias de seguridad realizadas por el departamento de TI son de manera mensual.

Interpretación: El departamento de TI dentro de su plan de contingencia está preparado para resolver eventualidades, pero con copias de seguridad que pueden tener un mes o más de desactualización. Es evidente que en ciertos departamentos los respaldos se los hace semanalmente, anualmente y en otro jamás se lo ha hecho.

20. ¿El personal de TI sabe cómo actuar ante alguna eventualidad con resultados trágicos relacionados a la seguridad informática?

Tabla 37 Percepción de los jefes de unidad frente a la manera de actuar del personal de TI ante un ciberataque con trágicos resultados.

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	3	23,1%
Casi Siempre	6	46,2%
A veces	3	23,1%
Casi Nunca	1	7,7%
Nunca	0	0%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

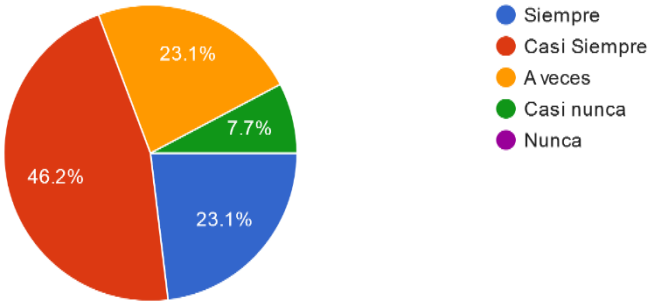


Figura 49 Percepción de los jefes de unidad frente a la manera de actuar del personal de TI ante un ciberataque con trágicos resultados.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: De las respuestas obtenidas en esta pregunta, queda evidenciado que el personal de TI casi siempre 46,2% conoce o sabe cómo actuar ante una eventualidad trágica de ciberseguridad, de la misma manera el 23,1% afirma que el departamento de TI "A veces" sabe cómo proceder, y con el mismo porcentaje 23,1% respondieron que "Siempre" actúa satisfactoriamente ante un riesgo informático.

Interpretación: Es notable que el personal de TI conoce técnicas o cuenta con un plan de contingencia ante un riesgo sea este natural o provocado. Esto es un indicador satisfactorio para el tema propuesto debido que, si el personal conoce de técnicas y mecanismos de seguridad informática, es posible la implementación de

un modelo de seguridad de la información lógica por la el grado de preparación que el personal posee.

21. ¿Considera que el personal de TI cuenta con un plan de contingencia para reaccionar oportunamente ante un ataque informático?

Tabla 38 Plan de contingencia para la reacción ante ataque un informático

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	1	7,7%
Casi Siempre	1	7,7%
A veces	6	46,2%
Casi Nunca	4	30,8%
Nunca	1	7,7%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

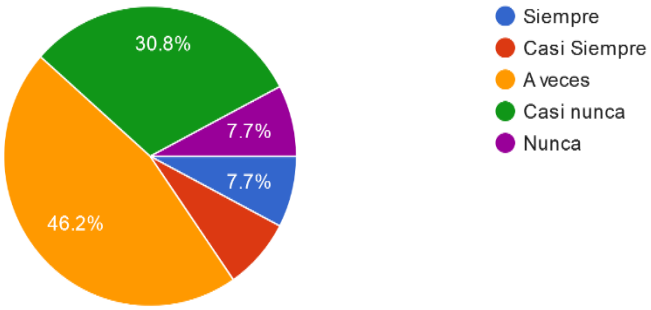


Figura 50 Plan de contingencia para la reacción ante ataque un informático

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Del total de los encuestados el 46,2% afirma que el personal de TI "A veces" sabe cómo reaccionar ante un ataque informático, seguido del 30,8% que mencionan que "Casi nunca" cuentan con un plan de contingencia para la atención oportuna de una eventualidad, por su parte el 7,7% se encuentra dividido entre "siempre" y "casi siempre", pero con este mismo porcentaje 7,7% afirma que "Nunca" saben cómo reaccionar debido que no cuentan con un plan de contingencia.

Interpretación: Es evidente que el personal de TI según los resultados de la pregunta 21, sabe cómo actuar ante una eventualidad, pero aun así no cuenta con un modelo o plan de contingencia para la reacción ante un ataque informático.

22. ¿La institución utiliza métodos específicos para la destrucción de la información sensible de sus usuarios?

Tabla 39 Métodos específicos para la destrucción de la información.

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	1	7,7%
Casi Siempre	0	0%
A veces	3	23,1%
Casi Nunca	2	15,4%
Nunca	7	53,8%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

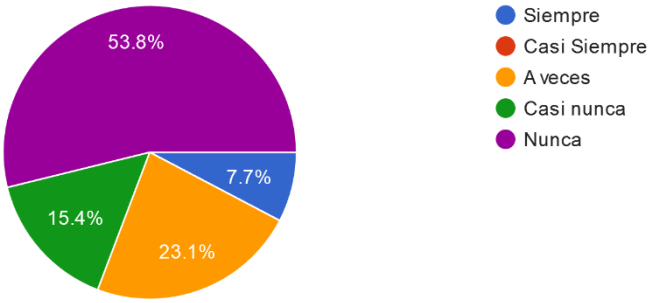


Figura 51 Métodos específicos para la destrucción de la información.

Elaborado por: *Vaca, P (2019)*

Análisis de Resultados: Tomando en cuenta la figura 51, el 53,8% afirma que en la institución no se usan métodos específicos de destrucción de la información, consecuentemente el 23,1% "A veces" utilizan estos métodos, del mismo modo el 15,4% responden "casi nunca", pero el 7,7% indican que siempre usan estos métodos.

Interpretación: Al no disponer de métodos de destrucción de la información se esta atentando contra un derecho que tienen las personas conocido como el derecho al olvido. Es importante mencionar que la información sensible puede ser recuperada de unidades de almacenamiento secundario, que se creía que ya no funcionaba, sea por actualización de hardware o muchos factores.

23. ¿Usted como funcionario conoce sus responsabilidades y las sanciones derivadas en la ley que pueden ser acreedores en temas de protección de la privacidad de la información?

Tabla 40 Responsabilidades y Sanciones derivadas de la ley.

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	7	53,8%
No	6	46,2%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

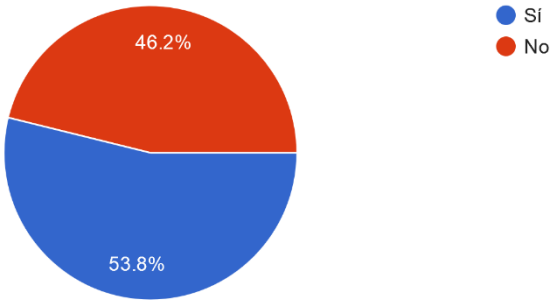


Figura 52 Responsabilidades y Sanciones derivadas de la ley.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Como se evidencia el grafico anterior, el 53,8% afirman si conocer sus responsabilidades y sanciones derivadas de la ley, sin embargo, el 46,2% mencionan no conocer.

Interpretación: Es importante saber que los funcionarios encuestados conocen de las responsabilidades y sanciones que se derivan de la ley en el caso de que exista fuga de información, por lo que es conveniente la implementación de un modelo de seguridad lógica de la información en la protección de datos sensibles, para que no se llegue a una instancia sancionadora.

24. ¿Cree que la aplicación de un modelo de seguridad de la información garantice la protección de los datos sensibles del Distrito de Educación 23D01 cuando estos sean transmitidos, subidos, receptados o generados?

Tabla 41 Aplicación de modelo de seguridad en la protección de datos sensibles.

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	11	84,6%
No	2	15,4%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

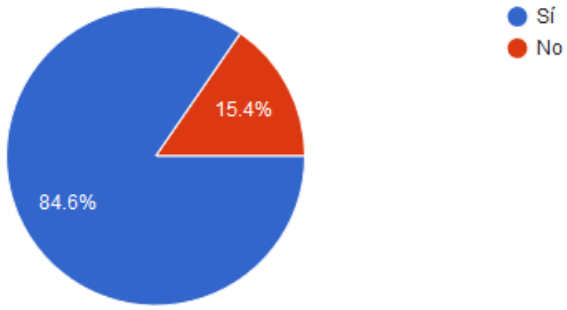


Figura 53 Aplicación de modelo de seguridad en la protección de datos sensibles.

Elaborado por: ***Vaca, P (2019)***

Análisis de Resultados: Tomando como base el gráfico de resultados anterior, el 86,24% de los encuestados creen que es conveniente aplicar un modelo de seguridad en la protección de los datos sensibles, frente al 15,4% que no lo toman como importante.

Interpretación: Los resultados de esta pregunta aclaran la situación actual referente al tratamiento de la información específicamente en la protección de datos sensibles y de la debida importancia que los jefes de unidad le toman a este tema. Esto también permite interpretar que dichos encargados departamentales necesitan contar con un modelo que tenga los respectivos lineamientos para la transmisión, recepción, carga o generación de este tipo de información.

4.2 Verificación de la Hipótesis

Para la verificación de la hipótesis y comprobar si es aplicable la propuesta de un modelo de gestión de seguridad lógica en la protección de la información sensible del Distrito de Educación 23D01, se ha tomado como referencia el método estadístico CHI-CUADRADO para la comprobación de las respectivas hipótesis planteadas en el tema: "MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR"

Se ha considerado como muestra las preguntas los ataques de phishing de la primera etapa de la recolección de datos y la pregunta N° 24 del cuestionario por la relación que tienen tanto con la variable independiente y dependiente en la protección de los datos sensibles de los distritos de educación.

Hipótesis Nula

H0: El modelo de gestión de la seguridad lógica de la información no incide en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

Hipótesis Alternativa

H1: El modelo de gestión de la seguridad lógica de la información incide en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

Combinación de Frecuencias:

Ataque N° 2. ¿El funcionario de la DD23D01 Educación de la ciudad de Santo Domingo identifica si un fichero contiene código malicioso antes de proceder a instalarlo?

Tabla 42 Resultados Manejo de modelo en el Distrito de Educación 23D01.

RESPUESTA	FRECUENCIA	PORCENTAJE
SI	1	7,69%
NO	12	92,31%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

Pregunta N°24. ¿Cree que la aplicación de un modelo de seguridad de la información garantice la protección de los datos sensibles del Distrito de Educación 23D01 cuando estos sean transmitidos, subidos, receptados o generados?

Tabla 43 Aplicación de modelo de seguridad en la protección de datos sensibles.

RESPUESTA	FRECUENCIA	PORCENTAJE
Sí	11	84,6%
No	2	15,4%
SUMAN	**13**	**100%**

Elaborado por: ***Vaca, P (2019)***

Tabla 44 Cálculo de Frecuencia Pregunta N°1

Pregunta	Cálculos
¿El funcionario de la DD23D01 Educación de la ciudad de Santo Domingo identifica si un fichero contiene código malicioso antes de proceder a instalarlo?	SI=13*0,462=6 (SI)
	NO= 13*0,0,538=7 (NO)

Elaborado por: ***Vaca, P (2019)***

Cálculo de la de Frecuencia Esperada

Respuestas:

- R1(SI)= 14/26= 0,46153846
- R2(NO)=12/26=0,53846154

Tabla 45 Cálculo de Frecuencia Pregunta N°2

Pregunta	Cálculos
¿Cree que la aplicación de un modelo de seguridad de la información garantice la protección de los datos sensibles del Distrito de Educación 23D01 cuando estos sean transmitidos, subidos, receptados o generados?	SI=13*0,462=6 (SI)
	NO= 13*0,0,538=7 (NO)

Elaborado por: *Vaca, P (2019)*

Tabla 46 Combinación de frecuencias para Comprobar Hipótesis

N°	Pregunta	SI	NO	Σ
1	¿El funcionario de la DD23D01 Educación de la ciudad de Santo Domingo identifica si un fichero contiene código malicioso antes de proceder a instalarlo?	1	12	13
2	¿Cree que la aplicación de un modelo de seguridad de la información garantice la protección de los datos sensibles del Distrito de Educación 23D01 cuando estos sean transmitidos, subidos, receptados o generados?	11	2	13
	TOTAL:	**12**	**14**	**26**

Elaborado por: ***Vaca, P (2019)***

Para comprobar la hipótesis, la fórmula de Chi cuadrado es la siguiente:

$$X^2 = \Sigma \frac{(Fo - Fe)^2}{Fe}$$

En donde:

X2 = Chi Cuadrado

∑ = Sumatoria

Fo = Frecuencia Observada

Fe = Frecuencia Esperada

Tabla 47 Cálculo Valores Frecuencia Esperada

Frecuencias	Pregunta N°1	Pregunta N°2	TOTAL
SI	6	6	23
NO	7	7	14
SUMAN:	**13**	**13**	**26**

Elaborado por: ***Vaca, P (2019)***

Tabla 48 Relación de las Frecuencias

Alternativa	F. Observada	F. Esperada	Fo-Fe	$(Fo - Fe)^2$	$\frac{(Fo - Fe)^2}{Fe}$
SI (P1)	1	6	-5	25	4,166666667
SI (P2)	11	6	5	25	4,166666667
NO (P1)	12	7	5	25	3,571428571
NO (P2)	2	7	-5	25	3,571428571
SUMAN:	**26**	**24**	**0**		**15,47619**

Elaborado por: ***Vaca, P (2019)***

Entonces: X^2c = 15,47619

Cálculo del grado de libertad

A continuación, se calcula el grado de libertad mismo que se lo calcula multiplicando el número de filas menos uno por el número de las columnas menos uno:

Fórmula:

Gl = (F-1) (C-1)

En donde:

Gl = Grados de Libertad

C = Número de variables

F = Número de frecuencias de respuestas

Desarrollo:

Gl = (2-1) (2-1)

Gl = (2) (1)

Gl = 1

El valor crítico para 1 grado de libertad y el nivel de significancia 0.05, se encuentra en la tabla de Chi- cuadrado.

Donde:

X^2c = Chi cuadrado calculado

X^2t = Chi cuadrado de la tabla según el nivel de significancia elegido.

Tabla 49 Distribución Chi Cuadrado X^2

TABLA DISTRIBUCIÓN X^2					
Grados de libertad	**PROBABILIDAD**				
	0,100	**0,050**	**0,025**	**0,010**	**0,005**
1	2,710	**3,840**	5,020	6,630	7,880
2	4,610	5,990	7,380	9,210	10,600
3	6,250	7,810	9,350	11,340	12,840
4	7,780	9,490	11,140	13,280	14,860
5	9,240	11,070	14,450	15,090	16,750

Fuente: Interaprendizaje de probabilidades y estadística inferencial.
Elaborado por: *Suárez M.* (2012)

Se observó según la tabla de distribución de Chi-cuadrado X^2 tomando en consideración el nivel de significancia y los grados de libertad, da como resultado el siguiente dato:

$$X^2\mathbf{t = 3,840}$$

Decisión final

1. Si X^2c < X^2t = se acepta la Hipótesis Nula (Ho)

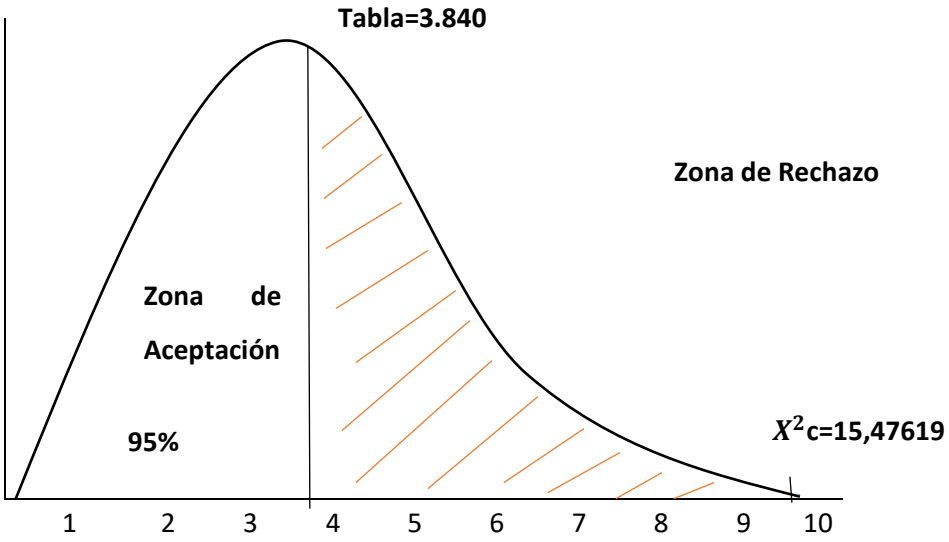
15,47619<3,840

2. Si X^2c > X^2t = se rechaza la Hipótesis Nula (Ho)

15,47619>3,840

De acuerdo a los resultados obtenidos se puede verificar que el valor de Chi-cuadrado calculado es mayor que el de Chi-cuadrado de la tabla por lo que se rechaza la Hipótesis Nula (Ho) y se acepta la Hipótesis Alternativa (H1) que dice: El modelo de gestión de la seguridad lógica de la información incide en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

Tabla 50 Zona de Aceptación de la Hipótesis



Fuente: Tabla relación de frecuencias y Distribución del Chi Cuadrado

Elaborado por: ***Vaca, P (2019)***

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Con la información obtenida a través de las técnicas de pen testing y las preguntas de las encuestas aplicadas a los jefes departamentales de la Dirección Distrital Educación 23D01 se concluye:

- Los resultados del pentesting referente al ataque de phishing y a la recolección de información mediante malwares troyanos de tipo keyloggers, constituyen un indicador clave para reconocer el deficiente nivel de madurez del personal que labora en la Dirección Distrital Educación 23D01 en temas de seguridad informática, y específicamente en el de exponer información o datos sensibles de si mismos y en sí de la organización.
- Con la aplicación de las técnicas pentesting y de la encuesta se determina que la Dirección Distrital Educación 23D01 no cuenta con procesos estandarizados y que deban cumplirse para que los datos sensibles que en esta organización se genera, transmite y guarda sean protegidos ante cualquier vulnerabilidad.
- Utilizando la metodología de análisis y gestión de riesgos de tecnologías de la información MAGERIT, permitió identificar el nivel de madurez en temas de seguridad de informática, con los que cuentan los funcionarios que aspectos como jefes departamentales de la Dirección Distrital Educación 23D01, reflejando que la Dirección Distrital 23D01 no cuenta con un nivel aceptable en tema de protección de datos personales.
- Al no tener un modelo de seguridad que sirva como lineamiento para la transmisión y protección de la información entre ella la de los datos sensibles y que llega a terceras personas que no sean tanto el concernido como los concernientes o encargados del tratamiento de la misma puede generar que el Distrito de Educación se vea afectado en ámbitos legales, perdidas de reputación e imagen y también puede llegar a tener un desenlace con pérdidas económicas.

5.2 Recomendaciones

Una vez finalizada las dos etapas que en este documento de investigación se lo incluyen en el apartado de análisis e interpretación de los datos se recomienda:

- Realizar evaluaciones mediante, técnicas de ethical hacking, pen testing auditorías internas, la aplicación de cuestionarios, y pruebas de tratamiento de la información para que se garantice la confidencialidad, integridad y disponibilidad de los datos sensibles.
- Realizar capacitaciones periódicas a los funcionarios de la institución mediante cursos e- conferencias y talleres con el objetivo de que se tenga el correcto conocimiento de cómo se deben tratar los datos sensibles que se trasmiten por medio de los sistemas de información que maneja el Distrito de Educación.
- Diseñar un modelo de la seguridad lógica de la información en la protección de los datos sensibles del Distrito de Educación 23D01 de la ciudad de Santo Domingo, que contenga lineamientos, procesos y todos los recursos necesarios, para mitigar en lo máximo posible cualquier ataque o vulnerabilidad, en los que se vean comprometidos los derechos de los usuarios referente al tratamiento de sus datos sensibles.
- Implementar un modelo de gestión de la seguridad lógica de información, en el cual se indiquen lineamientos, técnicas y mecanismos para proceder en la mitigación y acción ante una vulnerabilidad, de no ser así aumentará el riesgo a que ocurra pérdidas de información, falla en la integridad de los datos, suspensiones al momento de pretender recuperar los datos, o las mismas fugas de datos sensibles de los usuarios del sistema informático que pueden llevar a temas como perdida de reputación de la Dirección Distrital Educación 23D01,o caer en sanciones de acuerdo a la legislación de la Republica del Ecuador en protección de datos sensibles.

CAPITULO VI

PROPUESTA

6.1 Datos informativos

6.1.1 Institución ejecutora

Dirección Distrital 23D01 Educación Santo Domingo de los Tsáchilas.

6.1.2 Beneficiarios

Unidades departamentales del Distrito de Educación.

6.1.3 Ubicación

Provincia: Santo Domingo de los Tsáchilas.

Cantón: Santo Domingo.

Dirección: Calle Río Chimbo y Balzapamba.

6.1.4 Equipo técnico responsable

Investigador: Ing. Patricio Neptali Vaca Escobar

6.2 Antecedentes de la propuesta

La Dirección Distrital 23D01 Educación de la provincia de Santo Domingo de los Tsáchilas misma que pertenece a la Coordinación Zonal 4, es una institución de carácter públicos dependiente de los recursos financieros por parte del Gobierno Central. Fue creada bajo el Acuerdo Ministerial N° 133-12 suscrito por la Dra. Gloria Vidal Illingworth el 25 de enero del 2012 ex Ministra de Educación. El Artículo 1 del acuerdo menciona "Crear, dentro de la jurisdicción de la coordinación Zonal 4, el Distrito educativo intercultural y bilingüe "ALLURIQUÍN, LUZ DE AMERICA, ESFUERZO, TOACHI, PERIFERIA, RÍO VERDE, SANTO DOMINGO, ZARACAY, RÍO TOACHI, CHIGUILPE".

En el segundo Artículo del acuerdo se determina que "el referido Distrito educativo, estará conformado por las instituciones educativas públicas, fiscomisionales y particulares de todos los niveles y modalidades, que se encuentren situadas, o en lo posterior se ubiquen, dentro de la circunscripción territorial de su competencia".

Una vez conformada la Dirección Distrital 23D01 Educación de Santo Domingo pasa a cumplir con funciones del desarrollo y mantenimiento de las instituciones educativas, de tal manera que es la encargada de alojar toda la información tanto de la comunidad educativa, así como de los funcionarios, proveedores, entre otros.

Es así que mediante la encuesta realizada por medio de la aplicación de un cuestionario dirigido a cada uno de los jefes de cada una de las unidades del Distrito se ve la necesidad de proponer la aplicación de un modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles, para mitigar en lo máximo posible las vulnerabilidades existentes en las generación, manipulación y transmisión de información sensible.

6.3 Justificación

Mediante los resultados obtenidos en el análisis e interpretación de cada una de las preguntas realizadas a los jefes de unidad, permitió evidenciar que la falta de protección de los datos sensibles que se transmiten en la Dirección distrital 23D01 Educación de la ciudad de Santo Domingo debido a la manera como en la actualidad se trata este tipo de información.

La presente investigación se enfocará principalmente en proponer un modelo de gestión de seguridad en el tratamiento de la información, específicamente para la protección de los datos sensibles de la Dirección Distrital 23D01 Educación de la ciudad de Santo Domingo.

De la misma forma es importante proponer un modelo de gestión de seguridad de la información, debido a que permitirá ser una base sustentable para la transmisión de los datos sensibles de la organización. Esto se debe a que se implementará lineamientos y políticas para que en lo máximo posible se mitiguen las vulnerabilidades existentes en el tratamiento de este tipo de datos.

Este estudio se justifica debido a que se cuenta con la aprobación del Director Distrital, quien autorizó el acceso a la documentación lo que garantiza la continuidad del presente trabajo de investigación.

6.4 Objetivos

6.4.1 Objetivo General

Definir un modelo de gestión de la seguridad lógica de la información con lineamientos en los que se adopten buenas prácticas para el alcance de un nivel aceptable de los riesgos y amenazas existentes en el tratamiento de los datos sensibles de la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo.

6.4.2 Objetivos Específicos

- Determinar las fases del ciclo Deming o PDCA de ISO 27001:2013 para contar con lineamientos en la construcción del modelo de gestión.
- Desarrollar un modelo de gestión de la seguridad de la información lógica para la protección de datos personales que se capturan, procesan almacenan y distribuyen en la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo.
- Proponer un modelo de gestión de la seguridad de la información lógica en las que se compruebe mediante un análisis comparativo el uso de buenas prácticas de seguridad el tratamiento de datos sensibles en la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo.

6.5 Análisis de Factibilidad

6.5.1 Factibilidad tecnológica

El presente documento de investigación es tecnológicamente factible, debido a que la Dirección Distrital 23D01 Santo Domingo de los Tsáchilas cuenta con una infraestructura tecnológica necesaria para la evaluación mediante pruebas de identificación de vulnerabilidades en el tratamiento de información sensible.

6.5.2 Factibilidad organizacional

Organizacionalmente es factible, debido a que se cuenta con el visto bueno, la aprobación y la disposición del Director Distrital, quien tiene el conocimiento del problema existente en la institución en la manera como los datos sensibles son tratados actualmente.

6.5.3 Factibilidad económica-financiera

Este proyecto es factible económica-financiero, ya que no se necesita de un coste extra para la adquisición de equipos para la aplicación de modelo de gestión de seguridad de la información. Por otra parte, la Dirección Distrital cuenta con los recursos e infraestructura necesaria para que se realice la implementación del modelo de seguridad.

6.5.4 Factibilidad Legal

La presente investigación se fundamenta en el acuerdo ministerial N° 166 publicado mediante Registro Oficial No. 88 del 25 de septiembre de 2013, de la Ley Orgánica del Servicio Público, en su artículo 22, y de la norma de control interno (NCI) 401-10 – Seguridad de la tecnología de la información. Además, se encuentra legalmente aprobado por el alto directorio del distrito y del jefe de la Unidad de Tecnología de la información para el uso de los sistemas de información e infraestructura de la organización.

6.6 Fundamentación Teórica

El tratamiento de la información sensible que se manejan en la Dirección Distrital 23D01 Educación, debe acogerse a los siguientes aspectos legales:

- Estar definido en la constitución de la Republica del Ecuador con el Referéndum 2008.
- Acuerdo ministerial N° 166 publicado mediante registro oficial No. 88 del 25 de septiembre del 2013
- El artículo 22 de la Ley Orgánica del Servicio Público (LOSEP).
- La Norma de control interno (NCI) 401-10- Seguridad de la tecnología de la información.

6.6.1 Base o banco de datos

Para Rebollo & Saltor (2014), una base de datos es un conjunto organizado de datos personales, los cuales son objeto de tratamiento o procesamiento, digital o no, cualquiera que sea la modalidad de su formación, almacenamiento, organización o acceso.

6.6.2 Dato personal

Figura 54 Descripción de datos personales.

Fuente: (Dirección Nacional de Registros Públicos , 2019)

Se denomina a dato personal a cualquier tipo de información, que se le relaciona a una o varias personas mismas que pueden ser identificadas e identificables, entre estos se tiene: (nombres, apellidos, fecha de nacimiento, dirección, correo electrónico, números de teléfono, numero de cedula, matricula vehicular, información académica, entre otros), de los cuales se puede describir físicamente a una determinada persona (López, 2015).

6.6.3 Consentimiento del titular

Como lo mencionan Geraldes & López (2010), el consentimiento del titular, permitirá al encargado del tratamiento de los datos tener los permisos pertinentes para que los datos del titular se los pueda usar para los diversos fines con los que se diseñó la base de datos.

Por su parte, en el proyecto de la Ley Orgánica de los derechos a la intimidad y privacidad de los datos personales se lo menciona como toda manifestación de voluntad, libre, inequívoca, especifica e informada, mediante la cual el titular autoriza el tratamiento de datos personales.

6.6.4 Datos sensibles

Los datos sensibles hacen referencia a las características físicas de las personas, de las cuales se revele información que únicamente le pertenece a el como titular, o la persona que le haya autorizado su consentimiento para su respectivo uso. Entre estos datos se encuentran: estado patrimonial y financiero, creencias religiosas, salud, vida sexual, mismos que revelen la vida privada de las personas (DINARDAP, 2019).

6.6.5 Disociación de datos

Se conoce como Disociación de datos al procedimiento por el cual los datos personales entre ellos los sensibles no se los puedan vincular a una persona físicamente, es decir, esto permite que la persona con estos datos no sea identificada o identificable (DINARDAP, 2019).

6.6.6 Protección de datos personales

Potestad que dictamina la Ley para que el titular de los datos, sea quién decide a quien autoriza para que su información sea utilizada. Mediante la aplicación de este derecho el encargado del tratamiento de datos está en la obligación de acceder, rectificar, cancelar y oponerse al tratamiento de la información personal del titular (DINARDAP, 2019).

6.6.7 Responsable del tratamiento de la información

Como se describe en el artículo 4 de las definiciones del proyecto de Ley de protección de datos personales (Asamblea Nacional del Ecuador, 2016) el responsable es la persona natural o jurídica, pública o privada que sola o conjuntamente con otros, administra el sistema de tratamiento de datos personales por cuenta del responsable del archivo, registro, base o banco de datos. Toda operación de información que comprometa los datos personales, en el procedimiento mecánico o automatizado que tenga como fin la recolección,

ordenamiento, conservación, almacenamiento, modificación, evaluación, destrucción, procesamiento de datos, así como el acceso de terceros por cualquier medio, deberá observar estrictamente la normativa prevista, bajo los derechos de protección y salvaguardia de identidad.

6.6.8 Responsable del archivo, registro, base o banco de datos

Según (Enríquez Álvarez, 2017), el responsable del archivo es la persona natural o jurídica, pública o privada que es titular de un archivo, registro, base o banco de datos como custodio y operador de la información.

6.6.9 Titular de los datos

El titular de los datos cuenta con un derecho que le otorga la ley con el cual puede ejercer el control total sobre la manera en que su información personal es tratada, además de poder protegerlos en el caso de que exista usos malintencionados causado por terceros (San Martín, 2015).

6.6.10 Usuario de datos

Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos(Asamblea Nacional del Ecuador, 2016).

6.6.11 Tratamiento de datos

Figura 55 Procesos que intervienen en el tratamiento de datos personales

Fuente: (Dirección Nacional de Registros Públicos , 2019)

Para Ambrosio (2017), el tratamiento de datos es considerado como la cualquier operación o conjunto de operaciones que actúan sobre los datos personales, sean estos procedimientos automatizados o no, tales como: la captura, almacenamiento, adaptación, organización, modificación, transferencia, transmisión, derecho al olvido, destrucción supresión y limitación.

6.6.12 Tratamiento de datos sensibles

El artículo 5 de la Ley Orgánica de los Derechos a la Intimidad y Privacidad sobre los Datos Personales menciona que, se prohíbe el tratamiento de los datos sensibles en todo aquello que pueda afectar el derecho a la intimidad de la persona. Nadie podrá ser obligado a proporcionar datos sensibles, salvo las siguientes circunstancias (Asamblea Nacional del Ecuador, 2016):

1. El titular autoriza expresamente y por escrito el tratamiento de datos sensibles.
2. El tratamiento es necesario para salvaguardar el interés vital del titular si este se encuentra física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
3. El tratamiento se refiere a datos que son indispensables para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
4. El tratamiento tiene una finalidad estadística, científica o académica. En este evento deberán adoptarse las medidas conducentes a la suspensión de identidad de titulares.

6.7 Elaboración de la propuesta

Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador.

6.7.1 Fases de la implementación del modelo de seguridad de protección de la información sensible de los Distritos de Educación del Ecuador.

El modelo de gestión de la seguridad lógica de la información consta de 5 fases fundamentales, mismas que permitirán a los Distritos de Educación del Ecuador gestionar de manera eficiente la protección de sus datos sensibles.

El objetivo del presente documento es de brindar lineamentos a los responsables y encargados del tratamiento de datos, para poner en práctica un modelo, de tal manera que mediante un proceso de mejora continua se logre un nivel de madurez aceptable en el ejercicio de minimizar los riesgos frente al tratamiento de información personal.

Cabe recalcar que para la adopción del modelo es necesario acogerse a las normativas internas y a la legislación existente en cuanto al tratamiento de datos se refiere. Por tal razón la aplicación de un modelo de gestión de la seguridad de la información sensible, constituye una estrategia para hacer frente a los riesgos de seguridad y las amenazas informáticas que pueda comprometer la triada CID, es decir, poner en riesgo la confidencialidad, integridad o disponibilidad de la información sensible.

Es importante señalar que el alcance del modelo es la protección de los datos sensibles y su correcto tratamiento, controlado e informado, siendo su principal misión garantizar la privacidad de información de los datos sensibles de los usuarios.

Como es de conocimiento general, en la actualidad existen diversos Frameworks o marcos de referencia que sirven como punto de partida para la implementación de un modelo de seguridad. Así mismo, el modelo Deming o PHVA se lo considera como un referente para el modelo propuesto.

6.7.1.1 Detalle de las fases del modelo

En este epígrafe se dará a conocer las fases que se incluyen en el modelo de gestión de seguridad lógica de la información. En el detalle de las cinco fases se dan a conocer el contenido entre ellos: objetivos, herramientas que permiten que la seguridad de la información se convierta en un modelo de gestión en la protección de datos personales de las Direcciones Distritales Educación del Ecuador.

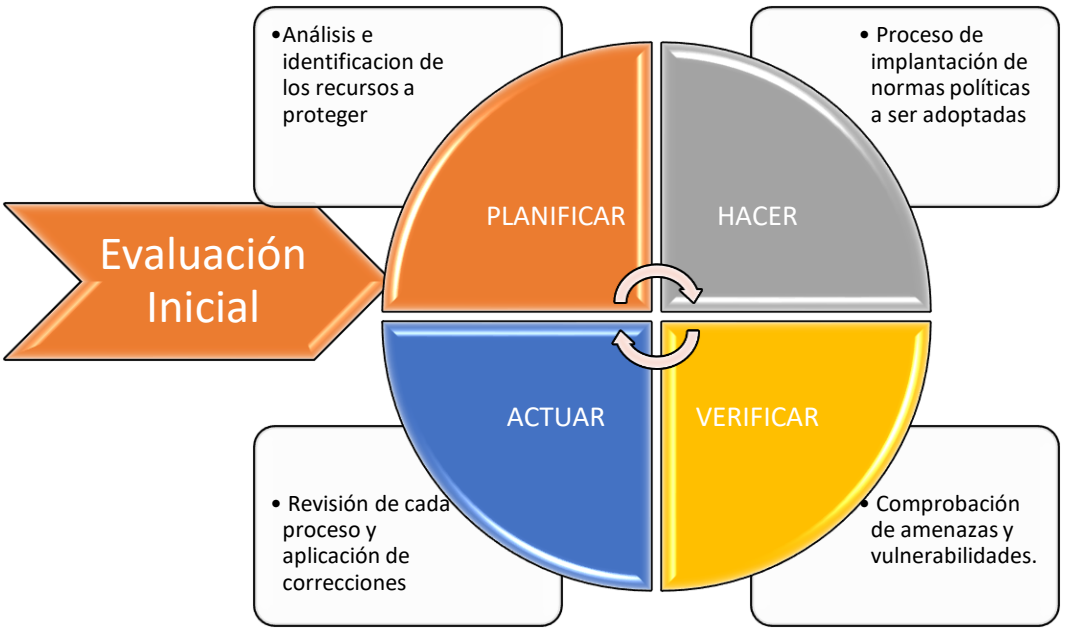


Figura 56 Descripción de las fases del modelo planteado.

Elaborado por: ***Vaca, P (2019)***

El alcance del modelo de gestión de la seguridad lógica de la información es de proveer de un marco de referencia para el tratamiento de tatos personales, mismo que permitirá mantener y mejorar la protección de datos personales para el cumplimiento ante las entidades regulatorias, una cultura de seguridad informática y fomentar buenas prácticas. Las fases, pasos y objetivos del ciclo PHVA se los detallan en la siguiente tabla:

Tabla 51 Fases, Pasos y Objetivos del MGSDP

Fase	Subfases	Objetivos Específicos
Planificar	1.- Alcance y objetivos 2.- Política de gestión de datos personales. 3.- Funciones y obligaciones de quienes traten datos personales. 4.- Inventario de datos personales. 5.- Análisis y riesgos de datos personales. 6.- Identificación de las medidas de seguridad y análisis de brecha.	Identificar los objetivos, políticas, procesos y procedimientos más importantes del modelo de gestión de seguridad de la información lógica para que con esto se cumpla lo establecido en los documentos reguladores y legisladores.
Hacer (Implementar y operar el modelo)	7.- Implementación de las medidas de seguridad aplicables a los datos personales	Llevar a cabo el desarrollo, implantación y operación de las políticas, objetivos y procedimientos del modelo de gestión de seguridad de la información (MGSDP), y de la misma forma sus controles o mecanismos con sus

		respectivos indicadores de desempeño (KPI).
Verificar (Monitorear y revisar el modelo)	8.- Revisiones y auditoría	Realizar evaluaciones periódicas y medir el cumplimiento del proceso verificando si es que los objetivos del modelo se encuentran alineados con los de la organización y con las políticas del mismo. De la misma manera informar a los Directivos para su respectiva revisión.
Actuar (mejorar el modelo)	9.- Mejora continua y capacitación.	Una vez revisada la fase de verificación por los Directivos e importante adoptar medidas correctivas y preventivas para lograr la mejora continua por otra parte es importante mantener capacitado e informado al personal para que en la Dirección Distrital se genere un ambiente hacia una cultura de seguridad informática.

Elaborado por: ***Vaca, P (2019)***

Descripción de la fase de Evaluación Inicial

6.7.1.2 Fase de Evaluación, Análisis de la situación inicial.

La meta que se persigue la fase de diagnóstico o evaluación inicial es de identificar la situación actual en temas de amenazas e identificación de los riesgos que existen en la Dirección Distrital Educación 23D01, referente a los requerimientos del modelo de gestión de la seguridad lógica de la información en la protección de los datos sensibles. Se recomienda utilizar el Anexo D del presente documento, acerca de los mecanismos y controles para reducir las vulnerabilidades existentes.

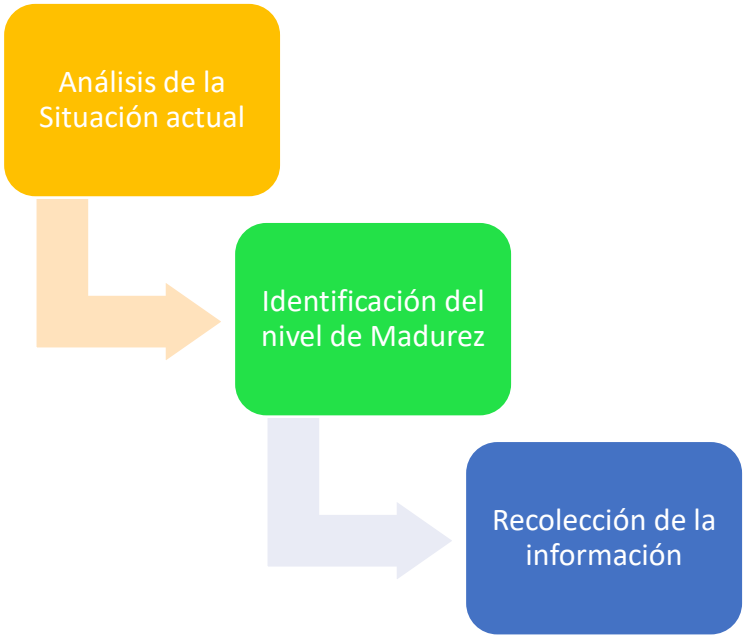


Figura 57 Subfase a cumplir en el diagnóstico.

Elaborado por: ***Vaca, P (2019)***

En la Tabla 52 se detalla la clasificación de la aplicación de los mecanismos de control de seguridad, en las que se les asigna una calificación según en el estado de la aplicación de un determinado mecanismo de control.

Tabla 52 Calificación de la aplicación de los mecanismos de control de seguridad

CALIFICACIÓN DE LOS MECANISMOS DE CONTROL	
Criterio	**Puntaje**
El control no aplica	N
El control es redundante	R
El control es efectivo, es clave y no se cumple o no se conoce	1
El control es efectivo, no es clave y no se cumple o no se conoce	2
El control no es efectivo y se cumple	3
El control es efectivo, no es clave y se cumple	4
El control es efectivo, es clave y se cumple	5

Elaborado por: Vaca, P (2019)
Fuente: (Martelo, Tovar, & Maza, 2018)

Por otra parte, existen metodologías que contribuyen en el análisis de la gestión de riesgos informáticos en los que se puede ver expuesta una organización. Estas metodologías se detallan en la Tabla 3 Metodologías empleadas en seguridad informática.

6.7.1.3 Fase de Planificación

En esta etapa se debe definir la estrategia a implementarse, con el objetivo de que se organice el trabajo a realizarse a partir de la información recogida en la fase de evaluación, llevándolas a la protección de la información sensible que existe en la Dirección Distrital Educación 23D01, de tal forma que se cumpla con las responsabilidades de seguridad lógica de la información. Es necesario recalcar que en esta fase se debe identificar los activos que se pretenden proteger y de que se intenta proteger.

Tabla 53 Resultado de la Fase de Planificación

Objetivo	Resultado	Instrumentos
Planificación	Entregable con la política de la privacidad, aprobada por el Directorio. Manual de políticas de seguridad y privacidad de los datos, debidamente autorizada y socializada al personal interno. Descripción de las funciones del personal en relación al tratamiento de la información. Procedimientos de privacidad. Plan de capacitación al personal de la organización.	Anexo A Política General.

Elaborado por: ***Vaca, P (2019)***

Además, en esta etapa se establecen los objetivos y procesos para llegar a obtener los resultados esperados por la organización. En esta fase se necesita por lo menos realizar las siguientes actividades:

1. Definir alcance y los objetivos de la gestión de datos personales.
2. Elaborar una política de gestión de datos personales.
3. Establecer las funciones y obligaciones de quienes traten los datos personales.

4. Elaborar un inventario de datos personales.
5. Analizar los riesgos a los que están sujetos los datos personales.
6. Identificar las medidas de seguridad.

Subfase I. Definir alcance y los objetivos de la gestión de datos personales.

El encargado del tratamiento de datos personales está en la obligación de definir los objetivos que se pretende cumplir en el proceso de gestión de datos personales. Se tiene que delimitar en que campos y escenarios de aplicación involucra el tratamiento de datos personales, detallados en la siguiente ilustración:

Figura 58 Subfase a cumplir en el diagnóstico.

Elaborado por: ***Vaca, P (2019)***

De la misma manera la regulación legislativa aplicable en este contexto, las obligaciones institucionales, el nivel de aceptación del riesgo y las necesidades propias de las partes interesadas.

Así mismo, el responsable de tratamiento de datos tendrá que considerar entre los objetivos que persigue el modelo aquellos que permitan el tratamiento veraz, informado y expresamente fiscalizado de la información personal, para que con esto se cumpla la garantía que tienen las personas en temas referentes a la privacidad especificado en el Artículo 178 del COIP y el consentimiento, el derecho a la transparencia y derecho de acceso detallados en los artículos 13, 20 y 21 respectivamente del anteproyecto presentado al Ministerio de Telecomunicaciones del Ecuador por la Dirección Nacional de Registro de Datos Personales (DINARDAP, 2019).

El objetivo se lo logra determinar mediante las siguientes sugerencias expuestas al encargado del tratamiento de datos:

Responsabilidad Contractual: Esta responsabilidad se da entre los acuerdos existentes entre los actores del tratamiento de datos y el flujo que tiene la información entre las distintas iteraciones existentes. A continuación, se da a conocer las distintas iteraciones y escenarios que pueden existir en el flujo de la información especificados en la figura 59 sobre el tratamiento de los datos sensibles que se manejan en la Dirección Distrital Educación 23D01:

Escenario 1: El titular entrega sus Datos Personales al responsable. Ejemplo: Esto se da cuando un usuario registra su información para recibir un servicio.

Escenario 2: El titular entrega sus datos al encargado. Ejemplo: Cuando se usa los datos personales de forma parcial o total en un contrato de servicio.

Escenario 3: El titular de los datos entrega sus datos al encargado. Ejemplo: cuando el dueño de los datos es atendido vía telefónica y proporciona sus datos.

Escenario 4: La persona responsable entrega la información al titular haciendo cumplir los artículos 21, 22, 23,24, que tratan de los derechos de Acceso,

Rectificación y Anulación, Eliminación, y Oposición respectivamente detallados en el anteproyecto de la ley de protección de datos enviados por la DINARDAP.

Escenario 5: El encargado de tratamiento de datos entrega los datos personales al titular basándose en los artículos 21,22,23 y 24 del anteproyecto de la ley de protección de datos.

Escenario 6: El responsable recibe los datos personales por parte del encargado, esto se da cuando existe la terminación de un contrato y estos datos migran hacia otro proveedor.

Escenario 7: Un responsable entrega los datos de un individuo a un tercero, este caso puede ser cuando existe una transferencia mediante un acuerdo de colaboración comercial.

Escenario 8: Un tercero recibe datos personales por parte del encargado, se da cuando el responsable indica que dichos datos sean transferidos.

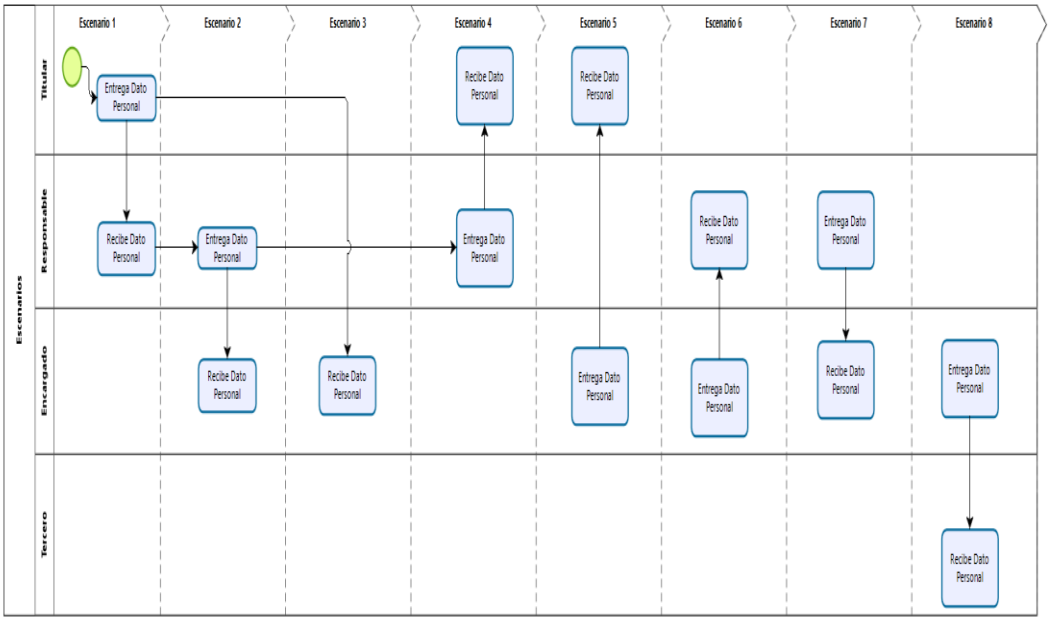


Figura 59 Flujo de tratamiento de Datos.

Elaborado por: ***Vaca, P (2019)***

Subfase II. Política de Aseguramiento y Protección de los Datos Sensibles

Luego de haber definido los objetivos y alcance del modelo la siguiente actividad a realizarse es definir e implementar una política de aseguramiento y protección de datos sensibles.

Es importante recalcar que se tiene que supervisar el cumplimiento de esta política, por parte del encargado del tratamiento de datos personales o a su vez por la alta dirección. La política debe ser clara y bien definida cumpliendo con los estándares de seguridad de la información, y estar acorde a lo dictaminado en la ley de protección de datos de los distintos reglamentos, constitución y leyes del Ecuador, además esta política debe ser de conocimiento general de todos los funcionarios de la Dirección Distrital Educación 23D01 y por lo menos se deben incluir los siguientes protocolos:

1. Dar cumplimiento de los artículos 1,2,3, 4 y 5 del anteproyecto de la ley LOPDP en los que se detallan: el Objeto, Finalidad, Ámbito de Aplicación Material, Ámbito de Aplicación Territorial y Ámbito de exclusión.
2. Realizar un correcto tratamiento y recopilación de datos personales enmarcados en aspectos establecidos por la ley.
3. Cumplir con los derechos que tiene el titular de los datos y cumpliendo con las exclusiones especificadas en el Artículo 5.
4. Hacer conocer al titular de los datos la finalidad que tiene recopilar sus datos personales y para que serán utilizados.
5. No adquirir datos personales por medios, métodos y técnicas no legales.
6. El tiempo que se conservan los datos personales en las bases de datos de la institución.
7. Supervisar de que se cumpla y se hagan cumplir estos principios.
8. Mantener la confidencialidad de los datos personales que reposan en las bases de datos del Mineduc.

Esta política se encuentra contenida en un documento (Anexo A) en el que se incluye la predisposición que los Directivos de la Dirección Distrital Educación 23D01 mantienen para brindar soporte en la implementación del modelo de seguridad de la información lógica de la institución.

Subfase III. Establecer las funciones y obligaciones de quienes traten los datos personales.

Figura 60 Funciones y obligaciones del personal que trata Datos Personales
Elaborado por: ***Vaca, P (2019)***

El responsable del tratamiento de datos personales es el que tiene que proporcionar y determinar los insumos correspondientes para establecer, implementar, administrar y brindar el respectivo mantenimiento al modelo de protección de datos. Para alinear los principios institucionales, con la protección de datos de manera correcta, el responsable de datos tiene que:

a) Establecer canales de comunicación con todos los usuarios entre ellos funcionarios, estudiantes, padres de familia y docentes en los que se dé a conocer la importancia de:
    a. Que se cumpla con la política de gestión de datos personales.
    b. Saber cuáles son los objetivos del modelo de gestión de protección de datos personales.

c. Que se entienda la importancia del mejoramiento de la protección de datos de manera continua.

b) Establecer los roles, responsabilidades y estructura organizacional para el manejo de datos personales.

c) Velar por que todos los funcionarios tengan asignados sus roles y funciones en el tratamiento de datos personales.

Subfase IV. Elaborar un inventario de datos personales.

Para que exista una buena gestión de datos personales, estos tienen que estar inventariados y categorizados según como son tratados por parte de la Dirección Distrital. De la misma manera estos datos tienen que ser especificados según el tratamiento al que son sometidos desde la obtención hasta la cancelación. En la siguiente tabla se detallan los niveles que cada uno de los datos suelen estar presentados.

Tabla 54 Categorías y descripción de los datos personales.

Categorías	Descripción	Ejemplo por tipo
Estándar	En este nivel se encuentran considerados datos de identificación básica de las personas que los muestra como identificada e identificable entre ellos se encuentran: nombres, edad, sexo, correo electrónico, estado civil, referencias personales, nivel académico, títulos, entre otros.	Datos de identificación y contacto
Sensible	En este grupo de datos se encuentran datos que permiten conocer la ubicación física de las personas, es decir, el lugar por en el que transitan dentro o fuera del país. Además, se encuentran datos que puedan dar a conocer estado de salud tanto del pasado como del presente o del futuro, origen racial o étnico, creencias religiosas, filosóficas y morales, movimientos sindicales y políticos, inclinaciones sexuales, o cualquier otro dato que conlleve a discriminación o sea un riesgo para la integridad de la persona. Por otra parte, datos que revelen: saldos bancarios, estados y números de cuenta, bienes e inmuebles, número de tarjeta de crédito o débito, contraseñas, información biométrica o datos que permitan acceder a bases de datos de los titulares.	Datos de ubicación física autenticación, salud, tratamiento jurídico, afiliación política y religiosa.
Especial	Dentro de este nivel se encuentran datos que puedan causar un daño significativo en la integridad física, económica o social de los titulares. Se encuentran: datos como número de tarjeta combinado con clave de la misma, fecha de vencimiento, así como datos de la banda magnética. Es necesario recalcar que en esta categoría también se tienen datos de titulares cuya profesión sea de alto riego debido a la jerarquía del cargo, haberes económicos, entre otros.	Titulares con cargos de alto riesgo, datos adicionales de las tarjetas de los titulares.

Elaborado por: ***Vaca, P (2019)***

Luego de que se hayan categorizado los datos personales como estándar, sensible, y especial, es importante definir la relación que estos tienen con el personal del Distrito. Con esto se logra identificar las áreas que necesitan de controles específicos de seguridad, así como la capacitación constante. De este modo, si es que existe algún tipo de solicitud de reclamo, actualización o actualización, se logre identificar quien fue exactamente el funcionario que dio tratamiento a esa información.

El cruce de información tiene que estar debidamente documentada, para lo cual se recomienda establecer una matriz ver Tabla 55 en la que se debe hacer constar el servidor público y que tipo de dato está a su cargo.

Tabla 55 Matriz de ejemplo del tratamiento de datos (funcionario-categoría de datos)

Departamentos	BDD Autoridades	BDD Docentes	BDD Estudiantes	BDD Comunidad Educativa
Dirección Distrital	UBC	UBC	UBC	UBC
Departamento Financiero		RAPD		
Departamento …X…	…	…	…	…

Elaborado por: ***Vaca, P (2019)***

En cuanto a lo que se describe en la tabla anterior cada una de las iniciales representan: (R) Recolección, (A) Almacenamiento, (U) Utilización, (B) Bloqueo, (C) Cancelación, (D) Divulgación de datos personales. Donde el Director Distrital puede hacer uso, bloquear y cancelar los datos personales de las autoridades, docentes, estudiantes y comunidad educativa.

Subfase V. Analizar los riesgos a los que están sujetos los datos personales

En este paso lo que se pretende determinar los riesgos a los que se encuentran sometidos los datos personales, en la mayoría de los casos se tendrá en mente que no se puede erradicarlos por completo, pero si se pueden mitigar las vulnerabilidades a los que se encuentran expuestos.

Para que se lleve a cabo la definición de un plan de los riesgos a tratar para que luego se implementen controles de seguridad, se tienen que establecer criterios de auditabilidad de los riesgos, lo que permite delimitar si un riesgo es aceptable según su impacto. De igual importancia es el factor del riesgo en base a los siguientes criterios:

Criterios de evaluación del riesgo

Es recomendable implementar criterios para la valoración del riesgo, ya que con esto se puede tener una perspectiva clara del riesgo existente en la seguridad de la información, basándose en los siguientes aspectos:

- El valor estratégico que tienen los datos para la Dirección Distrital Educación 23D01
- El nivel de criticidad que se encuentra involucrada la información.
- Los requerimientos establecidos por aspectos de legislación.
- El nivel de relevancia que tiene la triada CID, para la Dirección Distrital Educación 23D01.
- Las consecuencias y expectativas que tienen las consecuencias negativas para la Dirección Distrital Educación 23D01.

Criterios de impacto

Estos tipos de criterio se definen según el nivel de afectación y daño que puede causar al titular de los datos ocasionado por un evento negativo, entre los que se encuentran:

- El valor que representan los datos para la Dirección Distrital.
- El incumplimiento con los aspectos establecidos en la constitución y las leyes ecuatorianas de regulación de tratamiento de datos personales.
- Perjuicio en la integridad de los titulares.
- Daño a la reputación de la Dirección Distrital.

Criterios de aceptación del riesgo

En este punto la Dirección Distrital Educación 23D01 puede o no aceptar ciertos tipos de riesgo, pero siempre en base a: la naturaleza del riesgo, la consecuencia y el grado de probabilidad que pueden ser consideradas como muy significativos. Estos criterios dependen en su gran mayoría de las políticas, objetivos y metas de la Dirección Distrital Educación 23D01.

Los criterios de aceptación del riesgo se pueden expresar según el beneficio o el grado estimado que representa el riesgo. Esto se puede dar por ejemplo si es que la Dirección Distrital decide incumplir con lo establecido en la Constitución del Ecuador.

Hay que mencionar, además que dentro de los criterios de aceptación del riesgo pueden hacer constar requisitos en los que se pretenda una gestión futura. Sucede esto cuando en el Directorio existe el compromiso de aceptar un riesgo, pero poder mitigarlo en un futuro.

Por último, cuando se pretenda tomar cualquier criterio de aceptación del riesgo es necesario considerar:

- Políticas del tratamiento de datos personales.
- Legislación nacional y reglamentos regulatorios.
- Aspectos Operacionales.
- Tecnología.
- Presupuesto.

Valoración en relación al Riesgo

Una vez definido los criterios de aceptación del riesgo, el siguiente paso es realizar una valoración del riesgo en los que se identifica los activos con los que cuenta la organización, las vulnerabilidades existentes y los escenarios en los que se pueden ver comprometido los datos.

Inventario de los activos

Para la Dirección Distrital Educación 23D01 un activo es cualquier valor que necesita ser protegido. En las organizaciones los activos se pueden clasificar en:

- **Activos de Información:** en los que se hace constar la información relacionada a los datos personales y de los procesos propios que se realizan en la Dirección Distrital.
- **Activos de apoyo:** son los activos en los que se almacenan los activos de información, entre estos se tienen: hardware, software, redes informáticas, personal e infraestructura adicional.

Determinar las amenazas

Teniendo en cuenta que una amenaza cuenta con la posibilidad de afectar a un activo y de la misma manera causar una vulnerabilidad, estas amenazas tienen su origen natural o causado por el hombre de manera accidental o provocadas con malas intenciones, además estas pueden generarse dentro o fuera de la Dirección Distrital.

Es importante recalcar que los responsables departamentales deben proporcionar a los usuarios de los sistemas de información, planes de capacitación para que estos sepan como identificar y valorar las amenazas existentes con los datos, en el Anexo B se tiene una lista de las principales amenazas de las cuales se puede ver comprometida una organización.

Determinar las vulnerabilidades

Dando cumplimiento a lo expuesto en el Artículo 38 del anteproyecto de la LOPDP del Ecuador sobre el análisis de riesgos y determinación de niveles de seguridad aplicables, se tiene que todo tipo de vulnerabilidad puede presentarse de distinta manera y estas se las logra identificar dentro de las organizaciones, en el manejo de los datos por parte de los funcionarios, en la configuración y falta de actualización de los sistemas de información, en el mal uso del hardware, en la relación que existe con terceros, entre otros.

Aunque una vulnerabilidad por sí sola no puede causar ningún daño, pero cuando alguien la descubre y la explota puede existir fuga de datos y entre ellas datos sensibles, en el Anexo C se describen una lista de vulnerabilidades relacionadas con las amenazas.

Identificar los escenarios vulnerables y criticidad

Según lo expuesto en los Artículos 17 y 36 del Anteproyecto de la LOPDP el responsable de los datos, se ve en la obligación de implementar procesos de verificación, evaluación y valoración constante de la eficiencia, eficacia y efectividad de las herramientas empleadas tanto en los ámbitos: físico, técnico, operativo y jurídico con el que se brinde garantía a la seguridad del tratamiento. Así se tiene que, en cuanto a la verificación, evaluación y valoración de los escenarios con vulnerabilidad, esto se da cuando una amenaza explota cierta vulnerabilidad y logra apoderarse de los datos personales.

Una vez ya conocido los activos de información y los controles que la Dirección Distrital Educación 23D01 cuenta, con estos preceptos el encargado del tratamiento de datos puede realizar una estimación de los escenarios cuyo nivel de criticidad necesite de mecanismos de mitigación de riesgos sabiendo que el riesgo es la combinación perfecta entre la amenaza, vulnerabilidad y la criticidad a la que este lleve a la organización en cuanto a la protección de datos personales.

Subfase VI. Verificación de los mecanismos de seguridad y análisis de la brecha

En el Articulo 52 literal 2 del Anteproyecto de la LOPDP del Ecuador menciona que el responsable del tratamiento de datos personales está obligado a aplicar e implementar requisitos y herramientas administrativas, técnicas, fiscas organizativas a fin de garantizar el correcto tratamiento de datos.

En el Anexo D, se detallan una gran variedad de mecanismos de seguridad con los cuales la Dirección Distrital Educación 23D01 puede mitigar a los riesgos basándose en los siguientes dominios:

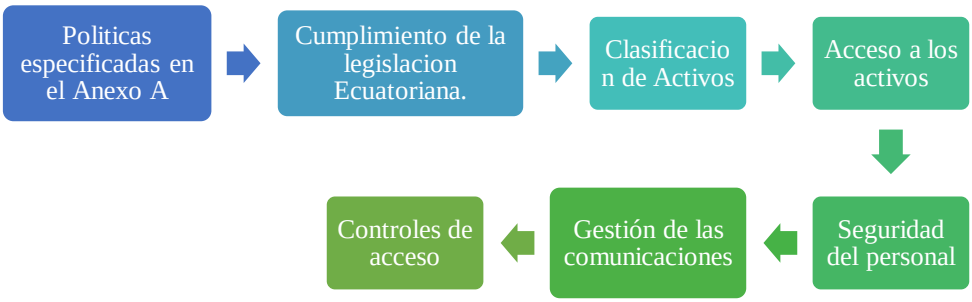


Figura 61 Dominios en la mitigación de riesgos en el tratamiento de datos personales.

Elaborado por: ***Vaca, P (2019)***

Cuando ya se hayan analizado e identificado los activos y los procesos referentes al tratamiento de datos personales, de igual manera las amenazas, vulnerabilidades y escenarios, el siguiente paso es el análisis de la brecha.

El análisis de la brecha se basa en identificar los mecanismos de control que se tienen para determinado riesgo identificado, así como cuales son los que operan a la perfección y en caso de existir fallos, elegir cuales de los controles se tienen que reemplazar para determinada amenaza o vulnerabilidad.

Figura 62 Análisis de brecha

Elaborado por: ***Vaca, P (2019)***

Resumen de la fase de Planificación

Con el fin de facilitar la aplicación del modelo en la primera fase, se detalla un diagrama en el cual se hacen constar los procesos que intervienen en cada una de las Subfases explicadas en la Figura 63:

- Definir alcance y objetivos.
- Elaborar una política de gestión de datos personales.
- Establecer funciones y obligaciones de los servidores que tratan datos personales.
- Elaborar un inventario de datos personales.
- Analizar los riesgos a los que están sujetos los datos personales.
- Identificar las medidas de seguridad en los datos personales.

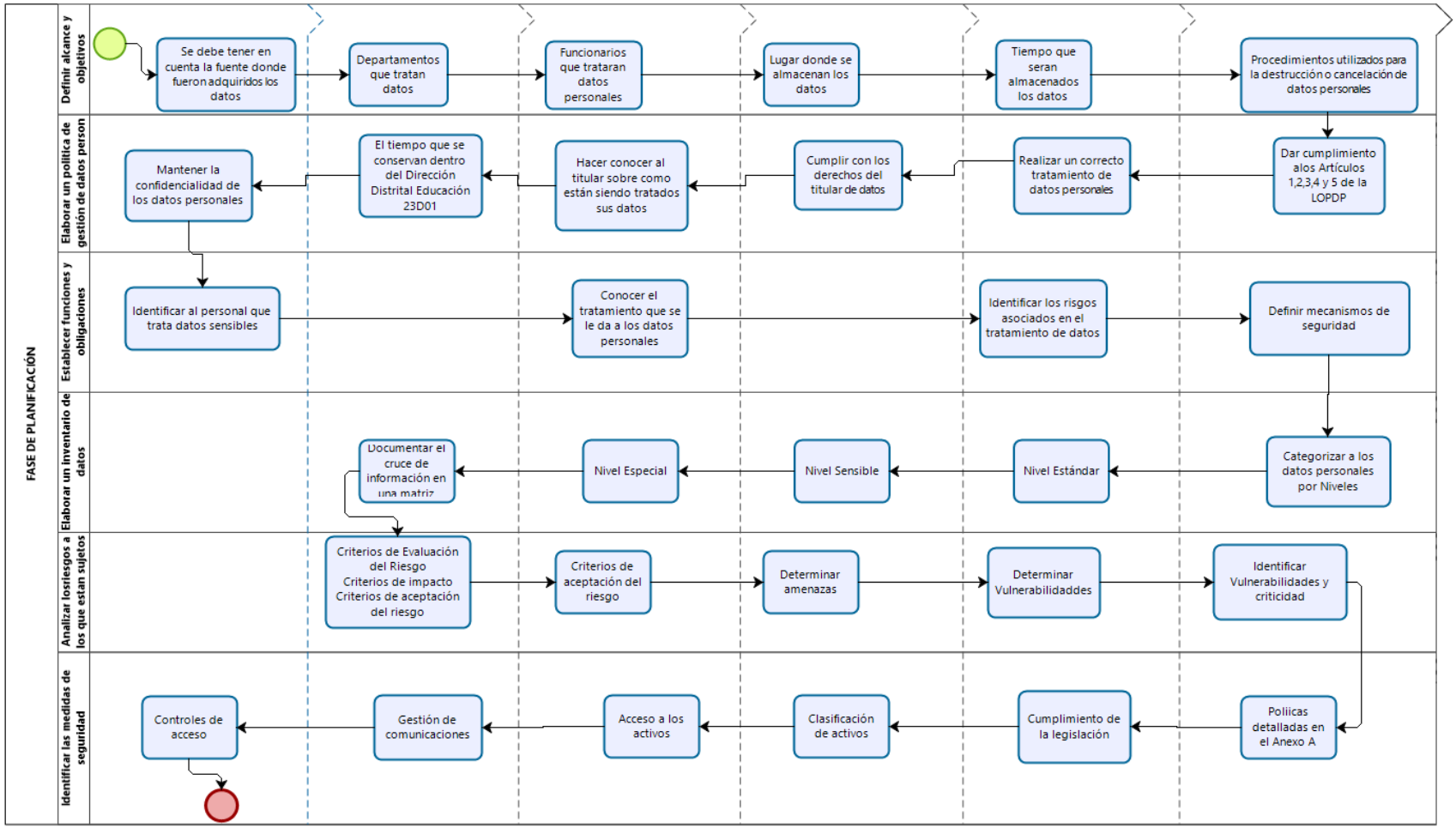


Figura 63 Resumen de la Fase I

Elaborado por: ***Vaca, P (2019)***

6.7.1.4 Fase de Implementación del modelo de gestión de seguridad de la información

En esta fase se implementarán y se pondrá en marcha las políticas, procesos, procedimientos y mecanismos de control resultantes del análisis de riesgos ejecutados en la primera fase.

Subfase VII. Implementación de los mecanismos de seguridad aplicables a los Datos Personales.

Para el cumplimiento de la implementación de los mecanismos de seguridad, la Dirección Distrital deberá asignar a un responsable que será el encargado de la rendición de cuentas de la gestión del tratamiento de datos personales. Además, entre otras funciones tendrá que cumplir con las siguientes funciones:

- Será el encargado de que se cumpla con las políticas de seguridad aprobadas por el Directorio de la Dirección Distrital.
- Tendrá que poner en marcha y revisar que las políticas se las cumpla sin excepciones.
- Garantizará que se implementen dichas políticas de protección de los datos sensibles que se alojan en los servidores de la Dirección Distrital.
- Revisará que se esté cumpliendo con la gestión de las políticas.
- Buscará medios de capacitación hacia los servidores públicos en el tratamiento de los datos sensibles.
- Aprobará los procedimientos en los que se vean involucrados el tratamiento de datos sensibles, entre ellos:
    - Manejo y comunicación de noticias de privacidad.
    - Administración y recepción de solicitudes de cumplimiento de derechos del tratamiento de datos sensibles.
    - Gestión de la recepción segura y legal de los datos personales.
    - Gestión de casos en los que se vean expuestos los datos sensibles.
    - Aprobación de contratos de terceros en los que intervengan datos de carácter sensible.
- Manejo y gestión de riesgos de los datos sensibles.

- Interpretación de las excepciones del tratamiento de datos sensibles según lo expuesto en la legislación ecuatoriana.
- Mantener actualizada a la organización en temas legales del tratamiento de datos personales.
- Implementar buenas prácticas de tratamiento de datos personales.

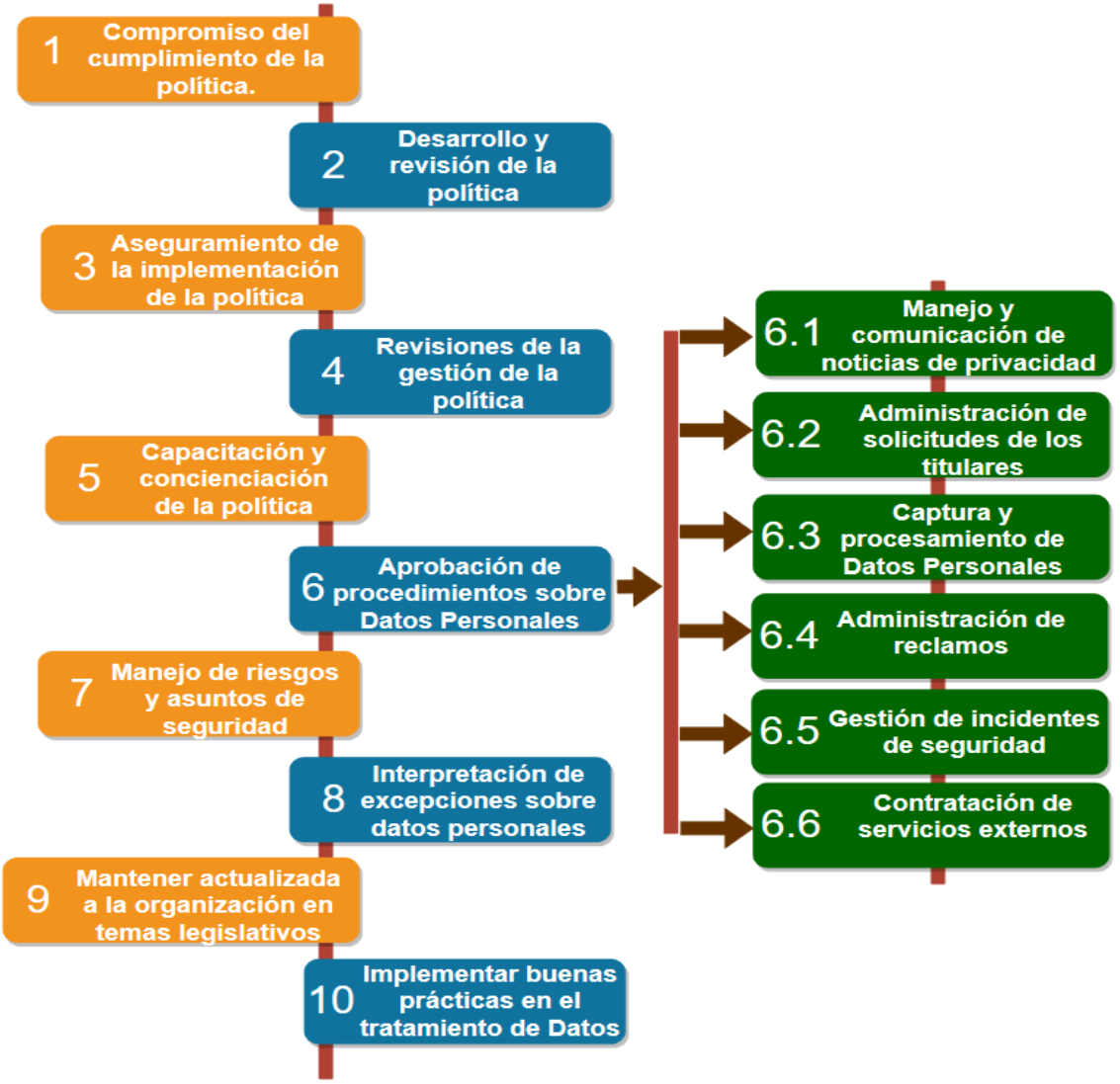


Figura 64 Implementación de los mecanismos aplicados a los Datos Personales
Elaborado por: ***Vaca, P (2019)***

Procedimientos para implementación de los mecanismos de seguridad

A continuación, se detallan los procedimientos a implementarse a partir de las políticas y mecanismos de control que se seleccionaron en la fase anterior para la mitigación de vulnerabilidades identificadas.

Estos procedimientos fueron tomados de la lista de controles que la norma ISO/IEC 27001 recomienda como uso de buenas prácticas en el proceso de protección de datos personales y de la seguridad de la información.

En la siguiente Figura se detallan los documentos que se generan a partir del desarrollo de la Fase II.

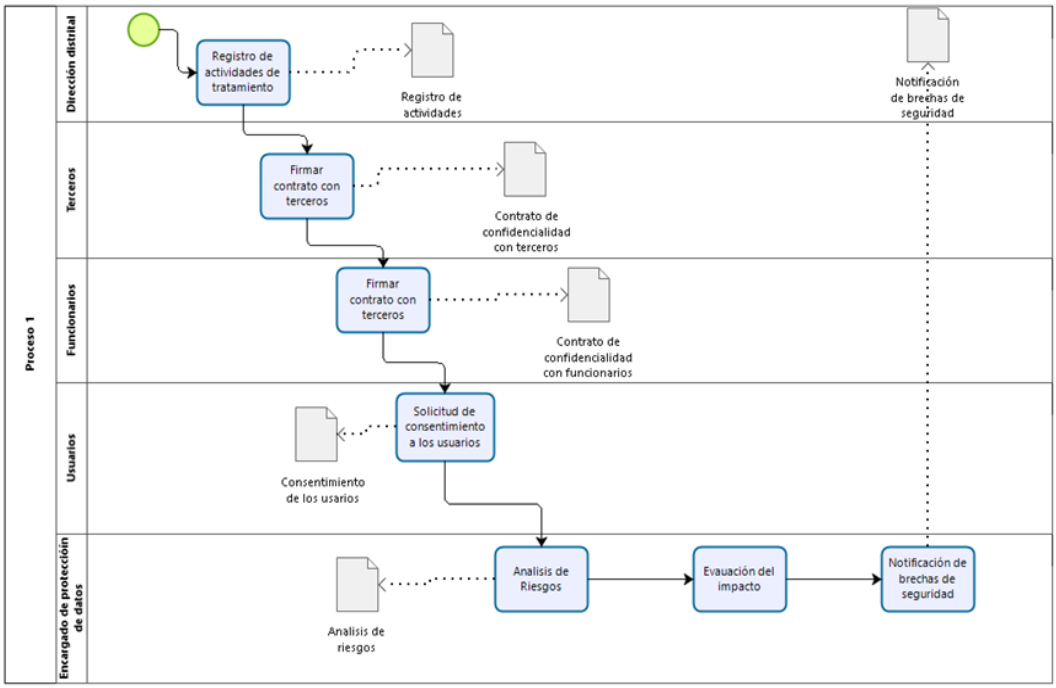


Figura 65 Documentos generados en la fase de implementación.

Elaborado por: ***Vaca, P (2019)***

Es importante documentar las actividades realizadas en el tratamiento de datos personales, debido a que, si existiera una brecha de seguridad, se cuente con los documentos necesarios que servirán de descargo para responder ante cualquier acción legal.

En la tabla se detallan el anexo correspondiente a cada documento que se generará en la implementación de la Fase II.

Tabla 56 Detalle de los instrumentos a utilizarse en la fase de implementación.

Objetivo	Resultado	Instrumentos
Implementación	Documento con guía detallada para la protección de datos en centros educativos.	Anexo E. Registro de Actividades.

	Documento modelo de contrato de confidencialidad con terceros.	Anexo F. Contrato de confidencialidad con terceros.
	Documento modelo de contrato de confidencialidad con funcionarios.	Anexo G. Contrato de confidencialidad con funcionarios.
	Documento con firmas de consentimiento de tratamiento de sus datos personales.	Anexo H. Contrato de consentimiento de los usuarios.
	Documento modelo para el análisis de riesgos.	Anexo I. Análisis de riesgos.
	Documento con notificación de brechas de seguridad.	Anexo J. Notificación de brechas de seguridad.

Elaborado por: Vaca, P (2019)

6.7.1.5 Fase de evaluación y monitoreo del modelo

Luego de aplicar las fases y Subfases anteriores con sus respectivos procedimientos y actividades, el paso siguiente es evaluar y medir la efectividad de las políticas, planes y procedimientos implementados, con el objetivo de que se haya conseguido la mejora planificada.

Subfase VIII. Revisiones de los factores de riesgo y auditoria.

Es recomendable que en la organización se realice el monitoreo constante de los riesgos y sus factores relacionados, debido a que estos son subjetivos y cambian sin ninguna notificación, y aparecen en escenarios críticos aun cuando ya se los creía mitigados.

Además, es recomendable que se tome en cuenta los siguientes aspectos a fin de que se garantice el monitoreo de los factores de riesgo:

- Activos informáticos que han sido adquiridos tienen que se ser incluidos en los alcances de gestión de riesgo.
- Migración o cambio de nuevas tecnologías.
- Amenazas nuevas que hayan aparecido interna o externamente y que no han sido consideradas en la valoración del riesgo.
- Posibilidad de que nuevas vulnerabilidades sean explotadas.
- Incidentes nuevos y vulneraciones de seguridad.

Por otra parte, se tiene que contar con un programa de auditoría interna con la finalidad de monitorear y revisar el cumplimiento del modelo. Además, se recomienda entes externos de auditoria a fin de que se quiera llegar a una certificación en seguridad de la información.

En la aplicación de la auditoria pueden surgir nuevos riesgos y vulnerabilidades que pueden ser explotadas, de ser así, es recomendable aplicar medidas preventivas para mitigar dichas amenazas.

De otro modo, si es que en la aplicación de la auditoria existe algún tipo de vulnerabilidad explotada se tiene que notificar como se menciona en el Anteproyecto de LOPDP Artículo 39, "***Notificación de vulnerabilidad.*** *- En caso de violación a las seguridades y establecidas o de filtración de datos personales el responsable del tratamiento deberá notificar a la autoridad de control hasta 72 horas después de tener conocimiento de ella".*

6.7.1.6 Actuar (mejorar el performance del modelo)

Subfase IX Mejora Continua y capacitación

En esta fase se adoptan las medidas correctivas en función de los resultados obtenidos en la fase de auditoria, con la finalidad de conseguir la mejora continua. Además, para conseguir esta mejora es fundamental la capacitación a los funcionarios de la Dirección Distrital Educación 23D01.

Es importante tener en cuenta los siguientes aspectos que intervienen en el proceso de mejora:

Acciones correctivas: Este tipo de acciones van enfocadas a eliminar las fallas causadas por la explotación de las amenazas.

Figura 66 Acciones correctivas Fase de Mejora Continua

Elaborado por: ***Vaca, P (2019)***

Acciones Preventivas: Constituyen un conjunto de acciones que sirven para identificar las posibles vulnerabilidades que desencadenan en la explotación de las amenazas potencialmente relevantes.

Capacitación: Es importante que dentro de las acciones preventivas se incluyan planes de capacitación que sirvan para concientizar a los servidores públicos. De otra manera los programas de capacitación deben incluir temas como muestran en la siguiente Figura.

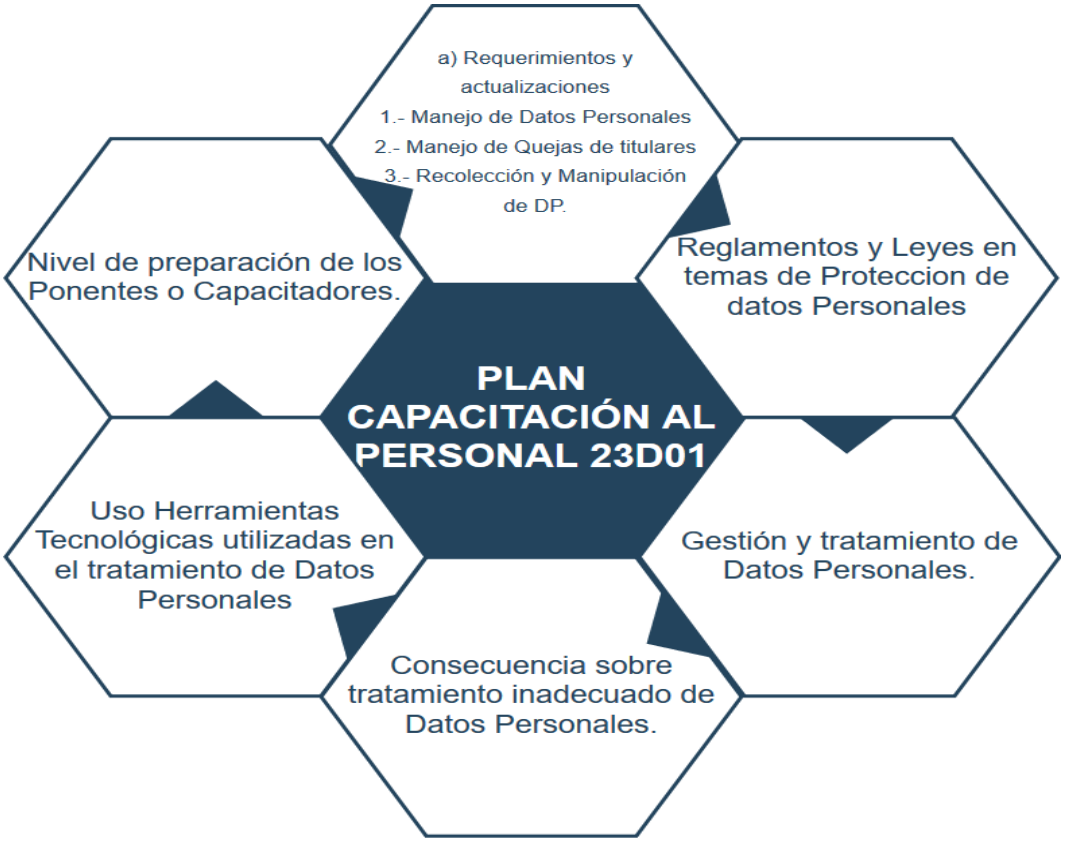


Figura 67 Aspectos a tener en cuenta en temas de capacitación

Elaborado por: ***Vaca, P (2019)***

Por tal razón estos planes de capacitación tienen que estar enfocados en aspectos como:

- **Concienciación:** Establecer planes periódicos y con una distancia reducida de tiempo en temas de difusión sobre la protección de datos personales.
- **Entrenamiento:** Establecer planes a mediano plazo con la finalidad de capacitar al personal en temas de seguridad y protección de datos personal.
- **Cambio cultural en temas de seguridad informática:** Establecer planes a largo plazo con el objetivo cambiar culturalmente al personal en temas de seguridad.

Es importante realizar un diagnóstico inicial para saber qué temas de capacitación se tienen que abordar con la finalidad de mejorar el tratamiento de datos personales.

6.7.2 Validación del modelo

Con el objetivo de validar el cumplimiento y correcto funcionamiento del modelo planteado, y en base a los datos obtenidos en la tabla anterior, se procede a realizar el proceso de simulación de la implementación del modelo, que a continuación se detalla:

6.7.2.1 Aplicación de la fase de Evaluación Inicial

Dando uso al Anexo D del presente modelo se procedió a evaluar la situación actual en la DD23D01 Educación, le que permite conocer cómo los usuarios de los sistemas de información tratan los datos personales, teniendo los siguientes resultados:

Tabla 57 Evaluación inicial mediante el Anexo D Mecanismos y Controles para reducir vulnerabilidades.

Id	Objetivo de control	Puntaje esperado	Puntaje Obtenido
1	Políticas de gestión de datos personales.	5	1
2	Monitoreo y Evaluación.	5	N
3	Identificación la legislación aplicable.	5	1
4	Registros de evidencia	5	1
5	Recolección de evidencia.	5	1
6	Revisión del cumplimiento técnico.	5	1
7	Inventario y clasificación de los datos personales	5	4
8	Inventarios de activos	5	4
9	Identificación del ciclo de vida de un dato en la Dirección Distrital.	5	1
10	Identificar responsabilidades de cada funcionario de la Dirección Distrital.	5	1
11	Acuerdo de confidencialidad.	5	1
12	Capacitación.	5	1
13	Proceso disciplinario.	5	1
14	Control perimetral	5	4
15	Seguridad de cableado	5	1
16	Control de los activos fuera de las instalaciones	5	1
17	Destrucción segura de la información.	5	1
18	Escritorio limpio	5	1
19	Control ante robo	5	1
20	Control de cambios operacionales.	5	1
21	Segregación de tareas	5	1

22	Protección ante malware	5	4
23	Registros y auditorías a los funcionarios	5	1
24	Controles de Red	5	1
25	Administración de medios de almacenamiento secundario.	5	1
26	Seguridad de medios que son movilizados	5	1
27	Manejo de correo electrónico y mensajería instantánea.	5	1
28	Disociación de datos	5	1
29	Normas de control de acceso	5	1
30	Manejo de usuarios y claves de seguridad	5	1
31	Computadores que dejen de usarse	5	1
32	Accesos externos a sistemas de información	5	N
33	Segregación de redes	5	N
34	Controles de inicio de sesión	5	3
35	Trazabilidad de tratamiento	5	3
36	Asilamiento de datos sensibles	5	1
37	Uso de dispositivos móviles internos.	5	1
38	Autenticación de segundo factor de autenticación mediante tokens TOTP (Time One- Time Password)	5	1
39	Cifrado	5	N
40	Firmas Electrónicas	5	N
41	Procedimientos para el manejo de incidentes	5	1
42	Procedimientos en caso de incidentes.	5	1
43	Reportes de incidentes de seguridad	5	1
44	Reporte de fallo en funcionamiento	5	1
45	Procedimientos de notificación de vulnerabilidades a los titulares de datos.	5	1
46	Aprendizaje de incidentes	5	1
47	Procedimientos de actualización del modelo de gestión	5	1

Elaborado por: Vaca, P (2019).

El cálculo se lo realizo dividendo el puntaje obtenido entre el puntaje esperado teniendo un porcentaje de cumplimiento del 25% de los mecanismos y controles que se necesitan para salvaguardar los datos personales.

$$\%\ \boldsymbol{Cumplimiento} = \frac{\sum Puntaje\ obtenido}{\sum Puntaje\ esperado}$$

$$\%\ \boldsymbol{Cumplimiento} = \frac{58}{235}$$

$$\%\ \boldsymbol{Cumplimiento} = 25\%$$

6.7.2.2 Aplicación de la fase de Planificación

Subfase I. Definir Alcance y los objetivos de la gestión de datos personales.

Alcance

La aplicación del presente modelo se pretende salvaguardar los datos sensibles que se capturan procesan y distribuyen en la Unidad de Apoyo a la Inclusión, específicamente en los tramites (DENUNCIAS, COBROS INDEBIDOS, LESIONES, DELITOS SEXUALES, MALTRATO PSICOLOGICO, INSTITUCIONES PARTICULARES, ABUSO DE AUTORIDAD, DROGAS).

Objetivos

Proteger los datos sensibles que se capturan, procesan y distribuyen en la Unidad de Asesoría Jurídica.

Subfase II. Políticas de aseguramiento y protección de datos sensibles.

Basándose en las políticas expuestas en el anexo A, se procede a difundir tanto al jefe de unidad como a los funcionarios pertenecientes a esta unidad.

Subfase III. Establecer las funciones y obligaciones de quienes traten los datos personales.

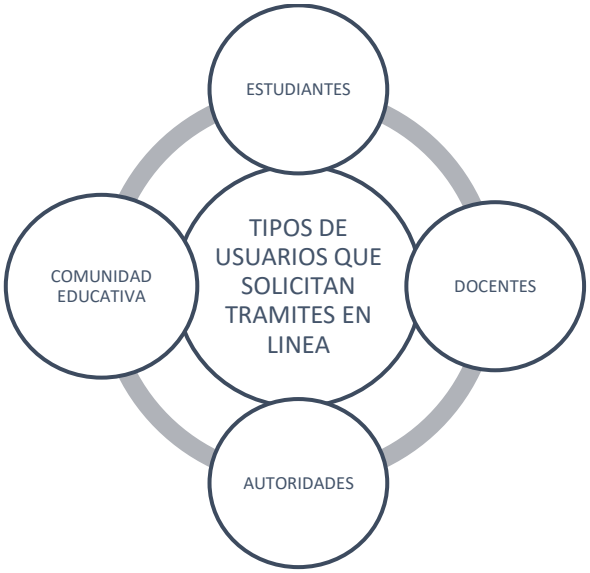


Figura 68 Tipos de usuarios que solicitan tramites ciudadanos

Fuente: (MINEDUC,2017)

La Dirección Distrital de Educación debe contar con un inventario de las bases de datos con las que cuenta, mantener un registro que tipo de datos e información reposan sobre estas. Por ejemplo, datos de los funcionarios, padres de familia, datos de estudiantes, docentes, autoridades. De la misma manera el lugar en el que están siendo almacenados los datos, sean estos, servidores, dispositivos móviles, en la nube, entre otros, así como su ubicación geográfica.

En la siguiente tabla se detallan las funciones y responsabilidades que deben cumplir los jefes departamentales de la Dirección Distrital Educación 23D01 de la Ciudad de Santo Domingo.

Tabla 58 Funciones y responsabilidades sobre el tratamiento de datos según el departamento.

Actividades	Director Distrital	U. Atención Ciudadana	U. Apoyo y Seguimiento	UDAI	DECE	U. Talento Humano.	U. Planificación	U. TICS	U. Administración Escolar.	U. Gestión de Riesgos	U. Asesoría Juridica	U. Administrativo Finaciero	U. Financiero
Políticas y objetivos del modelo de gestión de datos personales	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Funciones y obligaciones	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Análisis de riesgos de Datos Personales	✔							✔					
Implementación de Medidas de Seguridad	✔							✔					
Revisiones y auditoria	✔							✔					
Formación continua	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Elaborado por: ***Vaca, P (2019)***

Subfase IV. Elaborar un inventario de datos personales.

Categorización, evaluación de riesgos de los datos y activos de la Dirección Distrital Educación 23D01

Los datos personales que se capturan en la DD23D01, se rigen por lo establecido en la constitución del Ecuador, COIP y demás entes regulatorios de la protección de la intimidad de la información de los ciudadanos. Por otra parte, las medidas de seguridad a aplicarse en la protección de datos deben basarse en el inventario realizado por el encargado del tratamiento de datos, con la finalidad de no realizar esfuerzos y uso de mecanismos en escenarios que no se requieren salvaguardar datos que según su tipología pueden ser de carácter público.

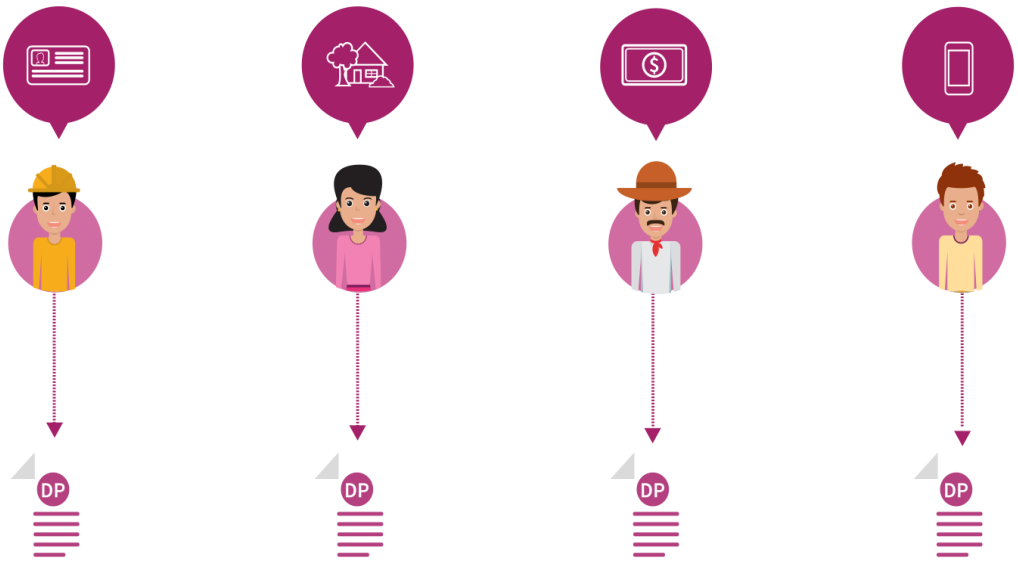


Figura 69 Categorización de Datos Personales

Fuente: (Instituto de Transparencia, Acceso a la Información Pública, 2019)

En la siguiente tabla se muestra el inventario de datos personales que se recaban en la DD23D01, de la misma forma se detalla el nivel de seguridad al que se encuentran expuestos que van desde el nivel estándar, sensible y especial.

Tabla 59 Categorización de los datos que se capturan en la Dirección Distrital 23D01

Ubicación del Sistema	Nombre del Sistema	Documentos y Datos Personales recabados	Medio a través del cual se obtienen los datos	Finalidades del tratamiento	Tipos de datos	Servidores públicos que tienen acceso	Nivel de seguridad
Unidad Atención Ciudadana	Módulo de Gestión de Atención Ciudadana (Mogac)	Número de documento de identidad de la persona que solicita el trámite.	Electrónico	**CERTIFICADO DE REMUNERACIONES**: Legalizar de forma ágil y oportuna las remuneraciones del docente y/o funcionario solicitante	Identificación No se recaban datos sensibles.	Docente / Autoridad	**Estándar**
	Mogac	Número de documento de identidad de la persona que solicita el trámite.	Electrónico	**CERTIFICADO DE TIEMPO DE SERVICIO:** Emitir un certificado en el que se demuestre que el docente no consta en el sumario administrativo y no haya sido sancionado acorde a los lineamientos del marco legal educativo**.**	Identificación No se recaban datos sensibles.	Docente / Autoridad	**Estándar**

Unidad de Apoyo Seguimiento y Regulación	CAS – ASRE MOGAC	- Número de documento de identidad de la persona que solicita el trámite - Número de cédula del representante legal o padre de familia - Número de cédula del estudiante (si lo tuviera) o nombres completos - Planilla de energía eléctrica del domicilio del estudiante. - Libreta de cualquier parcial del último año escolar		**TRASLADO DE ESTUDIANTES DE IE FISCAL A IE FISCAL:** Realizar el traslado del estudiante a otra Institución Educativa del mismo régimen escolar.	Identificación Código Único Eléctrico	Docente / Autoridad/ Estudiante	**Estándar**
UDAI	QUIPUX DROPBOX GOOGLE DRIVE	- Número de identificación del estudiante. - Datos de menores de edad. - Certificado o carné de discapacidad. - Certificado Médico - Datos sobre discapacidad del estudiante. - Porcentaje de discapacidad del estudiante	Electrónico	- Facilitar la inclusión de los niños, niñas y adolescentes con necesidades educativas especiales asociadas o no a una discapacidad, con preferencia de atención a quienes se encuentran en situación o riesgo de exclusión, marginación o de abandono del proceso. - Desarrollar lineamientos de orientación psicopedagógica y de sensibilización para: docentes, padres de familia y estudiantes.	Identificación Porcentaje de discapacidad	- Analista Udai	**Especial**
DECE	MOGAC	DENUNCIAS (COBROS INDEBIDOS, LESIONES, DELITOS SEXUALES, MALTRATO PSICOLOGICO, INSTITUCIONES PARTICULARES, ABUSO DE AUTORIDAD, DROGAS)	Electrónico	Establecer y estandarizar los procesos de denuncias mediante una atención adecuada del marco legal educativo, entregando un mejor servicio al ciudadano con la oportuna respuesta a lo solicitado	Identificación Denuncia escrita digital Fotografías. Copias de facturas.	Jefe departamental/ Autoridad	**Especial**
Unidad de Talento Humano	SGCD – TTHH MOGAC	- Número de documento de identidad de la persona que solicita el trámite.	Electrónico	**CERTIFICADO DE TIEMPO DE SERVICIO:** Otorgar de manera oportuna el certificado solicitado por el docente	Identificación No se recaban datos sensibles.	Docente / Jefe departamental/ Autoridad	**Estándar**

		- Número de documento de identidad de la persona que solicita el trámite.	Electrónico	**CERTIFICADO DE NO ESTAR INMERSO EN SUMARIO ADMINISTRATIVO Y DE NO HABER SIDO SANCIONADO:** Emitir un certificado en el que se demuestre que el docente no consta en el sumario administrativo y no haya sido sancionado acorde a los lineamientos del marco legal educativo.	Identificación Según sea el caso se pueden entregar datos sensibles.	Docente / Jefe departamental/ Autoridad	**Sensible**
		- Número de documento de identidad de la persona que solicita el trámite - Solicitud de Permisos y Licencias aprobado por la Autoridad de la Institución Educativa Documento habilitante, según tipo de Permiso y/o Licencia: - Certificado Médico - Acta de Matrimonio - Acta de Defunción	Electrónico	**SOLICITUD DE PERMISOS Y LICENCIAS:** Proveer al funcionario docente o administrativo un tiempo específico para el bienestar personal según su requerimiento, cumpliendo con las leyes para este efecto.	Identificación Fecha y lugar de registro matrimonio. Datos de relacionados a la salud del titular. Según sea el caso se pueden entregar datos sensibles.	Docente / Jefe departamental/ Autoridad	**Sensible**

		|- Número de documento de identidad de la persona que solicita el trámite - Carta de renuncia dirigida al Director(a) Distrital. - Acta de entrega recepción de documentos receptada por el Director/Rector. (En caso de Unidocentes deberá entregar los bienes y/o documentos al Distrito). - Documento Paz y Salvo firmado por el Director/Rector. (En caso de Unidocentes deberá realizar el Paz y Salvo al Distrito).	Electrónico	**RENUNCIAS:** Determinar un procedimiento consistente que permita realizar la separación voluntaria del personal de la Institución Educativa y que se encuentre alineado a la legislación vigente.	Identificación Fecha de ingreso y salida al Mineduc. Última Remuneración. Dirección de vivienda. Correo electrónico. Teléfono convencional. Teléfono celular Datos de la Unidad donde prestaba sus servicios.	Docente / Jefe departamental/ Autoridad	**Sensible**

		- Número de documento de identidad de la persona que solicita el trámite - Oficio del docente indicando la causa por la que se solicita el traslado del docente. - Certificado médico emitido por el IESS, en el cual se certifique que el docente o su hijo menor de edad bajo su cuidado, adolece de una enfermedad catastrófica o de alta complejidad y que requieran vivir cerca de un centro de salud para recibir atención médica especializada, y que necesita un tratamiento mayor a 180 días. - Resolución de autorización de traslado del docente por bienestar social - Acción de personal.	Electrónico.	**TRASLADO DE DOCENTES POR BIENESTAR SOCIAL:** Autorizar el traslado a aquellos docentes en funciones que requieren cambiar su lugar de trabajo, con el carácter de urgente, por adolecer ellos o sus hijos menores de edad bajo su cuidado, de una enfermedad catastrófica o de alta complejidad y que requieren vivir cerca de un centro de salud para recibir atención médica especializada	Identificación Dirección de vivienda. Correo electrónico. Teléfono convencional. Teléfono celular Datos de Enfermedades catastróficas, raras o huérfanas, según Ministerio de Salud Pública	Docente/ Jefe departamental/ Autoridad	**Especial**
Unidad de Administración Escolar	MOGAC	-Número de documento de identidad de la persona que solicita el trámite -Oficio indicando el mantenimiento solicitado en la Institución Educativa.	Electrónico	ACEPTACIÓN DE LA PROPUESTA DEL PLAN DE GESTIÓN DE RIESGOS PARA IE PARTICULARES, FISCOMISIONALES Y MUNICIPALES	Identificación	Institución Educativa	**Estándar**
Unidad de Asesoría Jurídica	MOGAC	DENUNCIAS (COBROS INDEBIDOS, LESIONES, DELITOS SEXUALES, MALTRATO PSICOLOGICO, INSTITUCIONES PARTICULARES, ABUSO DE AUTORIDAD, DROGAS)	Electrónico	Establecer y estandarizar los procesos de denuncias mediante una atención adecuada del marco legal educativo, entregando un mejor servicio al ciudadano con la oportuna respuesta a lo solicitado	• Identificación • Denuncia escrita digital • Fotografías. • Copias de facturas.	Jefe departamental/ Autoridad	**Especial**
Unidad Administrativo Financiero	Mogac Esigef	Número de documento de identidad de la persona que solicita el trámite.	Electrónico	**CERTIFICADO DE REMUNERACIONES**: Legalizar de forma ágil y oportuna las remuneraciones del docente y/o funcionario solicitante	• Identificación No se recaban datos sensibles.	Docente / Autoridad	**Estándar**

Elaborado por: ***Vaca, P (2019)***

Subfase V. Analizar los riesgos a los que están sujetos los datos personales

Tomando como referencia el Anexo I del presente documento se procede a realizar el análisis de riesgos a los que están expuestos los datos personales, para ello se aplicó una encuesta de categorización de datos personales aplicada al Ingeniero Fabricio Zavala, director del departamento de Tecnologías de la información y Comunicación de la DD23D01 Educación de la ciudad de Santo Domingo.

Tabla 60 Aplicación de cuestionario para analizar los riesgos a los que están sujetos los datos personales

Preguntas	Respuestas
FINALIDADES DE TRATAMIENTO	
¿En este proceso se van a tratar datos personales?	Si
¿En el proceso de captura de datos existen datos que van a ser tratados a gran escala? Por favor, detalle los puntos indicados en los siguientes ítems para determinar si se trata de un tratamiento a gran escala:	De 0 a 10.000
Seleccione las categorías de los datos tratados:	Datos especialmente protegidos
El tiempo de permanencia y tratamiento de los datos personales:	Meses Años
Indique la extensión geográfica del tratamiento:	Regional Nacional
¿La información solicitada tiene como objetivo la monitorización o evaluación sistemática de aspectos personales mediante lo cual se puede determinar hábitos, comportamientos, preferencias hábitos, gustos, intereses de personas identificadas o identificables?	Si
¿La información solicitada tiene como finalidad el tratamiento de datos sensibles?	Datos de porcentaje de discapacidad del estudiante. Vida sexual u orientación sexual Datos relativos a la salud Datos de violencia o malos tratos.
¿La captura de datos personales genera algún tipo de contacto con los interesados de tal manera que, este contacto, genere un acto intrusivo o que pueda ser intrusivo por medio del uso de tecnologías?	No
¿El tratamiento de los datos genera que un gran número de personas tengan acceso a los mismos?	Si
TECNOLOGIAS EMPLEADAS PARA EL TRATAMIENTO	
¿El uso de tecnologías para la captura, procesamiento y almacenamiento de los datos resultan o pueden ser consideradas como inmaduras, debido a que son tecnologías recién salidas al mercado o que por alguna razón representan algún tipo de riesgo?	Si

PERCEPCIONES DE LA EXISTENCIA DE UN RIESGO ELEVADO POR PARATE DEL RESPONSABLE DE LA ACTIVIDAD DEL TRATAMIENTO	
¿El tratamiento de esta información desencadena con una pérdida o alteración de la información?	Si
¿La información capturada es almacenada en papel?	Si
De ser así, indique las medidas que se aplican para salvaguardar esta información	Otros, Se almacenan en cuenta de Dropbox personal del responsable de unidad, y él envió de información se lo hace vía correo electrónico y Quipux.
TERCEROS QUE INTERVENGAN EN EL TRATAMIENTO	
¿Interviene algún proveedor en el proceso?	Si
De ser así, indicar el nombre de la entidad	Dropbox, Quipux, Google Drive.

Elaborado por: Vaca, P (2019)

Con la aplicación del Anexo I, se tiene que en la DD23D01 Educación Santo Domingo, se manejan datos de carácter sensible y que tienen que ser protegidos con un alto grado de confidencialidad.

El proceso de identificación de riesgos a los cuales se encuentran sometidos los datos personales, se complementa mediante el uso de una metodología que ya fue explicada en el capítulo IV del presente de documento de investigación de los cuales se obtuvieron los siguientes resultados:

- Una vez obtenido los datos de usuarios afectados en ataques de phishing y keyloggers satisfactorios y contando con las ponderaciones y dimensiones en aspectos de seguridad informática se procederá calcular el riesgo que estos ataques implican para la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo mediante la siguiente formula:

$$Riesgo = Amenaza\ x\ Vulenerabilidad$$

Tabla 61 Cálculo del riesgo

Amenaza	Escala amenaza	Vulnerabilidad	Impacto	Riesgo
Phishing	VI 0.33	84,62%	Alto	27,9%
Phishing	IG 0.66	84,62%	Alto	55,84%
Phishing	DS 0.99	84,62%	Alto	83,77%
Keyloggers	VI 0.33	92,31%	Alto	30,46%
Keyloggers	IG 0.66	92,31%	Alto	60,92%
Keyloggers	DS 0.99	92,31%	Alto	91,39%

Elaborado por: *Vaca, P (2019)*

Inventario de los activos de la Dirección Distrital Educación 23D01

En este paso se han realizado el inventario de los dispositivos que se utilizan en la DD23D01 utilizando la siguiente nomenclatura:

- **SI:** Activo de tipo Sistema de Información.
- **SFT:** Activo de tipo Software.
- **AF:** Activo de tipo físico.

En la siguiente matriz se detalla el inventario de activos y datos que se manejan en cada una de las unidades especificadas en la Tabla 6 Población de estudio del presente documento de investigación.

Tabla 62 Inventario de Activos Informáticos de las unidades administrativas de la DD23D01

Id	ACTIVO	CARACTERISTICAS
AF-01	Servidor de Ficheros	• Respaldo de información mediante carpetas compartidas. • Almacenamiento: 5TB. • Procesador: Intel Core 2 Duo.
AF-02	Computadores	• Total: 51 • Procesador: 3101 MHz • Memoria RAM: 4096 MB
AF-03	Impresoras	• Total: 18 • Escaneo de documentos, copia e impresión.
AF-04	Equipos activos de red	• Total: 5
SI-01	MOGAC (Módulo de atención ciudadana)	• Proporciona a las plataformas de Atención Ciudadana la posibilidad de mantener un control local en tiempo real sobre todos los requisitos introducidos por los ciudadanos, a través de diversos módulos que permiten la generación de turnos, registros, informes, respuestas y archivo de procedimientos dentro de cada Distrito a nivel nacional.
SI-02	QUIPUX (Sistema de gestión documental)	• Utilizado para la elaboración de oficios, memorandos, circulares y cualquier trámite formal en la DD23D01 Educación.
SFT-01	Servidor de respaldo de información.	• Windows 8.1

Elaborado por: ***Vaca, P (2019)***

El proceso de identificación de riesgos se lo realiza mediante la evaluación de cada uno de los activos en el cual se realiza una ponderación entre un rango del 1 al 5 según el grado de afectación a la confidencialidad, integridad y disponibilidad de los activos.

Para ello en la siguiente matriz se muestra según sea el caso, el cómo se vea afectado cada uno de los activos de la DD23D01 Educación de la ciudad de Santo Domingo:

Tabla 63 Matriz de identificación de riesgos según el activo.

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de Ficheros	4	4	4	4
Computadores	4	3	4	4
Impresoras	2	2	3	2
Equipos activos de red	3	3	3	3
MOGAC (Módulo de atención ciudadana)	4	4	4	4
QUIPUX (Sistema de gestión documental)	4	4	4	4
Servidor de respaldo de información.	4	4	4	4

Elaborado por: *Vaca, P (2019)*

De los resultados obtenidos en la matriz anterior se evaluará aquellos que su valor promedio entre confidencialidad, integridad y disponibilidad hay sido mayor o igual a tres.

Tabla 64 Activos a ser evaluados por el grado de riesgo.

Activo	Total
Servidor de Ficheros	4
Computadores	4
Equipos activos de red	3
MOGAC (Módulo de atención ciudadana)	4
QUIPUX (Sistema de gestión documental)	4
Servidor de respaldo de información.	4

Elaborado por: *Vaca, P (2019)*

Determinar las amenazas existentes

Una vez analizado y realizado un inventario tanto de los activos como de los datos personales que se capturan en la DD23D01, el siguiente paso es determinar las amenazas que pueden afectar la integridad de los datos.

Identificación de vulnerabilidades existentes

Una vez identificadas las amenazas existentes, es importante conocer cuáles son las vulnerabilidades que pueden ser explotadas y con esto exista fuga de información sensible.

Tabla 65 Listado de vulnerabilidades identificadas en la DD23D01 Educación

Activo	Amenazas	Vulnerabilidades	Vulneración a los datos personales	Valoración del activo (1-5)	Probabilidad de explotación de amenaza (1-5)	Total
Servidor de Ficheros	Fallo en el sistema de información personal	Falta de mantenimiento	Pérdida o daño.	4	3	12
	Deficiencia en el performance del equipo	No contar con un procedimiento para el reemplazo de equipos	Pérdida, daño o destrucción.	4	2	8
	Pérdida o robo de medios de almacenamiento electrónico.	Almacenamiento no cifrado	Pérdida, copias no autorizadas, acceso o tratamiento no autorizado.	4	3	12
		No contar con procedimientos de destrucción de medios electrónicos.	Pérdida, copias no autorizadas, acceso o tratamiento no autorizado.	4	2	8
Computadores	Fallo en el sistema de información personal	Falta de mantenimiento	Pérdida o daño.	4	3	12
	Deficiencia en el performance del equipo	No contar con un procedimiento para el reemplazo de equipos	Pérdida, daño o destrucción.	3	2	8
	Pérdida o robo de medios de almacenamiento electrónico.	Almacenamiento no cifrado	Pérdida, copias no autorizadas, acceso o tratamiento no autorizado.	4	2	8
		No contar con procedimientos de destrucción de medios electrónicos.	Pérdida, copias no autorizadas, acceso o tratamiento no autorizado.	4	3	12
Equipos de Red	Falsificación de usuarios.	Carencia de mecanismos de autentificación e identificación de usuarios.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.	4	3	12
	Penetración en los sistemas de información.	Contraseñas no cifradas	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.	4	3	12
	Intrusión a los datos de los usuarios.	Mal uso de protocolos de Red.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Canales encubiertos y tráfico clandestino.	Carencia de monitoreo de los componentes de las redes.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Fraude y robo.	Admisión de personal incorrecto.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.	4	2	8
	Código malicioso ejecutado.	Descarga de aplicaciones sin control.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.	4	4	16

MOGAC	Privilegios sin control en os usuarios.	Falta de actualizaciones referentes a parches de seguridad	Tratamiento, uso y acceso no autorizado.	4	3	12
	Acceso no autorizado a los sistemas.	Sesiones iniciadas sin el usuario autorizado frente al computador.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Acceso de personas a información confidencial.	Inadecuado borrado de información sensible.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Acceso a los sistemas de información	Error en la asignación de privilegios de acceso.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Errores operacionales en los sistemas de información.	Interfaces sin estándares de usabilidad	Tratamiento, uso, acceso no autorizado, daño, alteración o modificación.	4	3	12
QUIPUX	Privilegios sin control en os usuarios.	Falta de actualizaciones referentes a parches de seguridad	Tratamiento, uso y acceso no autorizado.	4	3	12
	Acceso no autorizado a los sistemas.	Sesiones iniciadas sin el usuario autorizado frente al computador.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Acceso de personas a información confidencial.	Inadecuado borrado de información sensible.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Acceso a los sistemas de información	Error en la asignación de privilegios de acceso.	Tratamiento, uso y acceso no autorizado.	4	3	12
	Errores operacionales en los sistemas de información.	Interfaces sin estándares de usabilidad	Tratamiento, uso, acceso no autorizado, daño, alteración o modificación.	4	3	12
Personal	Fraude y robo.	Carencia de cultura en seguridad de la información. Admisión de personal incorrecto.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.	4	3	12
	Errores operacionales de los sistemas de información.	Incorrecto uso de hardware y software.	Perdida, destrucción tratamiento, uso y acceso no autorizado.	4	4	16
	Fuga de información sin control.	Falta de auditorías internas en el uso de sistemas de información por parte de los servidores públicos.	Perdida, destrucción tratamiento, uso y acceso no autorizado.	4	3	12
	Fraude y robo.	Admisión de personal incorrecto.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.	4	3	12

Elaborado por: Vaca, P (2019).

Identificar los escenarios vulnerables y criticidad.

Aunque ya se ha venido mencionado en los apartados anteriores se ha identificado la Unidad de Apoyo a la inclusión (UDAI), debido que en esta unidad se tratan datos personales y se lo tratará como un escenario de vulnerabilidad y criticidad.

Subfase VI. Verificación de los mecanismos de seguridad y análisis de la brecha

Se propone una serie de mecanismos de seguridad aplicables para la protección de datos personales en la UDAI especificados en el Anexo D del presente documento.

Tabla 66 Detalle de mecanismos recomendados en la UDAI.

Objetivo de control	Detalle	Aplica
Políticas aplicadas en el modelo de gestión de datos personales		
Políticas de gestión de datos personales.	El directorio debe tener aprobadas las políticas de gestión de datos personales, de igual manera la implementación y mantenimiento de controles y mecanismos establecidos para la salvaguardar los datos sensibles de la Dirección Distrital.	Si
Monitoreo y Evaluación.	Las políticas deben ser monitoreadas y auditadas para comprobar si es que se las está cumpliendo con normalidad, asimismo cuando exista un nuevo riesgo.	Si
Cumplimiento Legal		
Identificación la legislación aplicable.	Es importante identificar los deberes y responsabilidades de los servidores públicos de la Dirección Distrital Educación 23D01, referente al tratamiento de datos personales y sus consecuencias legales, en caso de que se incumpla con algún derecho de los usuarios.	Si
Registros de evidencia	Se debe mantener en lo máximo posible cualquier documentación que en un futuro sean como descargo de evidencia ante una vulneración en los datos personales.	Si
Recolección de evidencia.	La evidencia tiene que ser debidamente recolectada en caso de alguna vulnerabilidad que haya sido explotada.	Si
Revisión del cumplimiento técnico.	Debe existir revisiones periódicas de los activos, así como de los controles, de manera tal que se verifique el correcto funcionamiento, así como de las amenazas y vulnerabilidades existentes.	Si

Clasificación y acceso a los activos		
Inventario y clasificación de los datos personales	Se debe contar con un registro de datos personales capturados y tratados por la Dirección Distrital en cualquier medio de almacenamiento, prestando total atención a los datos sensibles.	Si
Inventarios de activos	Bajo el concepto de que la información hoy en día se considera como el bien más preciado de toda organización, se debe tener un de los activos de información, identificando a los usuarios que cuentan con responsabilidad sobre los datos personales.	Si
Identificación del ciclo de vida de un dato en la Dirección Distrital.	Es recomendable tener identificado el ciclo de vida de un dato o tipo de información sensible que reposa sobre los medios de almacenamiento de la Dirección Distrital y cuál es su tratamiento.	Si
Seguridad Personal		
Identificar responsabilidades de cada funcionario de la Dirección Distrital.	Es importante que el personal que labora en la Dirección Distrital conozca de las responsabilidades que tiene en el tratamiento de datos sensibles de los usuarios, de igual manera de las sanciones que pueden desencadenar del mal tratamiento de los mismos.	Si
Acuerdo de confidencialidad.	El nuevo personal contratado debe firmar acuerdos de confidencialidad, así como de no divulgación de información sensible. Anexo G	Si
Capacitación.	El personal debe estar constantemente capacitado y recibir programas de concienciación referente a la seguridad de la información y protección de datos personales.	Si
Proceso disciplinario.	La Dirección Distrital tiene que disponer de un proceso disciplinario para aquellos funcionarios que no cumplan con lo establecido en la política de tratamiento de datos sensibles, controles y mecanismos existentes.	Si
Seguridad Física		
Control perimetral	Identificar si existe control de acceso perimetral, es decir, puertas con control de acceso, guardias, cámaras de seguridad, entre otros.	Si
Seguridad de cableado	Se debe evaluar el estado de las conexiones de cableado, ya que con esto se impide la intercepción por parte de terceros.	Si

Control de los activos fuera de las instalaciones	La Dirección Distrital debe contar con mecanismos para controlar que ningún activo con información sensible salga de la misma.	Si
Destrucción segura de la información.	Cuando se da de baja cualquier activo que contengan datos sensibles como medios de almacenamiento, tiene que aplicársele borrado seguro. Este borrado tiene que registrarse para futuras auditorias.	Si
Escritorio limpio	Cuando un reporte o informe que contenga información sensible no se lo esté utilizando se lo debe de almacenar en lugares seguros fuera del alcance de terceros.	Si
Control ante robo	La organización tiene que auditar e identificar los activos que contengan información sensible y sean susceptibles a cualquier tipo de robo.	Si
Gestión de operaciones		
Control de cambios operacionales.	Se recomienda tener procedimientos para documentar y evaluar cualquier cambio que afecte el tratamiento de datos personales.	Si
Segregación de tareas	Se recomienda aislar las funciones, operaciones y responsabilidades en el tratamiento de datos personales.	Si
Protección ante malware	Es recomendable capacitar y concienciar a los funcionarios para que: 1. No instalen cualquier aplicativo en PC's que sirvan para el tratamiento de datos personales. 2. Mantener o informar para que sus computadores se encuentren debidamente actualizados. 3. Reportar cualquier acción fuera de lo normal en las mencionadas computadoras.	Si
Registros y auditorías a los funcionarios	El encargado de tratamiento de datos personales debe realizar auditorías para que se analice los registros en los que se han visto expuesto los datos personales.	Si
Controles de Red	El administrador de la red tiene que tener segmentada la red y los recursos que se comparten con normalidad y los que tienen que ser restringidos.	Si
Administración de medios de almacenamiento secundario.	Tiene que existir políticas y procedimientos para la utilización de medios extraíbles como discos duros externos, CD, DVD, pendrive entre otros.	Si

Seguridad de medios que son movilizados	Debe existir mecanismos de protección para asegurar el transporte de medios que por alguna u otra razón tienen que ser transportados con mecanismos como contraseñas, encriptación, entre otros.	Si
Manejo de correo electrónico y mensajería instantánea.	El personal debe hacer uso correcto y seguro de correo electrónico, mensajería instantánea, empleando mecanismos que mitiguen la recepción de ficheros que en su estructura contenga código malicioso.	Si
Disociación de datos	Los datos deben almacenarse de manera aislada para que con esto no contribuyan con información valiosa y haga una persona como identificable.	Si
Control de acceso		
Normas de control de acceso	La organización debe contar con normas y privilegios para cada usuario limitando el uso de los sistemas de información según su perfil.	Si
Manejo de usuarios y claves de seguridad	Los funcionarios deben ser identificados en el sistema para que pueda ser controlada la actividad que realizan dentro de los sistemas de información. Además, todos los funcionarios tienen que mantener el sigilo referente al manejo de contraseñas y de los controles que se realizan a los funcionarios.	Si
Computadores que dejen de usarse	Los computadores tienen que estar configurados para que cuando un funcionario de la organización lo deje de utilizar se suspenda o cierre sesión de manera automática.	Si
Accesos externos a sistemas de información	La organización debe contar con mecanismos como protocolos de autenticación, cifrado, conexiones mediante claves públicas, entre otros, para que con esto se brinde seguridad cuando un usuario habilitado se conecte a los sistemas de información.	Si
Segregación de redes	Se debe utilizar mecanismos de seguridad que permitan separar a los usuarios el acceso a la red. Estos mecanismos pueden ser utilización de servicios como Firewalls, VPN, entre otros.	Si
Controles de inicio de sesión	Cualquier acceso a la información sensible se la debe realizar mediante inicios de sesión seguros.	Si
Trazabilidad de tratamiento	Este control permite identificar al funcionario que accedió a los datos personales y que tratamiento realizó sobre ellos.	Si

Asilamiento de datos sensibles	El encargado del tratamiento de datos debe auditar y evaluar los activos que manejen datos sensibles para que se los coloque en entornos aislados.	Si
Uso de dispositivos móviles internos.	Dentro de este grupo se encuentran las laptops, netbooks, tablets, smartphones que se ha entregado a los funcionarios. De este modo debe existir planes y acuerdos de concientización de las consecuencias que puedan generarse si estos llegaran a perderse.	Si
Autenticación de segundo factor de autenticación mediante tokens TOTP (Time One-Time Password)	En el caso de uso de almacenamiento por parte de terceros como Dropbox, Google drive, etc. Se debe implementar mecanismos de segundo factor de autenticación.	Si
Mantenimiento de sistemas		
Cifrado	El encargado de protección de datos tiene que identificar los datos que por su naturaleza tienen que estar protegidos mediante cifrado.	Si
Firmas Electrónicas	Para la verificación y validación de los documentos enviados como recibidos se pueden aplicar técnicas como firmas electrónicas.	Si
Vulneraciones de seguridad		
Procedimientos para el manejo de incidentes	La Dirección Distrital tiene que implementar procedimientos para el manejo de incidentes, debido a que al tenerlos se puede dar pronta y efectiva respuesta a cualquier incidente de vulnerabilidades y para que posteriormente se realice tareas de corrección.	Si
Procedimientos en caso de incidentes.	Se tiene que contar con procesos tales como reporte, seguimiento, mitigación y registro documental de un altercado de seguridad, de tal manera que se pueda verificar	Si
Reportes de incidentes de seguridad	Para que un reporte sea válido, este debe pasar por un proceso formal y seguir un protocolo para su validación.	Si
Reporte de fallo en funcionamiento	La organización debe contar con un proceso formal para reportar fallos en producción de hardware como de software.	Si
Procedimientos de notificación de	La Dirección Distrital debe manejar procedimientos referentes a la notificación de vulnerabilidades de los datos	Si

vulnerabilidades a los titulares de datos.	de los titulares cuando se vean afectados sus derechos. Dentro de estos procedimientos se tiene que constar la magnitud de la vulneración y los mecanismos de protección que los titulares de los datos necesiten.	
Aprendizaje de incidentes	Cuando se requiera, se debe establecer mecanismos para monitorear, el tipo, volumen y afectaciones de la vulnerabilidad.	Si
Procedimientos de actualización del modelo de gestión	Es importante que luego de cada incidente se revise, evalué y actualice los mecanismos de seguridad aplicados para que con esto se aplique la mejora continua del modelo de gestión.	Si

Elaborado por: Vaca, P (2019)

Fase de implementación del modelo de gestión de seguridad de la información

En esta fase se da cumplimiento a la fase de implementación, detallando cada documento que se generó en la aplicación de la misma, en relación a los requerimientos de seguridad de la información, políticas y mecanismos que se analizaron en la Fase I.

Tabla 67 Detalle de cumplimiento de documentos aplicados en la fase implementación.

Objetivo	Resultado	Instrumentos	Cumplimiento
Implementación	Documento con guía detallada para la protección de datos en centros educativos.	Anexo E. Registro de Actividades.	Aplicado
	Documento modelo de contrato de confidencialidad con terceros.	Anexo F. Contrato de confidencialidad con terceros.	No aplica
	Documento modelo de contrato de confidencialidad con funcionarios.	Anexo G. Contrato de confidencialidad con funcionarios.	Aplicado
	Documento con firmas de consentimiento de tratamiento de sus datos personales.	Anexo H. Contrato de consentimiento de los usuarios.	Aplicado
	Documento modelo para el análisis de riesgos.	Anexo I. Análisis de riesgos.	Aplicado
	Documento con notificación de brechas de seguridad.	Anexo J. Notificación de brechas de seguridad.	Aplicado

Elaborado por: Vaca, P.

6.7.2.3 Aplicación de la fase de evaluación y monitoreo del modelo

Tabla 68 Evaluación de mecanismos y controles recomendados en el tratamiento de datos personales.

Id	Objetivo de control	Puntaje esperado	Puntaje Obtenido
1	Políticas de gestión de datos personales.	5	5
2	Monitoreo y Evaluación.	5	N
3	Identificación la legislación aplicable.	5	4
4	Registros de evidencia	5	4
5	Recolección de evidencia.	5	4
6	Revisión del cumplimiento técnico.	5	4
7	Inventario y clasificación de los datos personales	5	4
8	Inventarios de activos	5	4
9	Identificación del ciclo de vida de un dato en la Dirección Distrital.	5	4
10	Identificar responsabilidades de cada funcionario de la Dirección Distrital.	5	4
11	Acuerdo de confidencialidad.	5	5
12	Capacitación.	5	4
13	Proceso disciplinario.	5	4
14	Control perimetral	5	4
15	Seguridad de cableado	5	4
16	Control de los activos fuera de las instalaciones	5	4
17	Destrucción segura de la información.	5	1
18	Escritorio limpio	5	5
19	Control ante robo	5	5
20	Control de cambios operacionales.	5	4
21	Segregación de tareas	5	4
22	Protección ante malware	5	4
23	Registros y auditorías a los funcionarios	5	4
24	Controles de Red	5	4
25	Administración de medios de almacenamiento secundario.	5	4
26	Seguridad de medios que son movilizados	5	4
27	Manejo de correo electrónico y mensajería instantánea.	5	5
28	Disociación de datos	5	2
29	Normas de control de acceso	5	4
30	Manejo de usuarios y claves de seguridad	5	4
31	Computadores que dejen de usarse	5	4
32	Accesos externos a sistemas de información	5	N
33	Segregación de redes	5	N

34	Controles de inicio de sesión	5	5
35	Trazabilidad de tratamiento	5	2
36	Asilamiento de datos sensibles	5	3
37	Uso de dispositivos móviles internos.	5	4
38	Autenticación de segundo factor de autenticación mediante tokens TOTP (Time One- Time Password)	5	5
39	Cifrado	5	N
40	Firmas Electrónicas	5	N
41	Procedimientos para el manejo de incidentes	5	4
42	Procedimientos en caso de incidentes.	5	4
43	Reportes de incidentes de seguridad	5	4
44	Reporte de fallo en funcionamiento	5	4
45	Procedimientos de notificación de vulnerabilidades a los titulares de datos.	5	5
46	Aprendizaje de incidentes	5	3
47	Procedimientos de actualización del modelo de gestión	5	3

Elaborado por: Vaca, P (2019)

Después de que se ha realizado la evaluación de los mecanismos de control aplicados a esta unidad administrativa, se procede a calcular el porcentaje de cumplimiento de cada política aplicada mediante el siguiente proceso: Se realizó el sumatorio total del porcentaje esperado entre la sumatoria de la calificación obtenida:

$$\%\ \boldsymbol{Cumplimiento} = \frac{\sum Puntaje\ obtenido}{\sum Puntaje\ esperado}$$

$$\%\ \boldsymbol{Cumplimiento} = \frac{166}{235}$$

$$\%\ \boldsymbol{Cumplimiento} = 71\%$$

Actuar (mejorar el performance del modelo)

Subfase IX Mejora Continua y capacitación

Una vez aplicado el modelo se logró identificar el porcentaje de cumplimiento del modelo que fue del 71% de los mecanismos recomendados y aplicados en esta unidad administrativa de la DD23D01. Por tal razón se sugiere planes de capacitación para que con esto se consiga un grado de cultura mayor en el tratamiento de datos personales.

6.8 Conclusiones

El desarrollo del presente documento permitió al investigador llevar a cabo las siguientes conclusiones:

- ✓ La Dirección Distrital 23D01 Educación de la ciudad de Santo Domingo en primera instancia no se encontraba preparada para tratar de manera segura los datos sensibles de las personas.
- ✓ Mediante el uso de técnicas pentesting se identificó las amenazas y vulnerabilidades a las que se encuentran expuestos los activos informáticos y por ende los datos sensibles de los usuarios que se capturan, almacenan y se distribuyen en la DD23D01 de la ciudad de Santo Domingo.
- ✓ El eslabón más vulnerable en la cadena de seguridad, es en si el usuario final, debido a que, si este no conoce cómo actuar ante una situación de amenaza, constituye una vulnerabilidad para la organización, en el caso de que no sea debidamente capacitado en el uso de herramientas tecnológicas, así como del modelo propuesto.
- ✓ Se brindó capacitación al personal que labora en la DD23D01 creando conciencia en cuál sería el peor de los escenarios en el caso de que los datos de los usuarios se vean vulnerados.
- ✓ Con la implementación del modelo en la Dirección Distrital en estudio se mitigo 46% las vulnerabilidades y amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de los datos personales de los usuarios.

6.9 Recomendaciones

- ✓ Adoptar una arquitectura empresarial en el proceso de gestión de seguridad de la información para que con esto se tenga un personal alineado a los objetivos y valores institucionales referente a la protección de la información.
- ✓ Utilizar el modelo propuesto en el proceso de gestión de datos personales para no llegar a consecuencias sancionatorias, por el desconocimiento del correcto manejo de datos e información sensible.

- ✓ Desarrollar planes de sensibilización y capacitación a todo el personal en el que se incluyan cursos o talleres en el uso del modelo y de la gestión de datos personales.
- ✓ Actualizar el modelo de gestión según la legislación o reglamentación nueva para que este no sea el causante del incumplimiento de la ley de protección de datos.
- ✓ Incluir dentro de la estructura organizacional un responsable técnicamente calificado, que figure como encargado de protección de datos, quien será el que audite, controle y garantice la aplicación del modelo de gestión en todas las unidades administrativas de la Dirección Distrital.

6.10 Bibliografía

Aguilera, P. (2010). Seguridad Informatica. Madrid: Editex, S.A.

Ambrosio Navas, S. (2017). *Protección de datos (Adaptado al RGPD).* Madrid: Elearning S.L.

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Paraninfo.

Baca, G. (2016). *Introducción a la seguridad informática.* Mexico: Patria.

Baena, G. (2014). *Metodología de la investigación.* Mexico: Grupo Editorial Patria.

Báez, J., & Pérez , d. (2007). *Investigación cualitativa.* Madrid: Gráficas Dehon.

Baud, J.-L. (2017). *ITIL V3 PREPARACIoN A LA CERTIFICACION ITIL FOUNDATION* (2 ed., Vol. 3). Barcelona: ENI.

Bernal Torres, C. (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales.* Mexico: Pearson Educación.

Calle, J. (1997). *Reingeniería y seguridad en el ciberespacio.* Madrid: Díaz de Santos, S.A.

Carpentier, J. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: ENI.

Castro, M., Díaz, G., Ignacio, A., & Elio, S. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid: UNED.

Chicano, E. (2014). *Auditoría de seguridad informática. IFCT0109.* Málaga: iceditorial.

Delgado , L. R., & Saltor, C. E. (2014). *El derecho a la protección de datos en España y Argentina:*. Madrid: Dykinson.

Desongles, J., Martos , F., Santos, M., & González , J. (2004). *Auxiliares Administrativos de la Diputacion Provincial de Huesca. Temario.* Sevulla: MAD, SL.

Díez Vegas, F. J., & Juez Martel, P. (1997). *Probabilidad y estadística en Medicina.* Madrid: Díaz de Santos, S.A.

Dirección Nacional de Registros Públicos . (01 de 07 de 2019). Obtenido de http://www.datospublicos.gob.ec/datos-personales/

Drummond, V. (2004). *Internet, privacidad y datos personales.* Marid: Reus.

Fuentelsaz Gallego, C., Icart Isern, M. T., & Pulpón Segura, A. (2006). *Elaboración y presentación de un proyecto de investigación y una tesina.* Barcelona: Gráficas Rey, S.L.

García, A., Cervigón, H., & Alegre Ramos, M. (2011). *Seguridad Informática.* Madrid: Parainfo.

García, P. (2006). *Introducción a la investigación bioantropólogica en actividad física, deporte y salud.* Caracas: Facultad de Ciencias Económicas y Sociales.

Geraldes, T., & López, L. (2010). *La Protección de Datos Personales en México.* México: UMSNH.

Gómez, Á. (2011). *Enciclopedia de la Seguridad Informática* (Segunda ed.). Madrid: Grupo Editorial RA-MA.

Hernández Chavarria, F. (2002). *Fundamentos de la epidemiología.* Costa Rica: asoingraf.

Hernández, B. (2001). *Técnicas estadísticas de investigación social.* Madrid: Díaz de Santos, S.A. 2001.

Ibáñez, J. (2015). *Métodos, técnicas e instrumentos de la investigación criminológica.* Madrid: DYKINSON.

IBM. (13 de 12 de 2016). *IBM*. Recuperado el 24 de 09 de 2018, de https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm

Jara, H., & Pacheco, F. (2013). Implementacion de un sistema para la gestión de la seguridad. *Ethical Hacking 2.0*, 352.

Landeau, R. (2007). *Elaboración de trabajos de investigación : a propósito de la falla tectónica de la Revolución Bolivariana.* Caracas: Alfa.

López, A. (2015). *Guía para gestionar los datos personales.* Madrid: Alianza Formación Empresarial.

Martinez Bencardino, C. (2016). *Estadística básica aplicada*. Bogotá: ECOE EDICIONES.

Merino, M. (2015). *Introducción a la investigación de mercados.* Madrid: Esic Editorial.

Namakforoosh, M. (2005). *Metodología de la investigación.* Mexico: Limusa grupo Noriega Editores.

Ospino, J. (2004). *Metodología de la investigación en ciencias de la salud.* Bogotá: Educc.

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *Scielo*, 229-230.

Packer, M. (2013). *La ciencia de la investigación cualitativa.* Bogotá: Ediciones Uniandes.

Rault, R., Laurent, S., ACISSI, & Agé, M. (2015). *Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (3ª edición).* Barcelona: ENI.

Rubio, M., Gómez, S., & Letón , E. (2017). *INTRODUCCIÓN A LA INFORMÁTICA BÁSICA.* Madrid: UNED.

Sábado, J. (2009). *Fundamentos de bioestadística y análisis de datos para enfermería.* Barcelona: Servci de Publicacions.

Salkind, N. (1999). *Métodos de investigación.* México: Prentice Hall.

San Martín, E. (2015). *Salvaguarda y seguridad de los datos. IFCT0310.* Málaga: IC Editorial.

Sanchez, A. (1998). *La protección del derecho a la libertad informática en la Unión Europea.* Sevilla: EUROPA ARTES GRÁFICAS, S.A.

Siddharth Kalla. (2010). *Explorable*. Obtenido de Estudio Correlacional: https://explorable.com/es/estudio-correlacional

Stallings, W. (2004). *Fundamentos de seguridad en redes. Aplicaciones y estándares.* Madrid: Pearson.

Suárez Ibujes, M. (2012). Interaprendizaje de probabilidades y estadística inferencial con excel, winstats y graph. *Interaprendizaje de probabilidades y estadística inferencial con excel, winstats y graph, Primera Edición*, 224. Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/940/1/Interaprendizaje%20de%20Probabilidades%20y%20Estad%C3%ADstica%20Inferencial%20con%20Excel,%20Winstats%20y%20Graph.pdf

Tamayo, M. (2004). *El proceso de la investigación cientifica.* Mexico: Limusa.

Universidadviu. (21 de 03 de 2018). *universidadviu*. Obtenido de https://www.universidadviu.com/crear-plan-seguridad-informatica-facilmente/

Amutio, M., Candau, J., & Mañas, J. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. 127. Retrieved from https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Arango, M., Londoño, J., & Zapata, J. (2010). *ARQUITECTURA EMPRESARIAL - UNA VISIÓN GENERAL*. https://doi.org/10.1111/j.1574-6976.2010.00236.x

Asamblea Nacional. (2008). Constitución del Ecuador. *Registro Oficial*, *449*(Principios de la participación Art.), 67. https://doi.org/10.1017/CBO9781107415324.004

Asamblea Nacional del Ecuador, E. (2016a). *Informe para segundo debate del proyecto de ley de Protección a la Intimidad y a los Datos Personales* (p. 8). p. 8.

Asamblea Nacional del Ecuador, E. (2016b). Proyecto de Ley de Protección de la Intimidad y a los Datos Personales. *Asamblea Nacional Del Ecuador*, p. 29. Retrieved from http://documentacion.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/ea7d10c2-791a-4e01-8ef6-f60e22ced64f/Ley de Protección a la Intimidad y a los Datos Personales

Bazán, V. (2012). El habeas data, su autonomía respecto del amparo y la tutela del derecho fundamental de autodeterminación informativa . *Anuario de Derecho Constitucional Latinoamericano*, *XVIII*, 37–76.

Becerra, C., Zarate, P., & Gomez, C. (2017). *Evaluación de Impacto para la Protección de la Privacidad de Grandes Datos / Big Data 2 Big Data / Open Data*. 170–184.

Caballero, M. (2017). Diseño de in sistema de gestión de la seguridad de la informacion para la red de datos de la veeduría distrital en la ciudad de Bogotá. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA*

ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA, 159. Retrieved from https://repository.unad.edu.co/bitstream/10596/17398/1/51573183.pdf

Cairo, M. M., Puga, O. V., Mallea, I. P., Cobas, R. P., & Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática Methodology for the Implementation of Automated Management of Computer Security Controls. *Revista Cubana De Ciencias Informáticas*, *10*(2), 14–27.

CHIAPAS, A., & MARTÍNEZ, J. (2009). *Modelo De Seguridad Para El Sevicio De Soporte Técnico Brindado Por Empresa Outsourcing*. 161. Retrieved from http://tesis.ipn.mx/dspace/handle/123456789/5532

Colombia, C. de la R. de. (2012). *Ldato peey 1581 de Octubre de 2012*. 1–15.

DINARDAP. (2019). *Anteproyecto de ley orgánica de protección de datos personales*. 1–46.

Dussan Clavijo, C. A. (2006). Entramado. *Entramado*, *2*(1). Retrieved from http://www.redalyc.org/html/2654/265420388008/

Enríquez Álvarez, L. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Foro Revista de Derecho*, *27*(27), 44–61.

Estrada, J. A., Estrada, J. C., Rodríguez, A., & Tipantuña, C. (2015). *556-3508-1-Pb*. *36*(1).

Gaona-garcía, P., Montenegro-marín, C., & Barón Velandia, J. (2016). Modelo ontológico para la predicción de ataques informáticos a partir de Honeynets virtualizadas Ontological model for predicting cyberattacks based on. *Revista Logos, Ciencia & Tecnología*, *8*(1), 101–114. Retrieved from http://revistalogos.policia.edu.co/index.php/rlct/index

Garcia, L., & Estiwar, L. (2013). *Guía : OWASP Top 10 – 2013*. 1–13.

García, R. (2012). *Protección de Datos Personales Ley 1581 Octubre de 2012*. 1–6.

General Data Protection Regulation. (2016). Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

personales y a la libre circulación de estos datos y por el que se deroga la D. *Diario Oficial de La Unión Europea*, *2014*(119), 1–88. https://doi.org/10.1016/j.yhbeh.2005.02.009

Gil, J. C. (2017). *El debido proceso en la Ley de Habeas Data*. Retrieved from http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/view/10657

Gómez, Á. (2011). *Enciclopedia de la Seguridad Informática. 2a Edición* (p. 828). p. 828. Retrieved from https://books.google.com/books?id=-JIGfAEACAAJ&pgis=1

Gordillo, J., & Restrepo, C. (2005). *Introducción al análisis del derecho fundamental del hábeas data*. *6*(2), 351–385.

Guillen Pinto, E. P., Ramirez López, L., & Cifuentes Sanabria, Y. P. (2017). Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles. *Universidad y Salud*, *19*(2), 280. https://doi.org/10.22267/rus.171902.90

Ifai. (2014). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Marzo 2014*.

Jaramillo, D., Cabrera-Silva, A., Abad, M., Torres, A., & Verdúm, J. C. (2015). Definici??n de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM-TOGAF. *2015 10th Iberian Conference on Information Systems and Technologies, CISTI 2015*, (September). https://doi.org/10.1109/CISTI.2015.7170391

Jaramillo, D., Cabrera, A., Torres, A., Abad, E., & Verdúm, J. (2016). *Definición de un Marco de Referencia de Ciberseguridad Empresarial basado en ADM-TOGAF Definition of Cybersecurity Businness Framework based on ADM-TOGAF*.

Kapersky, L. (2017). *ESTADÍSTICAS GENERALES DE 2017*.

Martelo, R. J., Tovar, L. C., & Maza, D. A. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Informacion Tecnologica*, *29*(1), 3–10. https://doi.org/10.4067/S0718-07642018000100002

Mendoza Enríquez, O. A. (2018). Ius : revista del Instituto de Ciencias Jurídicas de

Puebla. *Revista IUS*, *12*(41), 267–291. https://doi.org/http://dx.doi.org/

Mesquida, A. L., Mas, A., & Amengual, E. (2009). La madurez de los servicios TI. *Revista Española de Innovación, Calidad e Ingenieria Del Software*, *5*(2), 77–87. Retrieved from https://pdfs.semanticscholar.org/7777/49ac1eeaeb856537179ff441f3a50ad101ca.pdf

Naciones Unidas. (1948). *Resolución 217 (III) A Carta Internacional de los derechos del hombre Declaración universal de derechos del hombre*.

Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. *Article*, *1*, 14.

Nomura, T., Fukai, T., Hano, Y., & Fujimoto, T. (1983). Structure of Sanggenon G, a New Diels-Alder Adduct from the Chinese Crude Drug "Sang-Bai-Pi" (Morus Root Barks). *HETEROCYCLES*, *20*(4), 611. https://doi.org/10.3987/R-1983-04-0611

Outomuro, D., & Mirabile, L. M. (2015). Confidencialidad y privacidad en la medicina y en la investigación científica: desde la bioética a la ley. *Revista de Bioética*, *23*(2), 238–243. https://doi.org/10.1590/1983-80422015232062

Parada, D. J., & Flórez, A. (2018). *Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas*. *29*(1), 27–38. Retrieved from http://dx.doi.org/10.4067/S0718-07642018000100005

Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Maturity models in cybersecurity: A systematic review. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/CISTI.2017.7975865

Ríos, S. (2014). ITIL v3 Manual íntegro. *B-Able*, 101. Retrieved from http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science*, *121*, 568–575. https://doi.org/10.1016/j.procs.2017.11.075

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., … Castillo, M. (2014). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL*

ANÁLISIS DE VULNERABILIDADES. https://doi.org/10.13140/2.1.1072.6722

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Carrillo De Gea, J. M. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atencion Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

Santiago, C. (2013). *Propuesta de una Arquitectura Empresarial para una Instituciones de Educación Superior como apoyo a su desarrollo frente a los retos del Siglo XXI*. 29. Retrieved from http://www.escuelaing.edu.co/uploads/laboratorios/2734_plimeros.pdf

Solórzano Cadena, L., Rezabala Triviño, J., & Alfonso Aranda, I. (2013). *Estudio Sobre el Estado Del Arte de la Seguridad Informática en el Ecuador y sus Necesidades Reales*. (1), 8. Retrieved from http://www.dspace.espol.edu.ec/bitstream/123456789/24298/1/Articulo de Tesis Estudio del Estado del Arte de La Seguridad Informatica en el Ecuador.pdf

Veloz, J., Alcivar, A., Salvatierra, G., & Silva, C. (2017). INFOR ATICA Y SISTEMAS Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta KALI-LINUX. *Año*, *11*(1), 1–12.

ANEXOS

CUESTIONARIO
UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

FORMULARIO DE ENCUESTA DIRIGIDA A LOS FUNCIONARIOS DEL DISTRITO DE EDUCACION 23D01 DE LA CIUDAD DE SANTO DOMINGO.

Saludos cordiales: Le invitamos a contestar con la mayor objetividad el siguiente formulario a fin de obtener información valiosa y confiable, que será de uso científico-técnico y de máxima confidencialidad.

Este cuestionario forma parte de un programa de investigación que se lleva a cabo en la Universidad Técnica de Ambato a través de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

OBJETIVO

Conocer los procesos actuales para la gestión y protección de la seguridad de la información lógica, específicamente en el tratamiento de datos sensibles.

Aspectos Generales

1. **¿Conoce cuáles son los Datos Sensibles que se manejan en la Institución?**

Si	☐	No	☐

2. **¿Existen políticas institucionales de seguridad establecidas para el manejo de datos sensibles?**

Si	☐	No	☐

3. **¿La institución cuenta con procedimientos estandarizados sobre los lineamientos en el manejo de datos sensibles?**

Si	☐	No	☐

4. **¿Conoce si en la institución manejan un modelo para el tratamiento de datos sensibles?**

Si	☐	No	☐

5. **¿Al enviar datos sensibles a través del navegador, revisa si la dirección URL tiene una conexión segura, talvez usa un protocolo seguro cómo https?**

Si □		No □	

6. **¿En la institución hacen uso de herramientas seguras para subir, transmitir y generar información en los que intervengan datos sensibles?**

Si □		No □	

7. **¿Conoce quién es el responsable del tratamiento de los datos sensibles en el Distrito de Educación 23D01?**

Director de Sistemas □	Director de RRHH □	Oficial de seguridad de la información □	No existe Responsable □	No sé □

8. **¿El responsable de la protección de datos está dedicado a tiempo completo?**

No □	Si □	No sé □	No existe Responsable □

9. **¿En la actualidad, El Distrito de Educación 23D01 cuenta con una medida o plan para la protección de datos sensibles?**

Si □	No, pero estamos en proceso □	No □	No sé □

10. **¿El Distrito de Educación 23D01 cuenta con información clasificada en datos personales, sensibles, financieros/patrimoniales?**

Si □	No, pero estamos en proceso □	No □	No sé □

11. **¿En qué departamento del Distrito de Educación 23D01 cree usted que existe mayor relevancia respecto a los datos sensibles?**

Unidad Financiera ☐	Unidad Planificación ☐	Dece ☐	Unidad Talento Humano ☐	Unidad ☐ Asesoría Jurídica

12. ¿Utiliza métodos de encriptación para el envió de información sensible que lo realiza vía correo electrónico?

Siempre ☐	Casi Siempre ☐	A veces ☐	Casi nunca ☐	Nunca ☐

13. ¿El Distrito de Educación 23D01 le ha hecho firmar un acuerdo de confidencialidad de la información?

Siempre ☐	Casi Siempre ☐	A veces ☐	Casi nunca ☐	Nunca ☐

14. ¿Sabe reconocer un correo electrónico sospechoso?

Siempre ☐	Casi Siempre ☐	A veces ☐	Casi nunca ☐	Nunca ☐

15. ¿Cuál es el nivel de riesgo que tiene el Distrito de Educación 23 D01 en las siguientes situaciones para el robo o el mal uso de los datos sensibles?
Para sus respuestas utilizar la siguiente escala:

1. **Débil**
2. **Notable**
3. **Muy Fuerte**

Situación	**1**	**2**	**3**
Ataques cibernéticos a través de internet a través de correo electrónico			
Ataques cibernéticos a través de red local (realizados por terceros)			
Robo de información vía dispositivos usb, discos duros, celulares, Tablet.			
Robo de laptops y/o Pcs.			

16. ¿Cuál sería el impacto principal que pueda ser provocado por la fuga de datos sensibles del Distrito de Educación 23D01?

Legal	□	Económico	□	Imagen y Reputación	□	Operativo	□	Continuidad de negocio	

17. ¿Referente al manejo de sistemas de información del Mineduc, utiliza contraseñas fuertes y una diferente para cada servicio?

Siempre	□	Casi Siempre	□	A veces	□	Casi nunca	□	Nunca	

18. ¿Culturalmente y como medida de prevención cambia con regularidad las contraseñas de los sistemas de información de Mineduc?

Siempre	□	Casi Siempre	□	A veces	□	Casi nunca	□	Nunca	

19. ¿Con frecuencia el departamento de TI realiza copias de seguridad de los sistemas de información de Mineduc?

Diariamente	□
Semanalmente	□
Mensualmente	□
Anualmente	□
Nunca	□

20. ¿El personal de TI sabe como actuar ante alguna eventualidad con resultados trágicos relacionados a la seguridad informática?

Siempre	□	Casi Siempre	□	A veces	□	Casi nunca	□	Nunca	

21. ¿Considera que el personal de TI cuenta con un plan de contingencia para reaccionar oportunamente ante un ataque informático?

Siempre	□	Casi Siempre	□	A veces	□	Casi nunca	□	Nunca	

22. ¿La institución utiliza métodos específicos para la destrucción de la información sensible de sus usuarios?

Siempre	□	Casi Siempre	□	A veces	□	Casi nunca	□	Nunca	

23. ¿Usted como funcionario conoce sus responsabilidades y las sanciones derivadas en la ley que pueden ser acreedores?

Si	□	No	□

24. ¿Cree que la aplicación de un modelo de seguridad de la información garantice la protección de los datos sensibles del Distrito de Educación 23D01 cuando estos sean transmitidos, subidos, receptados o generados?

Si	□	No	□

Anexo A.

Políticas de protección de tratamiento de datos personales. Dirección Distrital Educación 23D01

Información del documento

Nombre del documento	Políticas de protección de tratamiento de datos personales Dirección Distrital Educación 23D01.
Versión	1.0

Marco legal en la protección de datos personales.

La Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo acuerda utilizar los datos personales de los usuarios, clientes y proveedores basándose en las normas establecidas por los entes legisladores dictaminado en:

1. El artículo 66 numeral 19 del artículo 66 de la Constitución de la República del Ecuador: "Se reconoce y garantizará a las personas: (…) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley";
2. En virtud de lo señalado, cabe destacar que el artículo 85 numeral 1 de la Carta Magna dispone que "(…) la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y el buen vivir y todos los derechos (…)".
3. El artículo 178 del Código Orgánico Integral Penal establece: "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años…";
4. El artículo 229 del código ibídem, manifiesta: "Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años".

Ámbito de aplicación

La presente política de protección de datos personales tiene como objeto el uso veraz y tratamiento de cualquier información confidencial o no que reposan en las bases de datos de la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo tales como:

4. Información de los usuarios de sistema educativo sean estos: Docentes, Padres de Familia, Estudiantes y servidores públicos en general.

Tratamiento de Datos Sensibles

Por parte de la Dirección Distrital Educación 23D01 queda netamente prohibido el tratamiento de datos sensibles, excepto cuando:

a) El titular de los datos haya realizado a debida autorización para el tratamiento de este tipo de información o cuando por casos de la ley no sea necesario solicitar que se otorgue algún tipo de autorización.
b) El titular se encuentre incapacitado física o jurídicamente para otorgar su tratamiento, cuando esto suceda el representante legal están en la capacidad de otorgar dicha autorización.
c) El tratamiento sea realizado bajo actividades que vayan acordes a la ley y siempre y cuando se cuente con las garantías pertinentes de una organización, fundación, ONG o cualquier otra organización sin ánimos de lucro.
d) El tratamiento conlleve un fin histórico, estadístico o científico.

Derechos del titular de Datos Personales

Por parte de la Dirección Distrital Educación 23D01 y respetando las excepciones establecidas en el tratamiento de datos sensibles, se otorgará los siguientes derechos:

a) El titular de datos personales tiene derecho a ser previamente comunicado, sea en el momento que sea cuando se captura, solicita almacena su información y principalmente cuando estos vayan a ser utilizados excepcionalmente de forma posterior cuando estos no se los haya obtenido

de forma directa, transparente, expresa e inequívoca desde los medios especificados en Artículo 20 literales “a” al “p” del anteproyecto de la LOPDP del Ecuador.

b) A conocer y acceder a toda su información de manera gratuita previo a una solicitud al encargado de datos personales, sobre el uso del cual se le están dando a sus datos personales especificados en el Artículo 21 de la LOPDP del Ecuador.
c) Solicitar que se le corrijan o actualicen los datos que se encuentran almacenados de manera errónea, estén incompletos, desactualizados, falsos e imprecisos.
d) A oponerse o negarse al tratamiento de sus datos cuando estos no sean utilizados de manera correcta o que conlleven a valoraciones o decisiones sin el consentimiento del titular.
e) A pedir que se suprima o elimine sus datos personales, con la finalidad de que dejen de ser tratados por el encargado del tratamiento de datos personales especificados en el artículo 23 de la LOPDP, excepto los literales especificados en el artículo 25 de las Excepciones a los derechos de eliminación y oposición.

Autorización y consentimiento del titular

Dando cumplimiento a lo especificado en la constitución del Ecuador y el anteproyecto de la LOPDP la Dirección Distrital Educación 23D01 de la ciudad de Santo Domingo solicitará la autorización previa e informada del titular de los datos.

Situaciones en las que no se requiere previa autorización: No se requerirá la autorización por parte del titular de los datos cuando se encuentre en los siguientes casos:

a) Datos solicitados por una institución del estado cuando se encuentre ejerciendo aspectos legales o por orden judicial con el fin de dar respuesta a requerimientos legales ante algún tipo de investigación judicial al titular de los datos.
b) Datos cuya naturaleza no sea vulnerable o de característica pública.
c) En el que el titular se vea afectado ante una urgencia médica o sanitaria.

d) Tratamiento de datos que hayan sido autorizados por la ley cuya finalidad sea para fines estadísticos o científicos.
e) Información referente con el registro Civil del titular.

Suministro de información

Atención Telefónica

Atención vía correo electrónico

Dirección: Calle Rio Chimbo y Balzapamba, Santo Domingo Ecuador.

Encargado: Encargado del departamento de Tics.

Procedimiento para la atención a reclamos, solicitud de edición de datos erróneos, actualización, cancelación y consulta de datos personales.

Atención a Reclamos: Cuando el titular de los datos considere que los mismos deben ser sometidos a una corrección, actualización o cancelación, o a su vez cuando exista una denuncia de mal uso debido al incumplimiento de lo impuesto por la constitución del Ecuador o por la LOPDP, tendrá el derecho de presentar un reclamo basándose en los siguientes preceptos:

Cualquier tipo de reclamo relacionado al incorrecto tratamiento de los datos personales, este se lo formulará por medio de solicitud dirigida a la Dirección Distrital Educación 23D01, en la que se hará constar el número de cédula de titular, detalle de los hechos que tienen origen como reclamo, la dirección adjuntando los documentos que le sirva como evidencia del caso. En caso de que el reclamo sea incompleto, se llamará al solicitante dentro de los 5 días siguientes a la receptación del reclamo para que rectifique las fallas. Una vez transcurrido dos meses desde que se emitió el reclamo, sin que el denunciante presente la documentación necesaria para que el reclamo sea completo, el encargado del tratamiento de datos entenderá que el titular ha desistido del reclamo.

Si es que se da el caso de quien reciba el reclamo no esté en la capacidad de resolverlo, trasladará dicho reclamo a quien corresponda en un máximo de 2 días laborables todo esto siempre y cuando el titular se encuentre debidamente informado.

Tanto el encargado y responsable de datos tendrán un máximo de 15 días laborables a partir del día siguiente a la fecha que fue receptado, para responder al reclamo.

En el caso de que no se pueda dar solución en este lapso de tiempo se informará al interesado de los motivos por los cuales no se pueden atender a su solicitud.

Atención a consultas: Para que un titular o la persona que le haya cedido sus derechos pueda consultar sus datos que reposen en cualquier base de datos de la Dirección Distrital Educación 23D01, la entidad entregará a ellos la información que se encuentra almacena en el registro individual o que se encuentre vinculada con la identificación del titular.

Las consultas se las atenderá en un lapso máximo de 10 días laborables que corre a partir de la fecha de recibo de la misma. En el caso que la Dirección Distrital Educación no tenga las posibilidades de atender a alguna consulta, se informará al solicitante dando a conocer las causas de la demora y dándoles a conocer la fecha en la que su consulta será atendida, que por ninguno de los casos supere los 5 días laborables.

Vigencia de la Política

La presente política se aplicará a partir del 31 de marzo del 2019.

Permanencia de datos

Los datos permanecerán almacenados durante el tiempo que sea necesario y siempre cumpliendo los parámetros y políticas especificadas para lo que fueron recolectados.

Restricciones y tratamiento de datos del usuario de la Dirección Distrital Educación 23D01

Estrato 1

Los datos sensibles que se trasmiten y recopilan en la Dirección Distrital Educación 23D01 tanto en servidores como en computadores, dispositivos de almacenamiento tales como: Pendrives, discos duros externos, unidades de CD, DVD y en cualquier otro dispositivo que pueda almacenar información no se realizará este tipo de almacenamiento. De igual forma se encuentra netamente prohibido a los funcionarios que acceden a las bases de datos por medio de accesos remotos tales como VPN, copiar, mover, almacenar datos de los usuarios a los PC’s.

Estrato 2

Los Backups de los datos que provienen de los usuarios de la Dirección Distrital Educación 23D01 que se encuentran funcionando de manera secundario, serán

almacenados solo si se encuentran encriptados y dicha clave debe ser administrada por el Director Distrital o el encargado de tratamiento de datos.

Estrato 3

Los dispositivos de almacenamiento o de respaldo de información que se usen en la Dirección Distrital Educación 23D01, tienen que necesariamente estar encriptados y mantenidos con certificados digitales.

Estrato 4

Los ficheros y directorios que contengan información sensible de los usuarios, tienen que estar correctamente encriptados.

Anexo B

Posibles amenazas que pueden afectar la integridad de los datos. Dirección Distrital Educación 23D01.

Es importante conocer cuáles pueden ser las amenazas que pueden vulnerar la integridad de los datos para que de esta manera se proceda a implementar mecanismos de seguridad para su mitigación.

Tabla 69 Clasificación de las amenazas que pueden suscitarse en la Dirección Distrital Educación 23D01

Nivel	Clasificación de las amenazas	Descripción
1	Divulgación causada inintencionalmente también llamada como (accidental).	Esto se puede dar cuando un funcionario de la Dirección Distrital, sin su voluntad, da a conocer información sensible de un usuario (estudiante, docente, autoridad, comunidad educativa). Un ejemplo de esto se da cuando el funcionario envía un correo electrónico a una dirección incorrecta.
2	Funcionario curioso.	Un servidor público con privilegios de control total a los datos de un usuario husmea a estos por simple curiosidad o para usos personales. Ejemplo, un servidor público accede a la información sensible de una autoridad.
3	Violación a la privacidad de los datos.	Un funcionario accede a la información sensible de un usuario y la divulga públicamente sin ánimo de obtener un beneficio económico o por algún tipo de venganza hacia otro.

4	Violación de la privacidad de los datos con intrusión física por parte de un ajeno a la Dirección Distrital.	Sucede esto cuando un ente ajeno a la organización de manera física y con actos forzosos accede a la información del sistema.
5	Intrusión no autorizada en a la red del sistema	Este tipo de intrusión se da cuando un ente ajeno, ex funcionario, usuario o hacker que logra apoderarse de los sistemas de información desde el exterior y accede a los datos sensibles de los usuarios o realiza un ataque de denegación de servicios para que los sistemas dejen de funcionar.

Elaborado por: Investigador.

Fuente: (Sánchez-Henarejos et al., 2014)

Anexo C

Posibles amenazas que pueden afectar la integridad de los datos. Dirección Distrital Educación 23D01

En la siguiente tabla se da a conocer una lista de vulnerabilidades relacionadas con las amenazas y sus posibles vulneraciones a los datos personales. A continuación, se detallan una lista de vulnerabilidades relacionadas con las amenazas.

Activo	**Vulnerabilidades**	**Amenazas**	**Vulneración a los datos personales**
Hardware	Falta de mantenimiento	Fallo en el sistema de información personal	Pérdida o daño.
	No contar con un procedimiento para el reemplazo de equipos	Deficiencia en el performance del equipo	Pérdida, daño o destrucción.
	Almacenamiento no cifrado	Pérdida o robo de medios de almacenamiento electrónico.	Pérdida, copias no autorizadas, acceso o tratamiento no autorizado.
	No contar con procedimientos de destrucción de medios electrónicos.	Pérdida o robo de medios de almacenamiento electrónico.	Pérdida, copias no autorizadas, acceso o tratamiento no autorizado.
Software	Falta de actualizaciones referentes a parches de seguridad	Privilegios sin control en os usuarios.	Tratamiento, uso y acceso no autorizado.
	Sesiones iniciadas sin el usuario autorizado frente al computador.	Acceso no autorizado a los sistemas.	Tratamiento, uso y acceso no autorizado.
	Inadecuado borrado de información sensible.	Acceso de personas a información confidencial.	Tratamiento, uso y acceso no autorizado.
	Error en la asignación de privilegios de acceso.	Acceso a los sistemas de información	Tratamiento, uso y acceso no autorizado.
	Interfaces sin estándares de usabilidad	Errores operacionales en los sistemas de información.	Tratamiento, uso, acceso no autorizado, daño, alteración o modificación.

Redes	Carencia de mecanismos de autentificación e identificación de usuarios.	Falsificación de usuarios.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.
	Contraseñas no cifradas	Penetración en los sistemas de información.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.
	Mal uso de protocolos de Red.	Intrusión a los datos de los usuarios.	Tratamiento, uso y acceso no autorizado.
	Carencia de monitoreo de los componentes de las redes.	Canales encubiertos y tráfico clandestino.	Tratamiento, uso y acceso no autorizado.
	Descarga de aplicaciones sin control.	Código malicioso ejecutado.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.
Personal	Carencia de cultura en seguridad de la información.	Fraude y robo.	Tratamiento, uso y acceso no autorizado.
	Admisión de personal incorrecto.	Fraude y robo.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.
	Incorrecto uso de hardware y software.	Errores operacionales de los sistemas de información.	Perdida, destrucción tratamiento, uso y acceso no autorizado.
	Falta de auditorías internas en el uso de sistemas de	Fuga de información sin control.	Perdida, destrucción tratamiento, uso y acceso no autorizado.

	información por parte de los servidores públicos.		
Dirección Distrital	Carencia de documentos o contratos para el tratamiento de datos personales.	Consecuencias legales.	Perdida, destrucción tratamiento, uso y acceso no autorizado.
	Carencia de políticas de uso de correo electrónico.	Fugas de información.	Perdida, destrucción tratamiento, uso y acceso no autorizado.
	Falta de procedimientos en casos de un incidente o vulneración.	Fuga o robo de datos.	Perdida, destrucción tratamiento, uso y acceso no autorizado.
	Carencia de mecanismos de autentificación e identificación de usuarios.	Falsificación de usuarios.	Pérdida, daño, destrucción, robo, tratamiento uso y copias no autorizadas, alteración de los datos personales.

Elaborado por: Investigador.

Fuente: (Ifai, 2014)

Anexo D

Mecanismos y controles para reducir las vulnerabilidades existentes. Dirección Distrital Educación 23D01.

En el presente anexo se detallan mecanismos de seguridad con los que se pretenden minimizar las vulnerabilidades que pueden presentarse en la Dirección Distrital Educación 23D01.

Objetivo de control	Detalle
Políticas aplicadas en el modelo de gestión de datos personales	
Políticas de gestión de datos personales.	El directorio debe tener aprobadas las políticas de gestión de datos personales, de igual manera la implementación y mantenimiento de controles y mecanismos establecidos para la salvaguardar los datos sensibles de la Dirección Distrital.
Monitoreo y Evaluación.	Las políticas deben ser monitoreadas y auditadas para comprobar si es que se las está cumpliendo con normalidad, asimismo cuando exista un nuevo riesgo.
Cumplimiento Legal	
Identificación la legislación aplicable.	Es importante identificar los deberes y responsabilidades de los servidores públicos de la Dirección Distrital Educación 23D01 referente al tratamiento de datos personales y sus consecuencias legales en caso de que se incumpla con algún derecho de los usuarios.
Registros de evidencia	Se debe mantener en lo máximo posible cualquier documentación que en un futuro sean como descargo de evidencia ante una vulneración en los datos personales.
Recolección de evidencia.	La evidencia tiene que ser debidamente recolectada en caso de alguna vulnerabilidad que haya sido explotada.
Revisión del cumplimiento técnico.	Debe existir revisiones periódicas de los activos, así como de los controles, de manera tal que se verifique el correcto funcionamiento, así como de las amenazas y vulnerabilidades existentes.
Clasificación y acceso a los activos	
Inventario y clasificación de los datos personales	Se debe contar con un registro de datos personales capturados y tratados por la Dirección Distrital en cualquier medio de almacenamiento, prestando total atención a los datos sensibles.
Inventarios de activos	Bajo el concepto de que la información hoy en día se considera como el bien más preciado de toda organización, se debe tener un de los activos de información, identificando a los usuarios que cuentan con responsabilidad sobre los datos personales.

Identificación del ciclo de vida de un dato en la Dirección Distrital.	Es recomendable tener identificado el ciclo de vida de un dato o tipo de información sensible que reposa sobre los medios de almacenamiento de la Dirección Distrital y cuál es su tratamiento.
Seguridad Personal	
Identificar responsabilidades de cada funcionario de la Dirección Distrital.	Es importante que el personal que labora en la Dirección Distrital conozca de las responsabilidades que tiene en el tratamiento de datos sensibles de los usuarios, de igual manera de las sanciones que pueden desencadenar del mal tratamiento de los mismos.
Selección del personal mediante filtros.	El personal a ser contratado por la Dirección Distrital para el manejo de sistemas en los que se involucren datos de carácter sensible, tiene que ser debidamente investigado mediante filtros como: referencias personales, formación académica y antecedentes legales y laborales.
Acuerdo de confidencialidad.	El nuevo personal contratado debe firmar acuerdos de confidencialidad, así como de no divulgación de información sensible.
Capacitación.	El personal debe estar constantemente capacitado y recibir programas de concienciación referente a la seguridad de la información y protección de datos personales.
Proceso disciplinario.	La Dirección Distrital tiene que disponer de un proceso disciplinario para aquellos funcionarios que no cumplan con lo establecido en la política de tratamiento de datos sensibles.
Seguridad Física	
Control perimetral	Identificar si existe control de acceso perimetral, es decir, puertas con control de acceso, guardias, cámaras de seguridad, entre otros.
Seguridad de cableado	Se debe evaluar el estado de las conexiones de cableado, ya que con esto se impide la intercepción por parte de terceros.
Control de los activos fuera de las instalaciones	La Dirección Distrital debe contar con mecanismos para controlar que ningún activo con información sensible salga de la misma.
Destrucción segura de la información.	Cuando se de baja cualquier activo que contengan datos sensibles como medios de almacenamiento, tiene que aplicársele borrado seguro. Este borrado tiene que registrarse para futuras auditorias.
Escritorio limpio	Cuando un reporte o informe que contenga información sensible no se lo esté utilizando se lo debe de almacenar en lugares seguros fuera del alcance de terceros.
Control ante robo	La organización tiene que auditar e identificar los activos que contengan información sensible y sean susceptibles a cualquier tipo de robo.

Gestión de operaciones	
Control de cambios operacionales.	Se recomienda tener procedimientos para documentar y evaluar cualquier cambio que afecte el tratamiento de datos personales.
Segregación de tareas	Se recomienda aislar las funciones, operaciones y responsabilidades en el tratamiento de datos personales.
Protección ante malware	Es recomendable capacitar y concienciar a los funcionarios para que: 5. No instalen cualquier aplicativo en PC's que sirvan para el tratamiento de datos personales. 6. Mantener o informar para que sus computadores se encuentren debidamente actualizados. 7. Reportar cualquier acción fuera de lo normal en las mencionadas computadoras.
Registros y auditorías a los funcionarios	El encargado de tratamiento de datos personales debe realizar auditorías para que se analice los registros en los que se han visto expuesto los datos personales.
Controles de Red	El administrador de la red tiene que tener segmentada la red y los recursos que se comparten con normalidad y los que tienen que ser restringidos.
Administración de medios de almacenamiento secundario.	Tiene que existir políticas y procedimientos para la utilización de medios extraíbles como discos duros externos, CD, DVD, pendrive entre otros.
Seguridad de medios que son movilizados	Debe existir mecanismos de protección para asegurar el transporte de medios que por alguna u otra razón tienen que ser transportados con mecanismos como contraseñas, encriptación, entre otros.
Manejo de correo electrónico y mensajería instantánea.	El personal debe hacer uso correcto y seguro de correo electrónico, mensajería instantánea, haciendo uso de mecanismos que mitiguen la recepción de ficheros que en su estructura contenga código malicioso.
Disociación de datos	Los datos deben almacenarse de manera aislada para que con esto no contribuyan con información valiosa y haga una persona como identificable.
Control de acceso	
Normas de control de acceso	La organización debe contar con normas y privilegios para cada usuario limitando el uso de los sistemas de información según su perfil.

Manejo de usuarios y claves de seguridad	Los funcionarios deben ser identificados en el sistema para que pueda ser controlada la actividad que realizan dentro de los sistemas de información. Además, todos los funcionarios tienen que mantener el sigilo referente al manejo de contraseñas y de los controles que se realizan a los funcionarios.
Computadores que dejen de usarse	Los computadores tienen que estar configurados para que cuando un funcionario de la organización lo deje de utilizar se suspenda o cierre sesión de manera automática.
Accesos externos a sistemas de información	La organización debe contar con mecanismos como protocolos de autenticación, cifrado, conexiones mediante claves públicas, entre otros, para que con esto se brinde seguridad cuando un usuario habilitado se conecte a los sistemas de información.
Segregación de redes	Se debe utilizar mecanismos de seguridad que permitan separar a los usuarios el acceso a la red. Estos mecanismos pueden ser utilización de servicios como Firewalls, VPN, entre otros.
Controles de inicio de sesión	Cualquier acceso a la información sensible se la debe realizar mediante inicios de sesión seguros.
Trazabilidad de tratamiento	Este control permite identificar al funcionario que accedió a los datos personales y que tratamiento realizó sobre ellos.
Asilamiento de datos sensibles	El encargado del tratamiento de datos debe auditar y evaluar los activos que manejen datos sensibles para que se los coloque en entornos aislados.
Uso de dispositivos móviles internos.	Dentro de este grupo se encuentran las laptops, netbooks, tablets, smartphones que se ha entregado a los funcionarios. De este modo debe existir planes y acuerdos de concientización de las consecuencias que puedan generarse si estos llegaran a perderse.
Mantenimiento de sistemas	
Cifrado	El encargado de protección de datos tiene que identificar los datos que por su naturaleza tienen que estar protegidos mediante cifrado.
Firmas Electrónicas	Para la verificación y validación de los documentos enviados como recibidos se pueden aplicar técnicas como firmas electrónicas.
Vulneraciones de seguridad	
Procedimientos para el manejo de incidentes	La Dirección Distrital tiene que implementar procedimientos para el manejo de incidentes, debido a que al tenerlos se puede dar pronta y efectiva respuesta a cualquier incidente de vulnerabilidades y para que posteriormente se realice tareas de corrección.

Procedimientos en caso de incidentes.	Se tiene que contar con procesos tales como reporte, seguimiento, mitigación y registro documental de un altercado de seguridad, de tal manera que se pueda verificar
Reportes de incidentes de seguridad	Para que un reporte sea válido, este debe pasar por un proceso formal y seguir un protocolo para su validación.
Reporte de fallo en funcionamiento	La organización debe contar con un proceso formal para reportar fallos en producción de hardware como de software.
Procedimientos de notificación de vulnerabilidades a los titulares de datos.	La Dirección Distrital debe manejar procedimientos referentes a la notificación de vulnerabilidades de los datos de los titulares cuando se vean afectados sus derechos. Dentro de estos procedimientos se tiene que constar la magnitud de la vulneración y los mecanismos de protección que los titulares de los datos necesiten.
Aprendizaje de incidentes	Cuando se requiera, se debe establecer mecanismos para monitorear, el tipo, volumen y afectaciones de la vulnerabilidad.
Procedimientos de actualización del modelo de gestión	Es importante que luego de cada incidente se revise, evalué y actualice los mecanismos de seguridad aplicados para que con esto se aplique la mejora continua del modelo de gestión.

Elaborado por: Investigador.

Fuente: (Ifai, 2014)

Anexo E. Registro de Actividades.

El o los responsables deberán mantener un registro de actividades del tratamiento de datos personales que se encuentren en su custodia con el fin de salvaguardar su confidencialidad, integridad y disponibilidad. A continuación, se detallan las actividades que tienen que documentarse en el proceso de tratamiento de datos personales:

Descripción del tratamiento:

Responsable del tratamiento	
Apellidos y Nombres:	
Cedula de Ciudadanía:	
Dirección:	
Teléfono:	
Correo electrónico:	

Descripción del tratamiento:	
Actividades del tratamiento:	Se tiene que describir que actividad relacionada al tratamiento de datos personales se harán constar, por ejemplo: Gestión de datos de estudiantes, atención ciudadana, datos financieros de los funcionarios, entre otros.
Finalidad del tratamiento:	Se detalla cual será el objetivo del tratamiento.
Interesados:	Se tiene que identificar mediante un listado los usuarios, interesados y personas que resulten afectados en el tratamiento de datos en una determinada actividad.
Categorías de datos:	Se detallan a tipos de datos se les realizará el tratamiento, por ejemplo: datos de salud, datos financieros, datos identificativos.

Ciclo de vida de la actividad del tratamiento de datos:

1.- Captura de los datos	
Actividades del proceso:	Tiene que detallarse los procesos que intervienen en la recolección de datos, entre ellos pueden

	hacerse constar: datos receptados por atención en línea, atención ciudadana, currículo vitae, formularios, encuestas, entre otros.
Datos tratados:	Detalle del tipo de datos que se capturan.
Intervinientes:	Se tiene que identificar mediante un listado los usuarios, interesados y personas que resulten afectados en la captura de datos en una determinada actividad.
Tecnologías:	Formatos tecnológicos que se utilizan en el proceso de recolección de datos personales, por ejemplo: Quipux, correo electrónico, Mogac (módulo de gestión de atención ciudadana), entre otros.
2.- Almacenamiento de los datos	
Actividades del proceso:	Descripción de los procesos que intervienen en el almacenamiento de la información.
Datos tratados:	Detalle del tipo de datos que se capturan.
Intervinientes:	Se tiene que identificar mediante un listado los usuarios, interesados y personas que resulten afectados en el almacenamiento de datos en una determinada actividad.
Tecnologías:	Tecnologías que intervienen en el almacenamiento de la información.
3.- Uso y Tratamiento de datos.	
Actividades del proceso:	Descripción del tratamiento o procesamiento que se le da a los datos personales.
Datos tratados:	Detalle del tipo de datos sobre los que se le dan tratamiento.
Intervinientes:	Usuarios que utilizan, manejan y procesan los datos personales.

Tecnologías:	Detalle de las tecnologías que se utilizan para el tratamiento de la información.
4.- Transferencia y Cesiones	
Actividades del proceso:	Descripción del proceso que conlleva el cese de la información.
Datos tratados:	Detalle del tipo de dato que se les da cesamiento.
Intervinientes:	Usuarios que intervienen en el cese de datos.
Tecnologías:	Detalle de las tecnologías que se utilizan para dar de baja a los datos personales.
5.- Destrucción de los datos	
Actividades del proceso:	Descripción del proceso que conlleva la destrucción de la información.
Datos tratados:	Detalle de los tipos de datos que se destruyen.
Intervinientes:	Usuarios que destruyen los datos personales.
Tecnologías:	Detalle de las tecnologías que se utilizan para destruir la información.

Anexo F. Contrato de confidencialidad con terceros.

Santo Domingo de los Tsáchilas, dd/mm/aa

CONTRATO DE CONFIDENCIALIDAD DE TRATAMIENTO DE DATOS POR PARTE DE TERCEROS DE LA DIRECCIÓN DISTRITAL EDUCACIÓN 23D01 DE LA CIUDAD DE SANTO DOMINGO.

Comparecen a la celebración del presente Acuerdo de Confidencialidad, por una parte, **Apellido Paterno Apellido Materno Primer Nombre Segundo Nombre**, con cédula de identidad Nro. **xxxxxxxxx-x**, **Cargo del solicitante**, que, de aquí en adelante, para efectos de este acuerdo. se le denominará el SOLICITANTE, y por otra parte la Dirección Distrital Educación 23D01 representado por el señor **Apellidos y Nombres del Encargado del tratamiento de datos**, con cedula de identidad número **xxxxxxxxx-x**, en calidad de Oficial de Seguridad de la Información, que para efectos de este acuerdo se le denominara RESPONSABLE DE LA ENTREGA DE LA INFORMACIÓN, quienes libre y voluntariamente, acuerdan suscribir el presente acuerdo de confidencialidad, de conformidad con las siguientes cláusulas.

CLÁUSULA PRIMERA. - ANTECEDENTES

1. Constitución de la República del Ecuador

El **Artículo 66**, de la Constitución de la República del Ecuador, reconoce y garantiza, en su numeral 19, "*El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley (...)*.

El **Artículo 18** del mismo cuerpo legal expresa en su numeral 2.- *Acceder libremente a la información generada en entidades públicas, o en las privadas que*

manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información".

2. Código Orgánico Integral Penal

El **Artículo 178** de Código Orgánico Integral Penal establece: *"La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años..."*

El **Artículo 229** del código ibidem. manifiesta: "*La persona que, en provecho propio o de un tercero, revele información registrada, contenida en fichero, archivos, bases de datos o medios semejantes. a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones: materializando voluntaria e intencionalmente la violación del secreto. la intimidad y la privacidad de las personas. será sancionada con pena privativa de libertad de uno a tres años."*

3. Ley del Sistema Nacional de Registro de Datos Públicos

El **Articulo 4** de la Ley del Sistema Nacional de Registro de Datos Públicos, prescribe. "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos. son responsables de la integridad. protección y control de los registros y bases de datos a su cargo.

Dichas instituciones responderán por la veracidad, autenticidad. custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando ésta o éste provee toda la información.

Las personas afectadas por información falsa o imprecisa. difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes. previo el ejercicio de la respectiva acción legal.

La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución."

Artículo 6.- *Accesibilidad y confidencialidad - Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia. estado de salud. orientación sexual. religión. condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales" (...)*

El inciso tercero del articulo 6 ibidem, señala: *La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos."*

El inciso quinto del mismo cuerpo legal, manifiesta: La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad." (...)

El artículo 27 del mismo cuerpo legal establece: "Responsabilidad del manejo de las licencias. - Las Registradoras o Registradores y máximas autoridades, a quienes se autoriza el manejo de las licencias para el acceso a los registros de datos autorizados por la ley, serán las o los responsables directos administrativa, civil y penalmente por el mal uso de las mismas."

4. Ley Orgánica de Transparencia y Acceso a la Información Pública expresa:

Artículo 5.- *Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas,*

que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

Articulo 6.- *Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.*

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.

No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas (...)".

Artículo 17.- de la información reservada. - No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos, de acuerdo a literal b "Las informaciones expresamente establecidas como reservadas en leyes vigentes"

5. Acuerdos

Mediante Acuerdo Ministerial No. 166 de 19 de septiembre de 2013, publicado en el Registro Oficial Suplemento No. 88 de 25 de septiembre de 2013, el señor Cristian Castillo Peñaherrera, Secretario Nacional de la Administración Pública acuerda disponer a las entidades de la Administración Pública Central. Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. Para lo cual las entidades de la Administración Pública implementarán el Esquema Gubernamental de Seguridad de la Información (EGSI).

El Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013, en el numeral 2.5. *"Acuerdos de Confidencialidad", literal a), determina la elaboración y aprobación*

de acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGS1".

CLÁUSULA SEGUNDA. - OBJETO

El objeto del presente Acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo la información de terceros y la que se genere de los procesos que se gestionen el MINEDUC.

CLÁUSULA TERCERA. - CONFIDENCIALIDAD ESTADÍSTICA O SECRETO ESTADÍSTICO

3.1. La legislación estadística garantizará la confidencialidad de los datos de los informantes. prohibiendo su uso en temas no relacionados a fines estadísticos. tales como: tributarios, militares o policiales

3.2. El personal estadístico del Sistema Estadístico Nacional, contará con procedimientos formales, para comunicar a las fuentes acerca del compromiso de confidencialidad. los usos primordiales y limitaciones de acceso a la información que proporcionan.

3.3. El Sistema Estadístico Nacional contará con protocolos que establezcan directrices sobre seguridad e integridad de las bases de datos estadísticos.

3.4. Los datos amparados por el secreto estadístico nacional. pueden ser intercambiados o compartidos entre los integrantes del Sistema Estadístico Nacional: únicamente con fines estadísticos y analíticos, para lo cual se justificará su uso. y además firmar acuerdos que garanticen la confidencialidad de los mismos. en este sentido el secreto estadístico se mantiene bajo la noción de transferencia de responsabilidad del mismo entre las entidades del Sistema Estadístico Nacional.

3.5. El personal encargado de la producción de estadísticas oficiales suscribirá acuerdos de confidencialidad estadística, cuyo incumplimiento puede conllevar a sanciones.

3.6. Los usuarios internos y externos del Sistema Estadístico Nacional, que acceden a las fuentes y datos individuales, para fines estadísticos y analíticos, estarán obligados a firmar acuerdos de confidencialidad estadística y a preservar en secreto dicha información, aún después de concluir su vinculación con las entidades del Sistema Estadístico.

3.7. Se asegurará que la difusión y publicación de las estadísticas oficiales no permita la identificación individual de las fuentes.

3.8. Las bases de datos con la información individual de las fuentes, se archivará de acuerdo a los protocolos de seguridad y confidencialidad determinados por la entidad custodia de las mismas.

CLÁUSULA CUARTA. - EXCLUSIVIDAD DE USO

4.1. Una vez que tenga acceso a la Información Confidencial, el/la SOLICITANTE procederá a utilizarla exclusivamente para los fines y en forma determinados en la cláusula segunda del presente acuerdo.

4.3. El/la solicitante no podrá archivar la información en medios de almacenamiento personal. físicos o digitales.

4.2. La Información Confidencial no podrá ser divulgada o compartida con ninguna otra persona o entidad, sin el previo consentimiento por escrito por parte del MINEDUC.

CLÁUSULA QUINTA. - FORMATO DE ENTREGA DE INFORMACIÓN CONFIDENCIAL

El/la SOLICITANTE tendrá acceso a la Información Confidencial a través de medios magnéticos, de conformidad al requerimiento realizado por el/la solicitante.

CLÁUSULA SEXTA. - RECEPCIÓN

El/la SOLICITANTE manifiesta expresamente su conformidad con la Información Confidencial a la que tiene acceso y procede a recibirla a satisfacción.

CLÁUSULA SÉPTIMA. - CONFIDENCIALIDAD

7.1. El/la SOLICITANTE deberá tratar de manera estrictamente confidencial la información que no haya sido difundida de manera oficial por parte del MINEDUC o se vuelva parte del dominio público sin incumplimiento del presente Acuerdo y no podrá transferirla, difundirla. publicitaria o cederla por ningún medio físico o electrónico. conforme a lo acordado en el presente Acuerdo.

7.2. Toda información Confidencial procesada en la Institución es de propiedad exclusiva del MINEDUC: por tanto, ningún solicitante podrá hacer uso de la misma para su beneficio personal e independiente y de terceros.

CLÁUSULA OCTAVA. - RESPONSABILIDADES Y SANCIONES

El/la solicitante declara conocer las responsabilidades y sanciones a la que se someterá por el incumplimiento de la Política de Seguridad de la Información, políticas y procedimientos relacionados y el presente Acuerdo de confidencialidad, sin perjuicio de las responsabilidades civiles o penales. de conformidad con la Constitución de la República del Ecuador y demás legislación vigente.

CLÁUSULA NOVENA. - VIGENCIA

9.1. El Acuerdo de Confidencialidad entrará en vigencia a partir de la fecha de su suscripción. Las partes expresamente declaran que la vigencia del Acuerdo será del plazo en el cual se cumpla el objeto del presente instrumento.

CLÁUSULA DÉCIMA. - LEY Y JURISDICCIÓN APLICABLE

10.1. Las Partes comprometen sus mejores esfuerzos para resolver de mutuo acuerdo, en el marco de la buena fe contractual, las indefiniciones diferencias, diferendos y/o controversias que se susciten con motivo de la interpretación, cumplimiento, eventual ejecución y/o extinción del presente Acuerdo.

10.2. Este Acuerdo se regirá e interpretará de conformidad con las leyes de la República del Ecuador y se someterá a la jurisdicción de sus jueces y tribunales.

En expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo de Confidencialidad las partes suscriben en (2) dos ejemplares de un mismo tenor y a un sólo efecto.

Santo Domingo de los Tsáchilas, a __ de _____ del ___.

Solicitante	Responsable de la entrega de la información
_____	_____
Apellidos y Nombres C.I xxxxxxxxx-x **Cargo**	Apellidos y Nombres C.I xxxxxxxxx-x **Oficial de Seguridad de la información- Dirección Distrital Educación 23D01**

Anexo G. Contrato de confidencialidad con funcionarios.

Yo, **APELLIDOS Y NOMBRES**, identificado(a) con documento de identidad **xxxxxxxxx-x**, como servidor público del Ministerio de Educación (MINEDUC), comprendo que durante mis labores en la institución tendré acceso a información confidencial y por esto me comprometo a no divulgar ningún tipo de información perteneciente al MINEDUC con propósitos diferentes a los descritos en mis funciones dentro de la institución.

CLÁUSULA PRIMERA. - DECLARATORIA DE CONFIDENCIALIDAD:

1. El servidor público se compromete a usar los recursos de información y tecnológicos del MINEDUC de manera legal, profesional y ética; es corresponsable solidario de mantener la misma de forma Confidencial, Íntegra y Disponible, lo que significa cumplir y hacer cumplir todos los procesos y políticas que garanticen el procesamiento seguro y confidencial de la información a la que tiene acceso dentro de sus labores profesionales.

2. El servidor público ha sido informado y acepta que el MINEDUC es el titular de la Información Institucional, la que comprende toda la información física o digital, recibida o generada durante los procesos estratégicos, operativos y de apoyo, así como la información relacionada a la correspondencia física o virtual y que se encuentra bajo su custodia en archivos físicos temporales o permanentes, bases de datos, redes electrónicas, sistemas de información institucionales, aquella almacenada en los recursos tecnológicos a nivel de usuario; y/o, la información que se encuentren en etapa de gestión en los procesos internos.

3. El servidor público declara que ha leído el Acuerdo de confidencialidad y acepta que la Información Institucional, es inalterable y de propiedad exclusiva del Ministerio de Educación, desde el momento en que le es comunicada o transferida, ya sea de manera electrónica o física, o por cualquier otro medio de comunicación que use el Ministerio de Educación del Ecuador.

4. El servidor público acepta que en atención a la naturaleza de la información y a los riesgos que el mal uso y/o divulgación de la misma implican para el Ministerio de Educación del Ecuador, está obligado a mantener en forma estrictamente reservada toda información confidencial o reservada como tal de acuerdo a la Ley Orgánica de Transparencia y Acceso a La Información Pública (LOTAIP) en sus artículos 6, 17, 18, y demás información sensible que se le proporcione o a la que tenga acceso en función del cargo que desempeña; por lo tanto se obliga a abstenerse de usar, disponer, divulgar y/o publicar por cualquier medio, oral o escrito, o ceder a terceros sin autorización debidamente documentada y aprobada, y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los intereses del Ministerio de Educación del Ecuador.

CLÁUSULA SEGUNDA. - OBLIGACIONES:

1. Es obligación del servidor público utilizar la información a la que tiene acceso en razón de su trabajo, únicamente para los fines legítimos y propios de sus labores, y a las disposiciones del Jefe de la unidad a la que pertenece. De igual forma, es deber de servidor público abstenerse de acceder a la información que no le haya sido autorizada, asignada o permitida, por lo cual dicha información oficial no puede, por ninguna circunstancia, ser usada para provecho o ventaja personal de los servidores públicos, sus familias o cualquier otra persona, ni en detrimento de terceros.

2. El servidor público no accederá a la información que el MINEDUC recopile o genere, a menos que su cargo o función lo requiera específicamente.

3. El servidor público no debe revelar sin autorización expresa, bajo ningún medio (electrónico, verbal o físico), la información sensible que maneja el MINEDUC que sea y confidencial misma que incluye pero no se limita a: información de los estudiantes, sus familiares, datos personales, números de cédula, información considerada como confidencial del colegio y/o escuela, y además los

planes de negocio y/o institucionales, programas, cartera de proyectos internos o externos, documentos relacionados con concursos públicos, rutinas de trabajo u otros aspectos que estén vinculados con la gestión y control del Ministerio de Educación del Ecuador.

4. La información será revelada únicamente a través de los canales de difusión autorizados, lo cuales serán definidos por el MINEDUC de acuerdo a la Ley.

5. El servidor público debe mantener especial cuidado con la información considerada confidencial o sensible, la cual deberá ser almacenada de forma segura tanto en formato físico como electrónica, manteniendo resguardo permanente de la misma.

6. El Servidor público se obliga a mantener una política de escritorio limpio, y guardar bajo llave la información sensible evitando que quede sin protección o sea accesible por cualquier otro servidor público, o por terceros externos a la institución no autorizados.

7. Llevar registro y control de la información sensible que esté bajo su administración y custodia.

8. El Servidor público debe informar al Jefe de la unidad a la que pertenece en caso de encontrar irregularidades en cuanto al manejo o accesos no autorizados a la información sensible o confidencial que le ha sido asignada.

CLÁUSULA TERCERA. - SANCIONES:

El presente Acuerdo y su contenido representan una obligación formal de servidor público con el Ministerio de Educación del Ecuador, cualquier incumplimiento al mismo, se considera una falta disciplinaria por la cual se aplicarán las sanciones establecidas en la Ley Orgánica del Servicio Público, Ley Orgánica de Transparencia y Acceso a La Información Pública (LOTAIP) (LOTAIP) o por el Código de Trabajo, según corresponda, sin perjuicio de las acciones penales a que hubiere lugar.

CLÁUSULA CUARTA. - DECLARACIÓN:

El servidor público declara que conoce que aquellos datos o información de carácter personal e íntimo o institucional ostentan la calidad de confidencial y que son materia de protección en virtud de la Constitución y la Ley.

CLÁUSULA QUINTA. - VIGENCIA:

Los compromisos establecidos en el presente Acuerdo de Confidencialidad tendrán vigencia durante el tiempo que servidor público esté vinculado laboralmente con el MINEDUC y por al menos dos (2) años posteriores a la terminación de la relación laboral de servidor público(a), con el fin de preservar la experiencia profesional y la Información Institucional.

CLÁUSULA SÉPTIMA. - ACEPTACIÓN:

Para constancia de que el contenido del presente Acuerdo de Confidencialidad ha sido comunicado, conocido y entendido a cabalidad por parte de servidor público(a), quien en consecuencia acepta su contenido y se compromete a su fiel cumplimiento, por lo cual lo suscribe tres ejemplares de igual tenor y valor.

Dado en la ciudad de _____, a los 24 días del mes de mayo del 2019.

APELLIDOS Y NOMBRES DEL FUNCIONARIO

FIRMA

C.C.

Anexo H. Contrato de consentimiento de los usuarios.

La Dirección Distrital Educación 23D01 consciente de salvaguardar la integridad de sus datos personales pone en su conocimiento:

CLAUSULA PRIMERA. - ANTECEDENTES:

1. El artículo 66 numeral 19 del artículo 66 de la Constitución de la República del Ecuador: "Se reconoce y garantizará a las personas: (…) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley";
2. En virtud de lo señalado, cabe destacar que el artículo 85 numeral 1 de la Carta Magna dispone que "(…) la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y el buen vivir y todos los derechos (…)".
3. El artículo 178 del Código Orgánico Integral Penal establece: "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años…";
4. El artículo 229 del código ibidem, manifiesta: "Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años".
5. Todos los datos de carácter personal solicitados y entregados por usted, son almacenados en un fichero de titularidad a cargo del responsable de datos de nuestra organización.
6. Se le solicitará específicamente datos que servirán para los procesos y servicios enmarcados en los sistemas de información de nuestra institución. De igual manera, de ser necesario se solicitarán datos de terceros como (representantes legales, tutores, o personas a cargo designada por el titular de los datos).
7. Los datos almacenados cuentan con el compromiso de confidencialidad, con los mecanismos de seguridad necesarias, y en ninguno de los casos son cedidos a terceras personas sin su consentimiento, de su representante o tutor legal, excepto sea considerado necesario para la correcta prestación de servicios.

8. Cuando se realice las relaciones entre la Dirección Distrital Educación 23D01 y su persona, sus datos permanecerán almacenados por un lapso de tiempo de _____, mediante lo cual seguirá almacenado o según lo requiera será devuelto a su persona o representante legal de manera total e integra.
9. Según sea el caso sus datos serán cedidos a la Zona 4 de Educación del Ecuador, Subsecretaria de Educación o Ministerio de Educación según sea el caso.

CLÁUSULA SEGUNDAS. - PROHIBICIONES DEL SERVIDOR. -

El servidor no podrá:

- Modificar, alterar, divulgar, comercializar, o difundir la información a la que acceda.
- Publicar, difundir, ceder, trasmitir o permitir a terceros no autorizados el acceso a la información constante en los sistemas de información del MINEDUC.
- Conferir certificaciones registrales de la información a la que acceda.
- Revelar su clave de acceso al MINEDUC a terceros.
- Utilizar las claves de acceso cuando está haciendo uso de vacaciones o permisos institucionales.
- Enlazar y relacionar la información a la que acceda, con la información propia de la entidad solicitante sin prestar atención a las actualizaciones de la misma.
- Utilizar una IP que no ha sido registrada en el MINEDUC para acceder al servicio requerido.

Apellidos y nombre del usuario: _____ N°. Cedula: _____-_
Representante legal (menores): _____ N°. Cedula: _____-_
Dado en la ciudad de _____, a los __ días del mes de _____ 20__.

_____

FIRMA

Anexo I. Análisis de riesgos.

CATEGORIZACIÓN DE DATOS PERSONALES

¿En este proceso se van a tratar datos personales?

- **Sí**
- **No**

FINALIDADES DE TRATAMIENTO

¿En el proceso de captura de datos existen datos que van a ser tratados a gran escala? Por favor, detalle los puntos indicados en los siguientes ítems para determinar si se trata de un tratamiento a gran escala:

Según el proceso seleccione, el número de afectados:

- De 0 a 10.000
- De 10.000 a 100.000
- Mas de 100.000

Seleccione las categorías de los datos tratados:

- Transacciones de bienes y servicios
- Datos de carácter identificativo
- Datos especialmente protegidos
- Datos académicos y profesionales
- Detalles de empleo
- Información comercial
- Datos económicos y financieros

El tiempo de permanencia y tratamiento de los datos personales:

- Inmediato
- Días
- Semanas
- Meses
- Años

Indique la extensión geográfica del tratamiento:

- Regional
- Nacional
- Internacional

¿La información solicitada tiene como objetivo la monitorización o evaluación sistemática de aspectos personales mediante lo cual se puede determinar hábitos, comportamientos, preferencias hábitos, gustos, intereses de personas identificadas o identificables?

- Si
- No

¿La información solicitada tiene como finalidad el tratamiento de datos sensibles?

- Ideología u opiniones políticas
- Afiliación sindical
- Religión u opiniones religiosas
- Creencias o creencias filosóficas
- Origen étnico o racial
- Datos relativos a salud
- Vida sexual u orientación sexual
- Datos de violencia de género y malos tratos
- Datos biométricos
- Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica
- Datos solicitados para fines policiales sin consentimiento de las personas afectadas
- Datos relativos a condenas y delitos penales"

¿La captura de datos personales genera algún tipo de contacto con los interesados de tal manera que, este contacto, genere un acto intrusivo o que pueda ser intrusivo por medio del uso de tecnologías?

Por ejemplo, llamadas telefónicas de call-center, vigilancia electrónica, datamining, la biometría, técnicas genéticas o de geolocalización.

- Si
- No

¿El tratamiento de los datos genera que un gran número de personas tengan acceso a los mismos?

- Si
- No

TECNOLOGIAS EMPLEADAS PARA EL TRATAMIENTO

¿El uso de tecnologías para la captura, procesamiento y almacenamiento de los datos resultan o pueden ser consideradas como inmaduras, debido a que son tecnologías recién salidas al mercado o que por alguna razón representan algún tipo de riesgo?

- Si
- No

PERCEPCIONES DE LA EXISTENCIA UN RIESGO ELEVADO POR PARTE DEL RESPONSABLE DE LA ACTIVIDAD DE TRATAMIENTO

¿El tratamiento de esta información desencadena con una pérdida o alteración de la información?

- Si
- No

¿La información capturada es almacenada en papel?

- Si
- No

De ser así, indique las medidas que se aplican para salvaguardar esta información:

- Se almacena en un lugar seguro bajo llave.
- Se destruye la información confidencial
- Se la guarda mediante registro biométrico
- Otros

TERCEROS QUE INTERVENGAN EN EL TRATAMIENTO

¿Interviene algún proveedor en el proceso?

- Si
- No

De ser así, indicar el nombre de la entidad.

_____

Anexo J. Notificación de brechas de seguridad.

Ministerio de Educación	**MINISTERIO DE EDUCACIÓN**	**V 1.0** **Página** 211/2
	DIRECCIÓN NACIONAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES	
	NOTIFICACION DE BRECHA DE SEGURIDAD	

NOMBRE DE LA INSTITUCIÓN	**DIRECCIÓN DISTRITAL EDUCACIÓN 23D01**
DATOS DEL RESPONSABLE DE PROTECCIÓN DE DATOS:	**APELLIDOS Y NOMBRES** **NUMERO DE TELEFONO** **CORREO ELECTRONICO**
DETALLE SI SE TRATA DE UNA PRIMERA O SEGUNDA NOTIFICACIÓN DE VIOLACIÓN DE SEGURIDAD;	
FECHA Y HORA ESTIMADA DEL INCIDENTE:	
TIPO DE DATOS VULNERADOS:	
MECANISMOS DE SEGURIDAD APLICADOS:	
DETALLE ADICIONAL SOBRE LA VULERACIÓN DE DATOS:	
RESUMEN DETALLADO DEL INCIDENTE:	
NÚMERO ESTIMADO DE PERSONAS AFECTADAS:	

DOCUMENTO DE NOTIFICACIÓN A LOS AFECTADOS:	
CONTENIDO DE LA NOTIFICACIÓN:	
MEDIOS DE COMUNICACIÓN UTLIZADOS PARA LA NOTIFICACIÓN:	
CASOS DE VIOLACIÓN DE DATOS SENSIBLES DE LOS AFECTADOS:	

Firmado en Santo Domingo a los __ días del mes _____ del 20__,

_____

Apellidos y nombres

RESPONABLE DEL TRATAMIENTO DE DATOS PERSONALES

Anexo K. Certificado de desarrollo del trabajo de investigación.

MINISTERIO DE EDUCACIÓN

COORDINACIÓN ZONAL 4

Santo Domingo, 08 de octubre del 2019.

Ingeniero
Patricio Vaca Escobar
Presente

En atención al oficio ingresado S/N de fecha 08 de octubre del 2019 tengo a bien **CERTIFICAR:**

Que el trabajo de investigación titulado "Modelo de Gestión de Seguridad Lógica de la Información en la Protección de los Datos Sensibles de los Distritos de Educación del Ecuador" está elaborado en base al proyecto de Ley Orgánica de Protección de Datos Personales, Constitución del Ecuador, Marcos de Referencia (Iso 27001) y servirá de guía para nuestra entidad ya que no existe un modelo gestión de tratamiento de la Información hacia una cultura de la Seguridad Informática.

Con sentimiento de consideración.

Distrito 23D01 Alluriquin-Luz de América
Esfuerzo Toachi Periferia - Rio Verde
Santo Domingo Zaracay Rio Toachi - Chiguilpe
Coordinación Zona 4
Ministerio de Educación

Mg. Rosa Inés Carrión Cajamarca
DIRECTORA DISTRITAL 23D01 DE EDUCACIÓN
SANTO DOMINGO DE LOS TSÁCHILAS

Anexo L. Activos Informáticos de las unidades administrativas de la DD23D01

Computer	Operating system	RAM (MB)	CPU (MHz)	Model	IP address	Architecture	Service pack
ADMINISTRATIVO							
ADFN01	Microsoft Windows 7 Ultimate	4096	3101	H81MLV3	10.2.8.100	x86 64 bit	Service Pack 1
ADMN01	Microsoft Windows 7 Ultimate	3543	2833	HP Compaq 6000 Pro MT PC	10.2.8.131	x86 32 bit	Service Pack 1
ADMN02	Microsoft Windows 7 Professional	4096	3201	H81MLV3	10.2.8.102	x86 64 bit	Service Pack 1
ADMN03	Microsoft Windows XP Professional	2048	2933	DG41TY	10.2.8.103	x86 32 bit	Service Pack 3
ADMN04	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.104	x86 64 bit	Service Pack 1
ADMN05	Microsoft Windows 7 Professional	2048	1999	Satellite C645	10.2.8.4	x86 32 bit	Service Pack 1
UNIDAD DE ASESORIA JURÍDICA							
ASJR02	Microsoft Windows 7 Ultimate	2048	2833	HP Compaq dc5800 Small Form Factor	10.2.8.122	x86 32 bit	Service Pack 1
ASJR03	Microsoft Windows 7 Ultimate	2048	2933	HP Compaq 6000 Pro MT PC	10.2.8.123	x86 32 bit	Service Pack 1
ASJU01-PC	Microsoft Windows 7 Ultimate	2048	3000	HP Compaq dc5800 Microtower	10.2.8.121	x86 32 bit	Service Pack 1
UNIDAD DE APOYO SEGUIMIENTO Y REGULACIÓN							
ASRE01	Microsoft Windows 7 Ultimate	2048	2933	HP Compaq 6000 Pro MT PC	10.2.8.61	x86 32 bit	Service Pack 1
ASRE02	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.62	x86 64 bit	Service Pack 1

ASRE03	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.63	x86 64 bit	Service Pack 1
ASRE04	Microsoft Windows 7 Home Premium	2048	2133	HP Compaq dc5700 Small Form Factor	10.2.8.64	x86 32 bit	
ASRE05	Microsoft Windows 7 Ultimate	2048	2667	HP xw4600 Workstation	10.2.8.65	x86 32 bit	
ASRELT01	Microsoft Windows 7 Professional	4096	2501	Latitude E6540	10.2.8.221	x86 64 bit	Service Pack 1
ASRELT02	Microsoft Windows 7 Ultimate	4096	2501	Latitude E6540	10.2.8.178	x86 64 bit	Service Pack 1
UNIDAD ATENCIÓN CIUDADANA							
ATCI01	Microsoft Windows 7 Home Premium	3505	3500	OptiPlex 3020	10.2.8.41	x86 32 bit	
ATCI02	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.42	x86 64 bit	Service Pack 1
ATCI03	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.43	x86 64 bit	Service Pack 1
ATCI04	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.44	x86 64 bit	Service Pack 1
ATCI05	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.45	x86 64 bit	Service Pack 1
ATCI06	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.46	x86 64 bit	Service Pack 1
ATCI07	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.47	x86 64 bit	Service Pack 1
ATCI08	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.175	x86 64 bit	Service Pack 1

ATCI09	Microsoft Windows 7 Professional	4096	3400	HP ProDesk 400 G1 MT	10.2.8.49	x86 64 bit	Service Pack 1
DESP01	Microsoft Windows 7 Professional	4096	2501	HP ProBook 440 G1	10.2.8.242	x86 64 bit	Service Pack 1
DESP02	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.32	x86 64 bit	Service Pack 1
UNIDAD ADMINISTRATIVO FINANCIERO							
FNNC01	Microsoft Windows 7 Professional	4096	3201	HP ProDesk 400 G1 MT	10.2.8.101	x86 64 bit	Service Pack 1
FNNC02	Microsoft Windows 7 Ultimate	2048	2933	HP Compaq 6000 Pro MT PC	10.2.8.92	x86 32 bit	Service Pack 1
FNNC03	Microsoft Windows 7 Professional	2048	2833	HP Compaq dc5800 Microtower	10.2.8.93	x86 64 bit	Service Pack 1
FNNC04	Microsoft Windows 7 Ultimate	2048	3000	HP xw4600 Workstation	10.2.8.237	x86 32 bit	
FNNC05	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.95	x86 64 bit	Service Pack 1
FNNC06	Microsoft Windows 7 Starter	2048	3000	HP Compaq dc5800 Microtower	10.2.8.96	x86 32 bit	
PLNF01	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.72	x86 64 bit	Service Pack 1
UNIDAD DE PLANIFICACÓN							
PLNF02	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.73	x86 64 bit	Service Pack 1
PLNF03	Microsoft Windows 7 Ultimate	2048	3000	HP xw4600 Workstation	10.2.8.74	x86 32 bit	Service Pack 1
PLNFLT01	Microsoft Windows 7 Ultimate	3536	2535	Latitude E6500	10.2.8.183	x86 32 bit	Service Pack 1
UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN							

TICS01	Microsoft Windows 7 Professional	4096	3201	HP ProDesk 400 G1 MT	10.2.8.168	x86 64 bit	Service Pack 1
TICS02	Microsoft Windows 7 Professional	3514	3201	HP ProDesk 400 G1 MT	10.2.8.216	x86 32 bit	
TICS03	Microsoft Windows 7 Professional	4096	3101	HP Compaq 6200 Pro MT PC	10.2.8.50	x86 64 bit	Service Pack 1
TICSINS01	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.5	x86 64 bit	Service Pack 1
TICSINS02	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.245	x86 64 bit	Service Pack 1
TICSINS03	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.51	x86 64 bit	Service Pack 1
TICSINS04	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.210	x86 64 bit	
TICSINS05	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.168	x86 64 bit	Service Pack 1
TICSINS06	Microsoft Windows 7 Professional	6144	2601	HP 14 Notebook PC	10.2.8.207	x86 64 bit	Service Pack 1
TICSINS07	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.206	x86 64 bit	Service Pack 1
TICSINS08	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.165	x86 64 bit	Service Pack 1
TICSINS09	Microsoft Windows 7 Professional	4096	2601	HP 1000 Notebook PC	10.2.8.155	x86 64 bit	Service Pack 1

TICSLT01	Microsoft Windows 7 Ultimate	3580	2200	HP Pavilion dv4 Notebook PC	10.2.8.244	x86 32 bit	Service Pack 1
UNIDAD DE TALENTO HUMANO							
TTHH01	Microsoft Windows 7 Ultimate	3567	2667	HP xw4600 Workstation	10.2.8.111	x86 32 bit	Service Pack 1
TTHH02	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.112	x86 64 bit	Service Pack 1
TTHH03	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.113	x86 64 bit	Service Pack 1
TTHH04	Microsoft Windows 7 Ultimate	2048	3000	HP xw4600 Workstation	10.2.8.114	x86 32 bit	Service Pack 1
TTHH05	Microsoft Windows 7 Ultimate	2048	3000	HP xw4600 Workstation	10.2.8.115	x86 32 bit	
TTHH06	Microsoft Windows 7 Ultimate	1024	3000	HP Compaq dx2400 Microtower PC	10.2.8.116	x86 32 bit	Service Pack 1
UDAI01	Microsoft Windows 7 Professional	4096	3500	OptiPlex 3020	10.2.8.85	x86 64 bit	Service Pack 1
UNIDAD DE APOYO A LA INCLUSIÓN							
UDAI02	Microsoft Windows 7 Ultimate	3567	2667	HP xw4600 Workstation	10.2.8.87	x86 32 bit	Service Pack 1
UDAI03	Microsoft Windows 7 Ultimate	1024	2833	HP Compaq dc5800 Microtower	10.2.8.172	x86 32 bit	Service Pack 1

Anexo M. Listado de tramites que se ingresan a través del módulo de atención ciudadana.

	UNIDADES
1	**ADMINISTRACION ESCOLAR**
1.1	**ACEPTACIÓN DE LA PROPUESTA DEL PLAN DE GESTIÓN DE RIESGOS PARA I.E. PARTICULARES FISCOMISIONALES Y MUNICIPALES**
1.1.2	52. ACEPTACION PROPUESTA DEL PLAN DE GESTION DE RIESGOS PARA IE PARTICULARES, FISCOMISIONALES Y MUNICIPALES 20150504.PDF
1.1.3	FORMATO INFORME DE ACEPTACION DE PROPUESTA DEL PLAN DE RIESGOS.DOC Form
1.2	**APROBACIÓN DE MANTENIMIENTO DE INFRAESTRUCTURA DE INSTITUCIONES EDUCATIVAS**
1.2.1	51. APROBACIÓN DE MANTENIMIENTO DE INFRAESTRUCTURA DE IE 20150504.PDF
1.2.2	MANUAL DE MANTENIMIENTO DE IE 20150504.PDF
1.3	**APROBACIÓN PARA ASIGNACION DE ALIMENTOS ESCOLARES**
1.3.1	67. APROBACIÓN PARA ASIGNACIÓN DE ALIMENTOS ESCOLARES 20150701.PDF
1.3.2	FORMATO-SOLICITUD DE REQUERIMIENTO DE ALIMENTOS ESCOLARES 20150701.XLSX
1.3.3	EQUERIMIENTO DE ACTUALIZACION O INGRESO DE IE PARA ALIMENTOS.XLSX
1.4	**ASIGNACION DE TEXTOS**
1.4.1	FORMATO-REQUERIMIENTO DE TEXTOS 20150701.XLS
1.4.2	FORMATO-SOLICITUD DE REQUERIMIENTO DE TEXTOS YO UNIFORMES ESCOLARES 20150701.XLSX
1.4.3	49. APROBACIÓN PARA ASIGNACIÓN DE TEXTOS Y UNIFORMES 20150701.PDF
1.5	**ASIGNACION DE UNIFORMES**
1.5.1	FORMATO-INGRESO DE TALLAS 20150701.XLS
1.5.2	FORMATO-SOLICITUD DE REQUERIMIENTO DE TEXTOS YO UNIFORMES ESCOLARES 20150701.XLSX
1.5.3	49. APROBACIÓN PARA ASIGNACIÓN DE TEXTOS Y UNIFORMES 20150701.PDF
1.6	**SOLICITUD DE ADECUACIONES DE INFRAESTRUCTURA**
1.6.1	53. SOLICITUD DE ADECUACIONES DE INFRAESTRUCTURA 20150701.PDF
1.6.2	FORMATO SOLICITUD DE ADECUACIONES 20150701.DOC
2.	**APOYO Y SEGUIMIENTO**
2.1	**APELACIONES EN ÚLTIMA INSTANCIA PARA REVISIÓN DE NOTAS DE EXÁMENES**
2.1.1	APELACIONES DE ÚLTIMA INSTANCIA PARA REVISIÓN DE NOTAS DE EXÁMENES.PDF

2.2	**CERTIFICACION DE DUPLICADO DE ACTAS DE GRADO**
2.2.1	MANUAL DE PROCESO DE CERTIFICACION DE DUPLICADO DE ACTAS DE GRADO.PDF
2.2.2	PROCEDIMIENTO PARA LA VERIFICACION DE DATOS DE ANTIGUOS BACHILLERES DE IE DEL SISTEMA EDUCATIVO FISCAL (25 AñOS ATRAS).PDF
2.2.3	INSTRUCTIVO PARA LA EMISION DE DUPLICADOS DE TITULOS Y CERTIFICACION DE ACTAS DE GRADO.PDF
2.3	**DUPLICADO DE TITULOS**
2.3.1	MANUAL DE PROCESO DUPLICADOS DE TITULOS.PDF
2.3.2	PROCEDIMIENTO PARA LA VERIFICACION DE DATOS DE ANTIGUOS BACHILLERES DE IE DEL SISTEMA EDUCATIVO FISCAL (25 AñOS ATRAS).PDF
2.3.3	INSTRUCTIVO PARA LA EMISION DE DUPLICADOS DE TITULOS Y CERTIFICACION DE ACTAS DE GRADO.PDF
2.4	**EXAMENES DE UBICACION PARA QUIENES NO CUENTEN CON DOCUMENTACION DE ESTUDIOS EN LA EDUCACION ORDINARIA**
2.4.1	7. EXAMENES DE UBICACION PARA QUIENES NO CUENTAN CON DOCUMENTACION 20150701.PDF
2.4.2	FORMATO RESOLUCION DE EXAMENES DE UBICACION PARA QUIENES NO CUENTAN CON DOCUMENTACION.DOC
2.5	**HOMOLOGACION DE TITULOS DE BACHILLER REALIZADOS EN EL EXTERIOR**
2.5.1	2. RECONOCIMIENTO DE ESTUDIOS Y HOMOLOGACIÓN DE TÍTULOS EXTERIOR 20150701.PDF
2.5.2	TABLA DE EQUIVALENCIA MERCOSUR 20150701.PDF
2.5.3	TABLA_EQUIVALENCIAS_CONVENIO ANDRES BELLO_ACTUAL 20150701.PDF
2.5.4	MATRIZ HOMOLOGACION TITULOS RECONOCIMIENTO DE ESTUDIOS DEL EXTERIOR.XLSX
2.5.5	FORMATO RESOLUCION HOMOLOGACION TITULOS EXTERIOR V2.0.DOC
2.6	**MATRICULA EXCEPCIONAL**
2.6.1	3. MATRICULA EXCEPCIONAL 20140219.PDF
2.6.2	INSTRUCTIVO_DE_MATRICULA_CONTINUA-DNRE-2016.04.05.2016.PDF
2.7	**RATIFICACION DE GOBIERNO ESCOLAR**
2.7.1	34. RATIFICACIÓN DE GOBIERNO ESCOLAR 20150701.PDF
2.8	**RATIFICACIÓN DE VOCALES DE CONSEJO EJECUTIVO IE FISCOMISIONAL**
	33. RATIFICACIÓN DE VOCALES DE CONSEJO EJECUTIVO 20150701 úLITMO.PDF
2.9	**RATIFICACIÓN DE VOCALES DE CONSEJO EJECUTIVO IE PARTICULAR Y MUNICIPAL**

2.9.1	**33. RATIFICACIÓN DE VOCALES DE CONSEJO EJECUTIVO 20150701 úLITMO.PDF**
2.10	**RATIFICACIÓN DE VOCALES DE CONSEJO EJECUTIVO IE PUBLICA**
2.10.1	**33. RATIFICACIÓN DE VOCALES DE CONSEJO EJECUTIVO 20150701 úLITMO.PDF**
2.11	**RECONOCIMIENTO DE ESTUDIOS REALIZADOS EN EL EXTERIOR**
2.11.1	2. RECONOCIMIENTO DE ESTUDIOS Y HOMOLOGACIÓN DE TÍTULOS EXTERIOR 20150701.PDF
2.11.2	TABLA DE EQUIVALENCIA MERCOSUR 20150701.PDF
2.11.3	RESOLUCION RECONOCIMIENTO ESTUDIOS REALIZADOS EN EL EXTERIOR.DOC
2.11.4	MATRIZ HOMOLOGACION TITULOS RECONOCIMIENTO DE ESTUDIOS DEL EXTERIOR.XLSX
2.11.5	LINEAMIENTOS RECONOCIMIENTO DE ESTUDIOS EN EL EXTERIOR.PDF
2.12	**REGISTRO DE CODIGO DE CONVIVENCIA**
2.12.1	9. REGISTRO DEL CÓDIGO DE CONVIVENCIA 20150701.PDF
2.12.2	FORMATO MATRIZ DE REGISTRO CODIGO DE CONVIVENCIA 20150701.XLSX
2.13	**REGISTRO DE PROYECTO EDUCATIVO INTERINSTITUCIONAL PEI**
2.13.1	8. REGISTRO DEL PROYECTO EDUCATIVO INTERINSTITUCIONAL(PEI) 20140219.PDF
2.14	**TRASLADO DE ESTUDIANTES DE IE FISCAL A IE FISCAL DEL MISMO RÉGIMEN**
2.14.1	TRASLADO DE ESTUDIANTES DE IE A IE FISCAL.PDF
2.15	**TRASPASO DE TERCERA MATRICULA**
2.15.1	TRASLADO POR TERCERA MATRICULA.PDF
2.15.2	FORMATO DE RESOLUCION DE TRASLADO DE ESTUDIANTES POR TERCERA MATRICULA..DOCX.DOCX
2.15.3	INSTRUCTIVO DE TRANSFERENCIA DE ESTUDIANTES_2016-03-02.PDF
2.15.4	MINEDUC-DNRE-2016-00383-M.PDF
3	**ASESORIA JURIDICA**
3.1	**REQUERIMIENTOS DE PERSONAS JURÍDICAS SIN FINES DE LUCRO (ORGANIZACIONES SOCIALES)**
3.1.1	MANUAL DE PROCESOS ZONAL INGRESO Y REGISTRO DE REQUISITOS DE PERSONA JURIDICAS SIN FINES DE LUCRO.PDF
3.1.2	RESOLUCION APROBACION DE PERSONAS SIN FINES DE LUCRO.DOC
3.1.3	35. REQUERIMIENTOS DE PERSONAS JURIDICAS SIN FINES DE LUCRO (ORGANIZACIONES SOCIALES).PDF
3.1.4	FORMATO RESOLUCION APROBACION DE REFORMAS Y CODIFICACION DE ESTATUTOS.DOC Formato
4	**ATENCION CIUDADANA**

4.1	**CERTIFICACIÓN DE PROMOCIONES DE INSTITUCIONES EDUCATIVAS DESAPARECIDAS**
4.1.1	15. CERTIFICACIÓN DE PROMOCIONES DE IE DESAPERECIDAS 20150504.PDF
4.1.2	FORMATO DE CERTIFICADO DE PROMOCIONES DE IE DESAPARECIDAS.DOC
4.2	**CERTIFICADO DE REMUNERACIONES**
4.2.1	INSTRUCTIVO GENERACION DE PLANTILLA PARA CERTIFICADO DE REMUNERACIONES 20150504.PDF
4.2.2	PLANTILLA CERTIFICADO DE REMUNERACIONES 20150504.XLS
4.2.3	FORMATO CERTIFICADO REMUNERACIONES 20150504.DOCX
4.2.4	55. CERTIFICADO DE REMUNERACIONES 20150504.PDF
4.3	**CERTIFICADO DE TERMINACION DE EDUCACIÓN GENERAL BÁSICA**
4.3.1	12. CERTIFICADO DE TERMINACIÓN DE PRIMARIA O EDUCACIÓN GENERAL BÁSICA.PDF
4.3.2	FORMATO DE CERTIFICADO DE TERMINACION DE EGB.PPT
4.4.	**CERTIFICADO DE TERMINACION DE PRIMARIA**
4.4.1	12. CERTIFICADO DE TERMINACIÓN DE PRIMARIA O EDUCACIÓN GENERAL BÁSICA.PDF
4..4.2	FORMATO CERTIFICADO DE PRIMARIA.PPT
4.5	**CERTIFICADO DE TIEMPO DE SERVICIO**
4.5.1	FORMATO DE CERTIFICADO DE TIEMPO DE SERVICIO 20150701.DOC
4.5.2	40. CERTIFICADO DE TIEMPO DE SERVICIO 20150701.PDF
4.6	**DUPLICADO DE TITULO ARTESANAL**
4.6.1	22. DUPLICADO DE TÍTULO ARTESANAL 20140219.PDF
4.7	**INSCRIPCIÓN DE ESTUDIANTES CON DISCAPACIDAD**
4.7.1	65. INSCRIPCION DE ESTUDIANTES CON DISCAPACIDAD 20150701.PDF
4.7.2	INSTRUCTIVO DEL PROCESO EN UDAI- VF 20150701.PDF
4.7.3	FORMULARIO DE INSCRIPCIONES.XLSM
4.8	**INSCRIPCIÓN PARA JOVENES O ADULTOS CON ESCOLARIDAD INCONCLUSA**
4.8.1	64. INSCRIPCION PARA JOVENES O ADULTOS CON ESCOLARIDAD INCONCLUSA 20150701.PDF
4.8.2	MODELO DE ATENCION PARA PERSONAS CON ESCOLARIDAD INCONCLUSA 20150701.DOCX
4.8.3	BASE DE PREGUNTAS FRECUENTES BACHILLERATO INTENSIVO.DOC
4.8.4	FORMULARIO INSCRIPCIONES BASICA SUPFLEXIBLE.XLSM
4.8.5	FORMULARIO INSCRIPCIONES BACHILLERATO.XLSM
4.9	**LEGALIZACION CUADROS DE CALIFICACIONES QUIMESTRALES, FINALES Y PROMOCIONES DE INSTITUCIONES EDUCATIVAS**
4.9.1	LINEAMIENTOS_EXPEDIENTES_ACADÉMICOS_SIERRA_2014-2015 (V.2).PDF

4.9.2	19. LEGALIZACION DE CUADROS DE CALIFICACIONES QUIMESTRALES FINALES 20150401.PDF
4.10	**LEGALIZACION DE DOCUMENTACION PARA EL EXTERIOR**
4.10.1	18. LEGALIZACION DE DOCUMENTACION PARA EL EXTERIOR 20150504.PDF
4.11	**LEGALIZACION DE DOCUMENTOS DE GREMIOS Y ASOCIACIONES DE FORMACION ARTESANAL**
4.11.1	20. LEGALIZACION DE DOCUMENTOS DE GREMIOS Y ASOCIACIONES DE FORMACION ARTESANAL 20140219.PDF
4.12	**RECONOCIMIENTO DE ESTUDIOS DE CENTROS OCUPACIONALES**
4.12.1	23. RECONOCIMIENTO DE ESTUDIOS DE CENTROS OCUPACIONALES 20140219.PDF
4.13	**RECTIFICACION DE NOMBRES Y/O APELLIDOS DE DOCUMENTOS OFICIALES**
4.13.1	17. RECTIFICACION DE NOMBRES Y O APELLIDOS DE DOCUMENTOS OFICIALES 20150701.PDF
5	**COORDINACION EDUCATIVA / APOYO Y SEGUIMIENTO**
5.1	**APROBACION DE EVENTOS ESTUDIANTILES ORGANIZADO POR INSTITUCIONES EDUCATIVAS (CONCURSOS, FERIAS, FESTIVALES, CAMPEONATOS Y EXPOSICIONES)**
5.1.1	62. APROBACION DE EVENTOS ESTUDIANTILES 14082015.PDF
5.1.2	FORMATO DE FICHA TECNICA Y PLANIFICACION DE EVENTOS ESTUDIANTILES 20150601.DOCX
5.1.3	FORMATO PARA APROBACION DE EVENTOS 20150731.DOC
5.2	**APROBACIÓN DE MALLAS CURRICULARES PARA BACHILLERATO INTERNACIONAL**
5.2.1	57. APROBACION DE MALLAS CURRICULARES PARA BI 20150601.PDF
5.2.2	INFORME TECNICO MALLAS CURRICULARES BI.DOCX
5.3	**APROBACION DE PROPUESTAS DE INNOVACION CURRICULAR**
5.3.1	58. APROBACIÓN DE PROPUESTA DE INNOVACIÓN CURRICULAR 20150814.PDF
5.3.2	FORMATO DE RESOLUCION DE PROPUESTAS DE INNOVACION CURRICULAR.DOCX
5.3.3	INSTRUCTIVO PARA LA APROBACION DE PROPUESTA DE INNOVACION CURRICULAR.PDF
5.4	**REGISTRO DEL PROGRAMA DE PARTICIPACION ESTUDIANTIL**
5.4.1	56. REGISTRO DE ESTUDIANTES EN PROGRAMA DE PARTICIPACION ESTUDIANTIL 20150713.PDF
5.4.2	MATRIZ MIPPE_25042016.XLSX
6	**DESARROLLO PROFESIONAL / TALENTO HUMANO**
6.1	**JUBILACIÓN POR INVALIDEZ**

6.1.1	47. JUBILACIONES POR ENFERMEDAD CATASTROFICA O INVALIDEZ 20150701.PDF
6.1.2	FORMULARIO SOLICITUD DE JUBILACION POR ENFERMEDAD CATASTROFICA O INVALIDEZ.DOCX
7	**JUNTA DE RESOLUCION DE CONFLICTOS**
7.1	**DENUNCIA POR ABUSO DE AUTORIDAD**
7.1.1	1. DENUNCIAS 20150601.PDF
7.1.2	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.2	**DENUNCIA POR COBROS INDEBIDOS**
7.2.1	FORMATO DE FICHA DE DENUNCIA POR COBROS INDEBIDOS 20150601.DOCX
7.2.2	1. DENUNCIAS 20150601.PDF
7.2.3	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.3	**DENUNCIA POR COBROS INDEBIDOS DE INSTITUCIONES EDUCATIVOS FISCOMISIONALES**
7.3.1	1. DENUNCIAS 20150601.PDF
7.3.2	FICHA DE DENUNCIA POR COBROS INDEBIDOS 20150601.DOCX
7.4	**DENUNCIA POR COBROS INDEBIDOS DE INSTITUCIONES EDUCATIVOS MUNICIPALES**
7.4.1	1. DENUNCIAS 20150601.PDF
7.4.2	FICHA DE DENUNCIA POR COBROS INDEBIDOS 20150601.DOCX
7.5	**DENUNCIA POR COBROS INDEBIDOS DE INSTITUCIONES EDUCATIVOS PARTICULARES**
7.5.1	1. DENUNCIAS 20150601.PDF
7.5.2	FICHA DE DENUNCIA POR COBROS INDEBIDOS 20150601.DOCX
7.6	**DENUNCIA POR COBROS INDEBIDOS DE INSTITUCIONES EDUCATIVOS PÚBLICAS**
7.6.1	1. DENUNCIAS 20150601.PDF
7.6.2	FICHA DE DENUNCIA POR COBROS INDEBIDOS 20150601.DOCX
7.7	**DENUNCIA POR DELITOS SEXUALES**
7.7.1	1. DENUNCIAS 20150601.PDF
7.7.2	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.8	**DENUNCIA POR DROGAS**
7.8.1	1. DENUNCIAS 20150601.PDF
7.8.2	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.9	**DENUNCIA POR LESIONES**
7.9.1	1. DENUNCIAS 20150601.PDF
7.9.2	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.10	**DENUNCIA POR MALTRATO PSICOLOGICO**
7.10.1	1. DENUNCIAS 20150601.PDF
7.10.2	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.11	**DENUNCIAS VARIAS A INSTITUCIONES PARTICULARES**

7.11.1	1. DENUNCIAS 20150601.PDF
7.11.2	FORMATO DE FICHA DE DENUNCIA VERBAL 20150601.DOCX
7.12	**RECURSOS INTERPUESTOS (APELACIÓN A DENUNCIAS)**
7.12.1	68. RECURSOS INTERPUESTOS 20150701.PDF
8	**PLANIFICACIÓN**
8.1	**AUTORIZACION DE AMPLIACIÓN DE OFERTA EDUCATIVA DE INSTITUCIONES EDUCATIVAS FISCOMISIONALES**
8.1.1	26. AUT CREAC Y FUNC; CAMBIO DE DOM, AMP DE OF DE IE.PDF
8.2	**AUTORIZACION DE AMPLIACIÓN DE OFERTA EDUCATIVA DE INSTITUCIONES EDUCATIVAS PARTICULARES**
8.2.1	26. AUT CREAC Y FUNC; CAMBIO DE DOM, AMP DE OF DE IE.PDF
8.3	**AUTORIZACION DE CAMBIO DE DOMICILIO DE INSTITUCIONES EDUCATIVAS FISCOMISIONALES**
8.3.1	26. AUT CREAC Y FUNC; CAMBIO DE DOM, AMP DE OF DE IE.PDF
8.4	**AUTORIZACION DE CAMBIO DE DOMICILIO DE INSTITUCIONES EDUCATIVAS PARTICULARES**
8.4.1	26. AUT CREAC Y FUNC; CAMBIO DE DOM, AMP DE OF DE IE.PDF
8.5	**AUTORIZACIÓN DE CREACION Y FUNCIONAMIENTO DE INSTITUCIONES EDUCATIVAS FISCOMISIONALES**
8.5.1	26. AUT CREAC Y FUNC; CAMBIO DE DOM, AMP DE OF DE IE.PDF
8.6	**AUTORIZACIÓN DE CREACION Y FUNCIONAMIENTO DE INSTITUCIONES EDUCATIVAS PARTICULARES**
8.6.1	26. AUT CREAC Y FUNC; CAMBIO DE DOM, AMP DE OF DE IE.PDF
8.7	**CAMBIO DE DENOMINACIÓN DE INSTITUCIONES EDUCATIVAS**
8.7.1	FORMATO DE RESOLUCION CAMBIO DE DENOMINACION DE IE.DOCX
8.7.2	32. CAMBIO DE DENOMINACION DE IE 20150701.PDF
8.7.3	FORMATO DE INFORME GENERAL-V2.0 (1).DOCX
8.8	**CIERRE VOLUNTARIO DE FUNCIONAMIENTO DE INSTITUCIONES EDUCATIVAS PARTICULARES Y FISCOMISIONALES**
8.8.1	31. CIERRE VOLUNTARIO DE FUNCIONAMIENTO JORNADAS NIVELES Y PARALELOS V2.PDF
8.8.2	FORMATO RESOLUCION CIERRE IE.DOCX
8.9	**CIERRE VOLUNTARIO DE JORNADAS DE INSTITUCIONES EDUCATIVAS PARTICULARES Y FISCOMISIONALES**
8.9.1	31. CIERRE VOLUNTARIO DE FUNCIONAMIENTO JORNADAS NIVELES Y PARALELOS V2.PDF
8.9.2	FORMATO RESOLUCION CIERRE IE.DOCX
8.10	**CIERRE VOLUNTARIO DE NIVELES EDUCATIVOS DE INSTITUCIONES EDUCATIVAS PARTICULARES Y FISCOMISIONALES**
8.10.1	31. CIERRE VOLUNTARIO DE FUNCIONAMIENTO JORNADAS NIVELES Y PARALELOS V2.PDF
8.10.2	FORMATO RESOLUCION CIERRE IE.DOCX

8.11	**CIERRE VOLUNTARIO DE PARALELOS DE INSTITUCIONES EDUCATIVAS PARTICULARES Y FISCOMISIONALES**
8.11.1	31. CIERRE VOLUNTARIO DE FUNCIONAMIENTO JORNADAS NIVELES Y PARALELOS V2.PDF
8.11.2	FORMATO RESOLUCION CIERRE IE.DOCX
8.12	**GESTIÓN DEL ARCHIVO MAESTRO DE INSTITUCIONES EDUCATIVAS**
8.12.1	29. GESTION DEL ARCHIVO MAESTRO DE INSTITUCIONES EDUCATIVAS 20150701.PDF
8.12.2	FORMATO DE INFORME GENERAL-V2.0 (1).DOCX
8.13	**RENOVACIÓN DE PERMISOS DE FUNCIONAMIENTO DE INSTITUCIONES EDUCATIVAS PARTICULARES Y FISCOMISIONALES**
8.13.1	FORMULARIO DECLARACION JURAMENTADA FISCOMISIONAL.DOC
8.13.2	FORMULARIO DECLARACION JURAMENTADA PARTICULAR.DOC
8.13.3	MINEDUC-ME-2016-00059-A.PDF
8.13.4	RENOVACION DE PERMISOS DE FUNCIONAMIENTO 15-09-2016.PDF
9	**TALENTO HUMANO**
9.1	**CERTIFICADO DE NO ESTAR INMERSO EN SUMARIO ADMINISTRATIVO Y NO HABER SIDO SANCIONADO**
9.1.1	41. CERTIFICADO NO ESTAR INMERSO SUM AD Y NO HAB SIDO S 20150504.PDF
9.1.2	FORMATO LOEI 20150504.DOC
9.1.3	FORMATO LOSEP 20150504.DOC
9.2	**COMISION DE SERVICIOS CON REMUNERACIÓN AL EXTERIOR POR ESTUDIOS**
9.2.1	37. COMISIÓN DE SERVICIOS CON REMUNERACIÓN 20150701.PDF
9.3	**RENUNCIAS**
9.3.1	RENUNCIAS.PDF
9.3.2	FORMATO PAZ Y SALVO.XLS
9.3.3	ACTA DE ENTREGA RECEPCION.DOC
9.3.4	INFORME FIN DE GESTION.DOCX
9.4	**SOLICITUD DE PERMISOS Y LICENCIAS**
9.4.1	45. SOLICITUD DE PERMISOS Y LICENCIAS 20150701.PDF
9.4.2	FORMATO DE SOLICITUD DE PERMISOS Y LICENCIAS 20150701.DOC
9.5	**SOLICITUD DE VACACIONES**
9.5.1	44. SOLICITUD DE VACACIONES 20150701.PDF
9.5.2	FORMULARIO DE SOLICITUD DE VACACIONES 20150701.DOC
9.6	**TRASLADO DE DOCENTES POR BIENESTAR SOCIAL**
9.6.1	28. TRASLADO DE DOCENTES POR BIENESTAR SOCIAL 20170701.PDF
9.6.2	FORMATO DE RESOLUCION DE TRASLADO DE DOCENTES POR BIENESTAR SOCIAL 20150701.DOC

Anexo N. Socialización y entrega del "MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR" en la Dirección Distrital 23D01 Educación.