ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

MAESTRÍA DE SEGURIDAD INFORMÁTICA APLICADA

"ASEGURAMIENTO DEL ENTORNO INFORMÁTICO EN LA DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DÉLEG-EDUCACIÓN"

TESIS DE GRADO

Previa a la obtención del Título de:

MASTER EN SEGURIDAD INFORMÁTICA APLICADA

DIEGO ESTEBAN IZQUIERDO CORONEL

Guayaquil-Ecuador

2015

AGRADECIMIENTO

A la Escuela Superior Politécnica del Litoral y sus Catedráticos por todos los conocimientos impartidos durante la Maestría Seguridad Informática Aplicada

A mi Director de Tesis, Ing. Lenin Freire Cobos, por su apoyo y colaboración incondicional a este trabajo de titulación.

DEDICATORIA

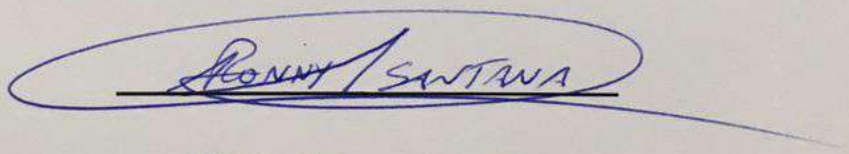
A Dios, por darme la oportunidad, el camino y la sabiduría para llegar a cumplir una meta más en mi vida.

A mis padres, que son mi apoyo incondicional, ya que son ejemplo de entrega y sacrificio.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo

DIRECTOR DE TESIS



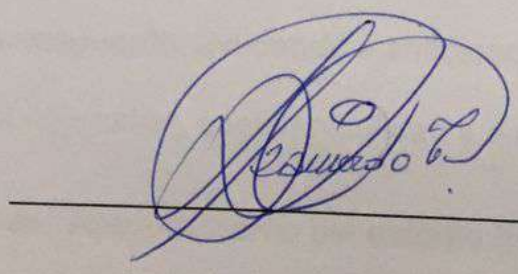
MSIG. Ronny Santana

MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de Graduación de la ESPOL)



Diego Esteban Izquierdo Coronel

RESUMEN

La sociedad hoy en día para el desarrollo laboral, donde los activos de la información forma parte trascendental, deben estar reguladas por ciertos controles, es por ello que toda empresa debe realizar un análisis profundo y exhaustivo sobre cómo se maneja y que tipo de controles tiene frente a las amenazas existentes en la actualidad. Se debe reconocer que los avances informáticos han agregado ventajas significativas en el manejo de los activos de la información sin embargo, trae consigo los llamados riesgos de la automatización de la información, los cuales al no ser identificados y tratados adecuadamente, han ocasionado muchas pérdidas tanto económicas, como al mismo tiempo se han detenido los procesos y secuencias de trabajo. De allí la importancia de generar un conjunto de políticas y técnicas de mitigación, teniendo en cuenta cada una de los ejes trasversales del manejo de la información como es la seguridad software, hardware y física de una empresa. Estos lineamientos permiten una mejor gestión de manejo de los Activos de la Información, su resguardo, ayudando a anticiparse ante cualquier eventualidad garantizando la integridad, confidencialidad y disponibilidad de la información.

Palabras Claves: Aseguramiento del entorno Informático, políticas y normas, integridad, confidencialidad y disponibilidad.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BACK-UP	Respaldo de Software y Procesos
FW	Firewall
ISO	Organización Internacional de Normalización
ID	Código de Identificación Única
IP	Protocolo De Internet
LAN	Red de Área Local
MAC	Control De Acceso Al Medio
PIN	Número de Identificación Personal
QUIPUX	Sistema de gestión de documentos
SO	Sistema Operativo
SW	Switch de acceso
TELCONET	Proveedor de Servicio de Internet privado
UPS	Dispositivo de suministro de energía ininterrumpido
WEB	Página o Sitio en Internet

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En una sociedad, donde la tecnología cumple un papel importante, una de las herramientas que han revolucionado el manejo de la información, es el avance acelerado de la informática, a la par van aumentando sus amenazas, vulnerabilidades y peligros. Tanto a nivel de Software como Hardware.

Es importante garantizar el buen manejo de la información, para ello se deben desarrollar políticas y normas que garanticen la confidencialidad y confiabilidad de la información ¿Cuáles son estas actividades que se tienen que incorporar?, realizando un estudio profundo de los requerimientos, posibles amenazas y vulnerabilidades. En el presente trabajo se incorporarán las normas internacional ISO “Estándar de Seguridad 27002”.

Se empezará realizando un análisis situacional de la empresa. La auditoría en una institución en la que el desarrollo y avance depende, como factor primordial la eficiente administración de la información y del adecuado uso de la tecnología de información, en la que los sistemas de gestión han

alcanzado un desarrollo tan notable, demanda la introducción muy diferente a la que fuera para esta disciplina durante su utilización.

En una auditoria informática se revisaran y evaluarán: los procesos, aplicaciones, aprovechamiento tanto de los recursos tecnológicos como físicos, las regulaciones que necesitan implementar, se detectarán los riesgos tecnológicos, como la seguridad en recursos, aplicaciones, y redes.

Dentro de los cuales se encontrarán frente a riesgos de seguridad, que son desconocidos por ciertos usuarios, para los cuales se tendrá que incorporar charlas de socialización y concienciación. Para ello se deberá establecer políticas se seguridad claras y concisas que puedan ser aplicadas, acorde a las necesidades de la empresa.

CAPÍTULO 1

Generalidades:

1.1. Antecedentes.

En el presente trabajo de propuesta de titulación con el tema de ASEGURAMIENTO DEL ENTORNO INFORMÁTICO EN LA DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DÉLEG-EDUCACIÓN, luego de un estudio minucioso de los activos de la información, es preciso delimitar cuales son los procesos y políticas que pueden ser implementados dentro de la institución, para garantizar la continuidad, seguridad y responsabilidad en las actividades que se llevan a cabo.

Los estándares internacionales ISO dictan los principios y lineamientos estandarizados para generar, mejorar, implementar y

mantener la seguridad de la información en una organización. Estos estándares permiten tener unos lineamientos sobre los objetivos de seguridad de la gestión de la información, determinando e identificando los riesgos y amenazas. Las normas ISO permiten realizar un estudio minuciosos sobre cuáles son las necesidades y requerimientos de la organización, permitiendo establecer las regulaciones y políticas necesarias para el correcto funcionamiento de la empresa.

1.2. Descripción del Problema

En la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN, a lo largo del trabajo y desempeño de la empresa no ha existido ningún tipo de control en cuanto al uso y manejo de la información, es por ello que se realiza en presente estudio. Los inconvenientes en la seguridad de la información, son riesgos que se pueden prevenir aun así la mayoría son inesperados, aunque en muchos casos se pueden prevenir.

Cuando hablamos de incidentes de Seguridad, o problemas de Seguridad Informática nos referimos a, que no existen políticas claras que eviten:

- ☞ Acceso no autorizado a la información;
- ☞ Descubrimiento de información;

- ☞ Modificación no autorizada de datos;
- ☞ Invasión a la privacidad;
- ☞ Denegación de servicios;

Los componentes de los entornos informatizados son distintos, por lo que las especificaciones de seguridad asociadas a cada uno varía notablemente dependiendo de la tecnología utilizada a nivel de plataforma, software base y dispositivos físicos.

La funcionalidad y características técnicas de los componentes de los entornos varían notablemente según la marca, en particular en los aspectos concernientes a establecer unas políticas claras de seguridad y de manejo eficiente de recursos.

Hoy en día la amenaza más común en los ambientes informatizados se centra en la eliminación o disminución de la disponibilidad de los recursos y servicios que utiliza el usuario.

Prácticamente toda la información vital de la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN se encuentra informatizada, no sólo al almacenada en dispositivos electrónicos, sino que, en la mayor parte de los casos, se encuentra distribuida físicamente y viaja constantemente a través de medios públicos como redes de Internet.

Es por eso que se pone énfasis en el crecimiento de soluciones para el problema de Seguridad Informática, por lo que el conocimiento en esta área ha crecido enormemente en los últimos años, al punto en que somos capaces de afirmar que es posible lograr una completa enumeración de las fallas de seguridad de los sistemas y los entornos en los que viven. Estas fallas de seguridad son las que se convierten en amenazas susceptibles de ser aprovechada por usuarios mal intencionados para cuásar daño o algún tipo de invasión a la confidencialidad. Protegerse contra accesos no autorizados es el problema más sencillo a resolver, ya que durante años se han desarrollado y perfeccionado algoritmos matemáticos para la inscripción de datos, para el intercambio seguro de información, para garantizar el correcto funcionamiento del software, que se ha traducido en herramientas capaces de proporcionar soluciones rápidas y sencillas a problemas técnicos de seguridad.

Desafortunadamente, no es suficiente simplemente arreglar los errores o eliminar las fallas técnicas de seguridad. El problema va mucho más allá.

La Seguridad Informática es un problema cultural, en el que el usuario juega un rol protagónico.

La responsabilidad sobre la seguridad de los datos y equipos ya no recae solamente en el personal técnico especializado encargado de resguardar los bienes y servicios brindados por el entorno, sino que es el usuario el que debe velar por la seguridad de los bienes físicos y lógicos que maneja.

Para ello debe existir una conciencia de trabajo seguro, de resguardo de la confidencialidad y de protección de los activos utilizados a diario en el trabajo de cada individuo.

Por esta razón se debe definir políticas y normas dentro del entorno informático que se deberá incorporar desde el principio de todo proceso, desde el diseño para garantizar la evaluación de todos los factores funcionales (y no solamente los técnicos) a tener en cuenta para el uso seguro del entorno. Si esto sucede, el objetivo inicial de la seguridad habrá sido logrado.

La seguridad, entonces, debe nacer en el diseño seguro de unas políticas claras y precisas, de la correcta formación de la estructura de la organización, de la adecuada distribución de tareas y contraposición de intereses en los roles de control y ejecución de tareas. Luego de lograr eso se deben implantar medidas de índole técnica que garanticen el adecuado uso de los recursos y servicios solamente a los usuarios autorizados, y la disponibilidad de los mismos.

Pero lo importante es ver que la Seguridad Informática ya no es un problema de la gente especializada en sistemas, sino que ha salido de los laboratorios y los centros de cómputo para instalarse en el escritorio del usuario, en donde nacen los problemas de Seguridad.

1.3. Solución del problema.

En la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN, es necesario estar protegidos de las múltiples y hasta desconocidas amenazas, garantizando fundamentalmente, la preservación de tres características:

- ☞ Integridad: Que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento;
- ☞ Confidencialidad: Que la información sea accesible solo a las personas autorizadas;
- ☞ Disponibilidad: Que los usuarios autorizados tengan acceso a la información y a los recursos, cuando lo necesiten.

La Seguridad de la Información en la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN se logrará implementando un conjunto adecuado de controles y normas que abarca políticas, prácticas y procedimientos.

La motivación de este trabajo es la falta de una herramienta que les permita a los profesionales Informáticos analizar e implementar técnicas de seguridad en su entorno de trabajo.

El propósito del presente proyecto es elaborar políticas, normas, metodologías y prácticas clara en la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN y factibles para convertir un entorno informatizado inseguro, en un entorno protegido y lograr una clara evaluación de los mismos teniente en cuenta el objetivo y los proceso manejados.

1.4. Objetivo general.

Asegurar el entorno informático estableciendo políticas y direccionamientos en el departamento Informático de la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN.

1.5. Objetivos específicos.

- ☞ Definir pautas con las que se debe emplear la seguridad informática en el departamento Informático del DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN.
- ☞ Crear un cambio cultural en el ambiente en el departamento Informático, al aplicar políticas que afecten al personal, al uso de los recursos y a la forma de trabajo, además de una conciencia

integral de la importancia de la seguridad del entorno informático y las implicaciones de las falencias en este tema.

- ☞ Brindar y aplicar una metodología de seguridad a nivel físico, lógico y organizacional del área informática, estableciendo políticas claras y concisas.
- ☞ Definir las pautas para la estabilización y mantenimiento del entorno informático en la DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DELEG-EDUCACIÓN.

1.6. Metodología.

La metodología de investigación a utilizar en el proyecto es evaluación de las diferentes actividades que se llevan a cabo en el manejo de la información dentro del Distrito para ello se realizara, encuestas, visitas técnicas, solicitud de los estándares utilizados y programas de trabajo, análisis, observación y evaluación a través de levantamientos de información, elaboración de informes.

Se desarrollará una evaluación de los sistemas en operación, para ello se realizara una recopilación, seguimiento y análisis de los procedimientos administrativos de cada sistema y actividad por departamento con entrevista a sus empleados. Se realizará solicitudes de la documentación de los sistemas en operación.

Se evaluara los equipos para ello se determinara sus características, se realizará un análisis de los mantenimientos y procedimientos que

tienen para dar de baja a los equipos. Determinar si se tiene un contrato de seguros, se realizará visitas técnicas de comprobación de seguridad física y lógica de las instalaciones Informáticas del Distrito. Determinar el estado del sistema electrónico y de red de los equipos.

CAPÍTULO 2

Marco teórico:

2.1. Definición de Seguridad y Control Interno

2.1.1. Seguridad.

El término seguridad posee múltiples usos. A grandes rasgos, puede afirmarse que este concepto que proviene del latín securitas hace foco en la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e

indubitable. La seguridad, por lo tanto, puede considerarse como una certeza.

Existen muchos tipos de seguridad, tantos como actividades pueda realizar el ser humano. En este trabajo citaremos tan sólo algunos conceptos en los que se utiliza el término haciendo referencia a un desarrollo seguro de una determinada actividad.

Una de las acepciones del término es el que se utiliza en informática, un concepto moderno pero sumamente importante para conservar los ordenadores y equipos relacionados en buen estado. La seguridad informática permite asegurarse que los recursos del sistema se utilizan de la manera en la que se espera y que quienes puedan acceder a la información que en él se encuentran sean las personas acreditadas para hacerlo.

En informática se habla de dos tipos de seguridades, la física (barreras físicas que impiden el paso al sistema de cualquier persona no acreditada. Se realiza a través de aplicaciones y procedimientos específicos que tienen el objeto de bloquear el acceso a dichos individuos) y la lógica (las formas en las que se desempeña este tipo de seguridad es a través de encriptación de códigos, de

modo que no puedan ser leídos o traducidos por los intrusos que pudieran sobre pasar las barreras físicas, códigos de autenticación y antivirus o pared de fuego, en el caso de usar un sistema operativo como Windows). A la hora de elaborar un diseño, ya sea de página web o de espacio en la red de cualquier tener en cuenta ambos tipos de seguridad es fundamental.

Cabe aclarar que en la seguridad informática existen ciertos conceptos que es necesario conocer y que tienen que ver con ella, estos son: hacker y cracker.

Un hacker es un individuo que se encuentra buscando siempre la forma de vulnerar las barreras de seguridad de los sistemas de información a fin de obtener algún tipo de información confidencial. El objetivo fundamental del verdadero hacker es aprender y satisfacer su curiosidad y creatividad, no busca hacer daño. Su afán es crear, no destruir.

Un cracker es aquel que tiene capacidades semejantes a la de un hacker pero que las utiliza con objetivos maliciosos. La razón de toda su investigación es destruir sistemas, borrar o robar datos y hacer daño por el solo hecho de divertirse [1].

2.1.2. Seguridad de la Información

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo

comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio [2].

2.1.3. La necesidad de la seguridad en la información

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por

computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para la operatividad del Distrito del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles.

La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas [2].

2.1.4. Establecer los requerimientos de seguridad

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad, Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el

procesamiento de la información que una organización ha desarrollado para sostener sus operaciones [2].

2.1.5. Evaluando los riesgos de la seguridad.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo [2].

2.1.6. Control

La palabra control proviene del término francés contrôle y significa comprobación, inspección, fiscalización o intervención. También puede hacer referencia al dominio, mando y preponderancia, o a la regulación sobre un sistema [3].

2.1.7. Control Interno

Tradicionalmente en materia de control interno se adoptaba un enfoque bastante restringido limitado a los controles contables internos. Durante el último decenio la prensa ha informado sobre escándalos relacionados con errores en el otorgamiento de créditos con garantía de inmuebles inexistentes o sobrevalorados, la manipulación de información financiera, operaciones bursátiles realizadas con información privilegiada y otros fallos de los controles que han afectado a las empresas de diferentes sectores. Un centro de informática de una empresa suele tener una importancia crucial por soportar los sistemas de información del negocio, por el volumen de recursos y presupuestos que maneja, etc. Por lo tanto aumenta las necesidades de control y auditoría, surgiendo en las organizaciones, como medidas organizativas [3].

2.1.8. Selección de Controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran

implementar para asegurar que los riesgos se reduzcan a un nivel aceptable. Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas conforme sea apropiado. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales relevantes.

Algunos de los controles en este estándar se pueden considerar principios guías para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones. Se explican con mayor detalle más abajo bajo el título “Punto de inicio de la seguridad de la información” [3].

2.1.9. Punto de inicio de la seguridad de la información

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la

seguridad de la información. Estos se basan en requerimientos legislativos esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

a. Protección de data y privacidad de la información personal.

b. Protección de los registros organizacionales.

c. Derechos de propiedad intelectual.

Los controles considerados práctica común para la seguridad de la información incluyen:

a. Documento de la política de seguridad de la información.

b. Asignación de responsabilidades de la seguridad de la información.

c. Conocimiento, educación y capacitación en seguridad de la información.

d. Procesamiento correcto en las aplicaciones.

e. Gestión de la vulnerabilidad técnica.

f. Gestión de la continuidad comercial.

g. Gestión de los incidentes y mejoras de la seguridad de la información.

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Se debiera notar que aunque los controles en este estándar son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo [3].

2.1.10. Factores de éxito críticos

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

a. Política, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales.

b. Un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la

información que sea consistente con la cultura organizacional.

c. Soporte visible y compromiso de todos los niveles de gestión.

d. Un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;

e. Marketing efectivo de la seguridad de la información con todos los gerentes, empleados y otras partes para lograr conciencia sobre el tema;

f. Distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los gerentes, empleados y otras partes involucradas;

g. Provisión para el financiamiento de las actividades de gestión de la seguridad de la información;

h. Proveer el conocimiento, capacitación y educación apropiados;

i. Establecer un proceso de gestión de incidentes de seguridad de la información;

j. Implementación de un sistema de medición1 que se utiliza para evaluar el desempeño en la gestión de la

seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

Desarrollo de sus propios lineamientos

Este código de práctica puede ser visto como un punto de inicio para desarrollar los lineamientos específicos de la organización. No todos los controles y lineamientos en este código de práctica pueden ser aplicables. Es más, se pueden requerir controles y lineamientos adicionales no incluidos en este estándar. Cuando los documentos son desarrollados conteniendo lineamientos o controles adicionales, cuando sea aplicable podría ser útil incluir referencias cruzadas con las cláusulas en este estándar para facilitar el chequeo de conformidad realizado por los auditores y socios comerciales [3].

2.2. Definición de Activos.

Los activos, desde el punto de vista contable, representan los bienes, derechos y otros recursos controlados económicamente por la empresa, resultantes de sucesos pasados, de los que se espera que la empresa obtenga beneficios o rendimientos económicos en el futuro.

En esta definición hay que destacar la esencia de la naturaleza del activo, que según el Marco Conceptual de la Contabilidad, radica en la capacidad de convertirse en rendimientos económicos que se transformen en futuras entradas de liquidez para la empresa.

Otro aspecto a tener en cuenta de la definición de activo es considerar el control económico como sentencia de vinculación del activo con la empresa, por lo que ya no es necesaria la propiedad en sentido jurídico del término. Claro ejemplo de esta situación se encuentra en las operaciones de arrendamiento financiero, donde la empresa arrendataria tiene el control económico del activo, pero no le han transferido la titularidad jurídica del mismo.

El activo es también conocido con el nombre de “estructura económica”, capital económico, capital en funcionamiento, actividad, sustancia, etc [4].

2.2.1. Criterios de Registro o Reconocimiento de un Activo

El registró o reconocimiento contable es el proceso por el que se incorporan al balance, a la cuenta de pérdidas y ganancias o al estado de cambios en el patrimonio neto, los diferentes elementos que constituyen las cuentas anuales. Para ser reconocido un elemento

debe reunir las características exigidas en la definición de los mismos, y además deberá presentar un valor que se podrá determinar con fiabilidad.

En concreto, los activos deben reconocerse en el balance cuando sea probable la obtención de beneficios o rendimientos económicos para la empresa en el futuro, y siempre que se puedan valorar con un adecuado grado de fiabilidad. El reconocimiento contable de un activo implica, al mismo tiempo, el reconocimiento de un pasivo, la disminución de otro activo o el reconocimiento de un ingreso u otros incrementos en el patrimonio neto [4].

2.2.2. La Información un Activo

La información ha llegado a ser considerada como el ACTIVO más valioso dentro de las empresas ya que juega un papel muy importante a la hora de la toma de decisiones y definición de nuevas estrategias de la operatividad del Distrito, algunos de ustedes se preguntarán ¿por qué?, otros sabrán que esto es verdad, pues la información como fuente del conocimiento otorga un bien a quien la posee, incluso en la actualidad es común escuchar acerca del espionaje, tráfico y/o robo de información como delito

grave, puesto que la información se ha convertido punto clave para el crecimiento, desarrollo o éxito personal, profesional y empresarial, ya que, entre mayor sea el conocimiento adquirido a través de la información mayor será el beneficio obtenido.

Un activo es un bien que tiene una empresa y que en el ámbito contable representa una cantidad monetaria, puede ser tangible o intangible, por otro lado, la información es un conjunto de datos ordenados de tal manera que sirven para dar solución a un problema y que es generada día a día durante las actividades de cualquier persona, empresa o institución, representa más que una cantidad monetaria, la existencia y permanencia de cualquier empresa en este mundo globalizado, pues la toma de decisiones estratégicas depende principalmente de ella.

A mediados de los setenta en el mundo empresarial, surgieron los conceptos de "empresa inteligente" y "administración del conocimiento", la inteligencia se da por el conocimiento y el conocimiento se obtiene de la basta información que podemos encontrar dentro de las bases de datos de la propia empresa y/o en la gran nube

tecnológica llamada internet. Es necesario que dicha información sea seleccionada y pase por un proceso de transformación para que dé como resultado un conocimiento valioso que dote de inteligencia a la toma de decisiones de los directivos de la empresa, utilizando las herramientas adecuadas, para así poder obtener el bien esperado, soportar el crecimiento y desarrollo empresarial.

La globalización ha obligado a las empresas a modificar sus procesos, a mejorar sus formas de trabajo y a transformar la manera de hacer la operatividad del Distrito, pero también les ha proporcionado la información necesaria y las herramientas exactas para adoptar nuevas estrategias basadas en las buenas prácticas empresariales, la administración correcta del conocimiento y el uso adecuado de las tecnologías de información. De esta manera se confirma que la información va más allá de ser un simple conjunto de datos, siendo un activo intangible y materia prima del conocimiento y del beneficio empresarial.

Pero, ¿cómo lograr que la información se transforme en conocimiento y beneficio empresarial?, de antemano, no

se puede negar que en las empresas se maneja una gran cantidad de información, aunque no toda sea realmente útil, es tanta que no resulta fácil traducirla a conocimiento valioso y aplicable a las necesidades de la empresa, pues se corre el riesgo de hacer aprendizajes falsos y/o erróneos o tal vez equivocarse en la toma de decisiones, porque la información no tiene la calidad requerida ni es evaluada debidamente, siendo deficiente para cumplir con el beneficio empresarial.

¿Cuántas veces ha solicitado, información sobre las ventas, el mantenimiento, producción, calidad, etc.?, y ¿cuántas veces esa información le ha resultado relevante o útil?

La mayoría de las empresas realizan esta actividad diaria, semanal, mensual o anualmente en forma de reportes, algunas incluso todavía lo hacen de manera manual y extrayendo la información de múltiples fuentes, generando información errónea, son muy pocas las que realmente le dan el uso correcto y aprovechan la información obtenida, por ello y utilizando las herramientas informáticas adecuadas, es imperativo mejorar el uso y aprovechamiento de dicha información

para evitar informes erróneos y/o manipulados, llevando a cabo una buena Administración del Conocimiento, definiendo indicadores clave y la forma en que éstos serán medidos y presentados, basándose en:

•Las MEJORES PRACTICAS del manejo de la información de la empresa y/o empresas homólogas que servirán de benchmarking o comparativo con la intención de adoptarlas.

•La recolección de PROPUESTAS DE MEJORA de los procesos, hechas por los operarios, quienes son los que conocen las necesidades y áreas de oportunidad que estos tienen.

•La DOCUMENTACIÓN de soluciones a problemas presentados a fin de crear una BASE de CONOCIMIENTO que permita dar respuestas inmediatas a los problemas presentados.

La constante evolución de las tecnologías de información y de las herramientas informáticas, permite gestionar adecuadamente el acceso, obtención y manipulación de la información, así mismo, aumentar la capacidad de procesamiento para lograr de esta forma que la información pueda ser transformada en conocimiento en

un tiempo más corto otorgándole a la empresa beneficios y ventajas competitivas como:

•Reducción de costos, haciendo uso de las buenas prácticas, mejorando los procesos y reduciendo el mantenimiento correctivo de la maquinaría o equipo, traduciéndose en ahorros.

•Mejora del Negocio, con la base de conocimiento creada y dada la información en tiempo real, permite llevar a cabo una toma de decisiones correcta al instante y/o anticipada para desarrollar estrategias que apoyen al crecimiento y desarrollo de la empresa.

•Aumento de la productividad, con el aprovechamiento de todos los recursos de la empresa [4].

2.3. Aseguramiento Informático. Tecnologías de la Información - Técnicas de seguridad Código de práctica para la gestión de la seguridad de la información

Alcance

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan

un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales [5].

2.3.1. Términos y definiciones

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

- ✓ Activo Cualquier cosa que tenga valor para la organización
- ✓ Control Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

- ✓ Lineamiento Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas
- ✓ Medios de procesamiento de la información Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.
- ✓ Seguridad de la información Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, norepudiación y confiabilidad
- ✓ Evento de seguridad de la información Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
- ✓ Incidente de seguridad de la información Un incidente de seguridad de la información es

indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

- ✓ Política Intención y dirección general expresada formalmente por la gerencia
- ✓ Riesgo Combinación de la probabilidad de un evento y su ocurrencia
- ✓ Análisis del riesgo Uso sistemático de la información para identificar las fuentes y calcular el riesgo
- ✓ Gestión del riesgo Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- ✓ Tratamiento del riesgo Proceso de selección e implementación de medidas para modificar el riesgo.
- ✓ Tercera persona Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

- ✓ Amenaza Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.
- ✓ Vulnerabilidad La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas [4].

2.3.2. Estructura de este estándar

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Cláusulas

Cada cláusula contiene un número de categorías de seguridad principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

a. Política de Seguridad.

b. Organización de la Seguridad de la Información.

c. Gestión de Activos.

d. Seguridad de Recursos Humanos.

e. Seguridad Física y Ambiental.

f. Gestión de Comunicaciones y Operaciones.

g. Control de Acceso.

h. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

i. Gestión de Incidentes de Seguridad de la Información.

j. Gestión de la Continuidad Comercial.

k. Conformidad.

Categorías de seguridad principales

Cada categoría de seguridad contiene:

a. Un objetivo de control que establece lo que se debiera lograr; y

b. Uno o más controles que se pueden aplicar para lograr el objetivo de control.

Las descripciones del control están estructuradas de la siguiente manera:

Control define el enunciado de control específico para satisfacer el objetivo de control.

Lineamiento de implementación proporciona información más detallada para apoyar la implementación del control

y cumplir con el objetivo de control. Parte de este lineamiento puede no ser adecuado en todos los casos y por lo tanto, pueden ser adecuadas otras maneras para implementar el control.

2.3.3. Evaluación y tratamiento del riesgo

Evaluación de los riesgos de seguridad

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos

estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

Tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es

efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a. Aplicar los controles apropiados para reducir los riesgos.

b. Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización.

c. Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

d. Transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles debieran asegurar

que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a. Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales.

b. Objetivos organizacionales;

c. Requerimientos y restricciones operacionales;

d. Costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;

e. La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Se debieran considerar los controles de seguridad de la información en los sistemas y la especificación de los requerimientos de proyectos, así como la etapa de diseño. El no hacerlo puede resultar en costos adicionales y soluciones menos efectivas, y tal vez, en el peor de los casos, la incapacidad de lograr la seguridad adecuada.

Se debiera tener en mente que ningún conjunto de controles puede lograr la seguridad completa, y que se

debiera implementar una acción de gestión adicional para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar los objetivos de la organización [4].

2.3.4. Política de seguridad. Política de seguridad de la información

2.3.5. Documento de la política de seguridad de la información

Control el documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

Lineamiento de implementación

El documento de la política de seguridad de la información debiera enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. El documento de la política debiera contener enunciados relacionados con:

a. Una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información (ver introducción);
b. Un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales;
c. Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo;
d. Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo:

1. Conformidad con los requerimientos legislativos, reguladores y restrictivos,
2. Educación, capacitación y conocimiento de seguridad,
3. Gestión de la continuidad del negocio,
4. Consecuencias de las violaciones de la política de seguridad de la información;

e. Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información,
f. Referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar.
g. Esta política de seguridad de la información se debiera comunicar a través de toda la organización a los usuarios en una forma que sea relevante, accesible y entendible para el lector objetivo [5].

2.4. Normas de Seguridad en Hardware y Software

2.4.1. Seguridad Hardware y ambiental

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras,

protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia [5].

Perímetro de seguridad física

Control se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información [5].

Lineamiento de implementación

Cuando sea apropiado, se debieran considerar e implementar los siguientes lineamientos para los perímetros de seguridad físicos:

a. Los perímetros de seguridad debieran estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo

b. Los perímetros de un edificio o local que contienen los medios de procesamiento de información debieran ser

físicamente sólidos (es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado); las paredes externas del local debieran ser una construcción sólida y todas las puertas externas debieran estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control; por ejemplo, vallas, alarmas, relojes, etc.; las puertas y ventanas debieran quedar aseguradas cuando están desatendidas y se debiera considerar una protección externa para las ventas, particularmente en el primer piso;

c. Se debiera contar con un área de recepción con un(a) recepcionista u otros medios para controlar el acceso físico al local o edificio; el acceso a los locales y edificios debieran restringirse solamente al personal autorizado;

d. Cuando sea aplicable, se debieran elaborar las barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental;

e. todas las puertas de emergencia en un perímetro de seguridad debieran contar con alarma, debieran ser monitoreadas y probadas en conjunción con las paredes

para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales; debieran operar en concordancia con el código contra-incendios local de una manera totalmente segura;

f. Se debieran instalar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales y debieran ser probados regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas debieran contar con alarma en todo momento; también se debiera proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto de comunicaciones;

g. Los medios de procesamiento de información manejados por la organización debieran estar físicamente separados de aquellas manejadas por terceros [5].

Controles de ingreso físico

Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Se debieran considerar los siguientes lineamientos:

a. Se debiera registrar la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes debieran ser supervisados a no ser que su acceso haya sido previamente aprobado; sólo se les debiera permitir acceso por propósitos específicos y autorizados y se debieran emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia;

b. El acceso a áreas donde se procesa o almacena información sensible se debiera controlar y restringir sólo a personas autorizadas; se debieran utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos;

c. Se debiera requerir que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible y se debiera notificar inmediatamente al personal de seguridad si se

encuentra a un visitante no acompañado y cualquiera que no use una identificación visible;

d. Al personal de servicio de apoyo de terceros se le debiera otorgar acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debiera ser autorizado y monitoreado;

e. Los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario [5].

Asegurar las oficinas, habitaciones y medios

Se debiera diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios.

Se debieran considerar los siguientes lineamientos para asegurar las oficinas, habitaciones y medios:

a. Se debiera tener en cuenta los estándares y regulaciones de sanidad y seguridad relevantes;

b. Se debieran localizar los medios claves para evitar el acceso del público;

c. Donde sea aplicables, los edificios debieran ser discretos y dar una indicación mínima de su propósito, sin carteles obvios dentro y fuera del edificio que indiquen la presencia de actividades de procesamiento de información;

d. Los directorios y teléfonos internos que identifiquen la ubicación de los medios de procesamiento de la información no debieran estar accesibles al público.

Protección contra amenazas externas e internas

Se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debiera prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debieran considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto,

explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a. Los materiales peligrosos o combustibles debieran ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deberían almacenarse en el área asegurada;

b. El equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;

c. Se debiera proporcionar equipo contra-incendios ubicado adecuadamente [5].

Trabajo en áreas aseguradas

Se debiera diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.

Se debieran considerar los siguientes lineamientos:

a. El personal debiera estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer;

b. Se debiera evitar el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos;

c. Las áreas aseguradas vacías debieran ser cerradas físicamente bajo llave y revisadas periódicamente;

d. No se debiera permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea autorizado.

Los arreglos para trabajar en las áreas aseguradas incluyen controles para los empleados, contratistas y terceros que trabajen en el área asegurada, así como otras actividades de terceros que allí se realicen.

Equipo de seguridad

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

Se debiera proteger el equipo de amenazas físicas y ambientales.

La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no-

autorizado a la información y proteger contra pérdida o daño. Esto también debiera considerar la ubicación y eliminación del equipo. Se pueden requerir controles especiales para proteger el equipo contra amenazas físicas, y salvaguardar los medios de soporte como el suministro eléctrico y la infraestructura del cableado.

Ubicación y protección del equipo

Se debiera ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado.

Se debieran considerar los siguientes lineamientos para la protección del equipo:

a. El equipo se debiera ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo;

b. Los medios de procesamiento de la información que manejan data confidencia debieran ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso; y se debieran asegurar los medios de almacenaje para evitar el acceso no autorizado;

c. Se debieran aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida;

d. Se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

e. Se debieran establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información;

f. Se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información;

g. se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones;

h. Se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial;

i. Se debiera proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación [5].

Servicios públicos de soporte

Se debiera proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; debieran ser adecuados para los sistemas que soportan. Los servicios públicos de soporte debieran ser inspeccionados regularmente y, conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla. Se debiera proveer un suministro eléctrico adecuado que esté de acuerdo a las especificaciones del fabricante del equipo.

Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporta las operaciones comerciales críticas. Los planes de contingencia para la energía debieran abarcar la acción a tomarse en el caso de una falla de energía prolongada. Se debiera considerar un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada. Se debiera tener disponible un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado. El equipo UPS y los generados se debieran chequear regularmente para asegurar que tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante. Además, se debiera considerar al uso de múltiples fuentes de energía, si el local es grande, una subestación de energía separada.

Se debieran colocar interruptores de energía de emergencia cerca de las salidas de emergencia en las habitaciones donde se encuentra el equipo para facilitar el cierre del paso de corriente en caso de una

emergencia. Se debiera proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal.

El suministro de energía debiera ser estable y adecuado para suministrar aire acondicionado, equipo de humidificación y los sistemas contra-incendios (donde se utilicen). El mal funcionamiento del sistema de suministro de agua pude dañar el equipo y evitar que el sistema contra-incendios funcione adecuadamente. Se debiera evaluar e instalar, si se requiere, un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.

El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de voz. Los servicios de voz debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia [5].

Seguridad del cableado

El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño.

Se debieran considerar los siguientes lineamientos para la seguridad del cableado:

a. Cuando sea posible, las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información debieran ser subterráneas o debieran estar sujetas a una alternativa de protección adecuada;

b. El cableado de la red debiera estar protegido contra intercepciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas;

c. Los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia;

d. Se debieran utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados;

e. Se debiera utilizar una lista de empalmes documentados para reducir la posibilidad de error;

f. Para sistemas sensibles o críticos se debieran considerar más controles como:

1. Instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación;

2. El uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada;

3. El uso de cableado de fibra óptica;

4. El uso de un escudo electromagnético para proteger los cables;

5. La iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves;

6. Acceso controlado para empalmar los paneles y los cuartos de cableado.

Mantenimiento de equipo

Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e integridad.

Se debieran considerar los siguientes lineamientos para el mantenimiento de equipo:

a. El equipo se debiera mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor;

b. Sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo;

c. Se debieran mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo;

d. Se debieran implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario, se debiera revisar la información confidencial del equipo, o se debiera verificar al personal de mantenimiento;

e. Se debieran cumplir con todos los requerimientos impuestos por las pólizas de seguros [5].

Seguridad del equipo fuera del local

Se debiera aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

Sin importar la propiedad, el uso de cualquier equipo de procesamiento de la información fuera del local de la organización debiera ser autorizado por la gerencia. Se debieran considerar los siguientes lineamientos para la protección del equipo fuera del local:

a. El equipo y medios sacados del local nunca debiera ser dejados desatendidos en lugares públicos; durante un viaje, las computadoras portátiles debieran ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada;

b. Se debieran observar en todo momento las instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos;

c. Se debieran determinar controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, política de escritorio vacío, controles de acceso para las computadoras y una comunicación segura con la oficina;

d. Se debiera contar con un seguro adecuado para proteger el equipo fuera del local.

Los riesgos de seguridad; por ejemplo, daño, robo o intercepción; puede variar considerablemente entre los locales y se debiera tomar esto en cuenta para determinar los controles más apropiados [5].

Seguridad de la eliminación o re-uso del equipo

Se debieran chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

Los dispositivos que contienen información confidencial debieran ser físicamente destruidos o se debieran destruir, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información

original, en lugar de simplemente utilizar la función estándar de borrar o formatear [5]

2.4.2. Seguridad en el Software

Protección contra el código malicioso y móvil

Proteger la integridad del software y la integración.

Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus cómputo, virus de red, caballos Troyanos y bombas lógicas. Los usuarios debieran estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes debieran introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles [6].

Controles contra códigos maliciosos

Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y se debieran implementar procedimientos para el apropiado conocimiento del usuario.

La protección contra códigos maliciosos se debiera basar en la detección de códigos maliciosos y la reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio. Se debieran considerar los siguientes lineamientos:

a. Establecer una política formal prohibiendo el uso de software no-autorizado;

b. Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse;

c. Realizar revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos comerciales críticos; se debiera investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas;

d. La instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo debieran incluir:

1. Chequeo de cualquier archivo en medios electrónicos u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo;

2. Chequear los adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos, este chequeo debiera llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico, computadoras desktop y cuando se ingresa a la red de la organización;

3. Chequear las páginas Web para detectar códigos maliciosos;

e. Definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su

uso, reporte y recuperación de ataques de códigos maliciosos;

f. Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación;

g. Implementar procedimiento para la recolección regular de información, como suscribirse a listas de correos y/o chequear Web Sites que dan información sobre códigos maliciosos nuevos;

h. Implementar procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos, los gerentes debieran asegurar que se utilicen fuentes calificadas; por ejemplo, periódicos acreditados, sitios de Internet confiables o proveedores que producen software para protegerse de códigos maliciosos; que diferencien entre bromas pesadas y códigos maliciosos reales; todos los usuarios debieran estar al tanto del problema de las bromas pesadas y qué hacer cuando se reciben [5].

Gestión de seguridad de la red

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de data, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas [6].

Controles de redes

Las redes debieran ser adecuadamente manejadas y controladas para poder proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

Los gerentes de la red debieran implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados. En particular, se debieran considerar los siguientes ítems:

a. Cuando sea apropiado, la responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo;

b. Se debieran establecer las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario;

c. Se debieran establecer controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o a través de las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y las computadoras conectadas;

d. Se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes;

e. Las actividades de gestión debieran estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.

Seguridad de los servicios de la red

En todo contrato de redes se debieran identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

Se debiera determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura, y se debiera acordar el derecho de auditoría.

Se debieran identificar los acuerdos de seguridad necesarios para servicios particulares; como las características de seguridad, niveles de servicio y requerimientos de gestión. La organización se debiera asegurar que los proveedores de servicio de red implementen estas medidas.

Las características de seguridad de los servicios de red pueden ser:

a. La tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red;

b. Parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red;

c. Cuando sea necesario, procedimientos para la utilización del servicio de red para restringir el acceso a los servicios de red o aplicaciones [6].

Registro de Fallas

Se debieran registrar y analizar las fallas, y se debieran tomar las acciones necesarias.

Se debieran registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación. Debieran existir reglas claras para manejar las fallas reportadas incluyendo:

a. Revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente;

b. Revisión de las medidas correctivas para asegurar que los controles no se hayan visto comprometidos, y que la acción tomada haya sido completamente autorizada.

Se debiera asegurar que el registro de errores está activado, si está disponible esta función del sistema [7].

Gestión de acceso del usuario

Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información

Se debieran establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta el des-registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debiera prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema [7].

Registro del usuario

El procedimiento de control del acceso para el registro y des-registro del usuario debiera incluir:

a. Utilizar IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones; sólo se debiera permitir el uso de IDs grupales cuando son necesarios por razones comerciales u operacionales, y debieran ser aprobados y documentados;

b. Chequear que el usuario tenga la autorización dada por el propietario del sistema para el uso del sistema o servicio de información; también puede ser apropiado una aprobación separada de la gerencia para los derechos de acceso;

c. Chequear que el nivel de acceso otorgado sea apropiado para el propósito comercial y que sea consistente con la política de seguridad de la organización

d. Proporcionar a los usuarios un enunciado escrito de sus derechos de acceso;

e. Requerir a los usuarios que firmen los enunciados indicando que entienden las condiciones de acceso

f. Asegurar que los proveedores del servicio no proporcionen acceso hasta que se hayan completado los procedimientos de autorización;

g. Mantener un registro formal de todas las personas registradas para usar el servicio;

h. Eliminar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto o trabajo o han dejado la organización;

i. Chequeo periódico para eliminar o bloquear los IDs de usuario y cuentas redundantes

j. Asegurar que no se emitan IDs de usuario redundantes a otros usuarios [7].

Gestión de privilegios

Se debiera restringir y controlar la asignación y uso de privilegios. Los sistemas multi-usuario que requieren protección contra el acceso no autorizado debieran controlar la asignación de privilegios a través de un proceso de autorización formal. Se debieran considerar los siguientes pasos:

a. los privilegios de acceso asociados con cada producto del sistema; por ejemplo, sistema de operación, sistema de gestión de base de datos y cada aplicación, y se debieran identificar los usuarios a quienes se les necesita asignar privilegios;

b. Los privilegios se debieran asignar a los usuarios sobre la base de “sólo lo que necesitan saber” y sobre una base de evento-por-evento en línea con la política de control del acceso; es decir, los requerimientos mínimos para su rol funcional, sólo cuando se necesitan;

c. Se debiera mantener un proceso de autorización y un registro de todos los privilegios asignados. No se debieran otorgar privilegios hasta que se complete el proceso de autorización.

d. Se debiera promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios;

e. Se debiera promover el desarrollo y uso de los programas que evitan la necesidad de correr con privilegios;

f. Los privilegios se debieran asignar a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio [7].

CAPÍTULO 3

3.1. Entorno de la Organización.

Ubicación:

La Dirección Distrital De Educación 03d01 Azogues-Biblian–Déleg-Educación, se encuentra situada en la Provincia del Cañar en la parroquia Azogues en las calles Fray Vicente Solano y Luis Cordero Crespo.

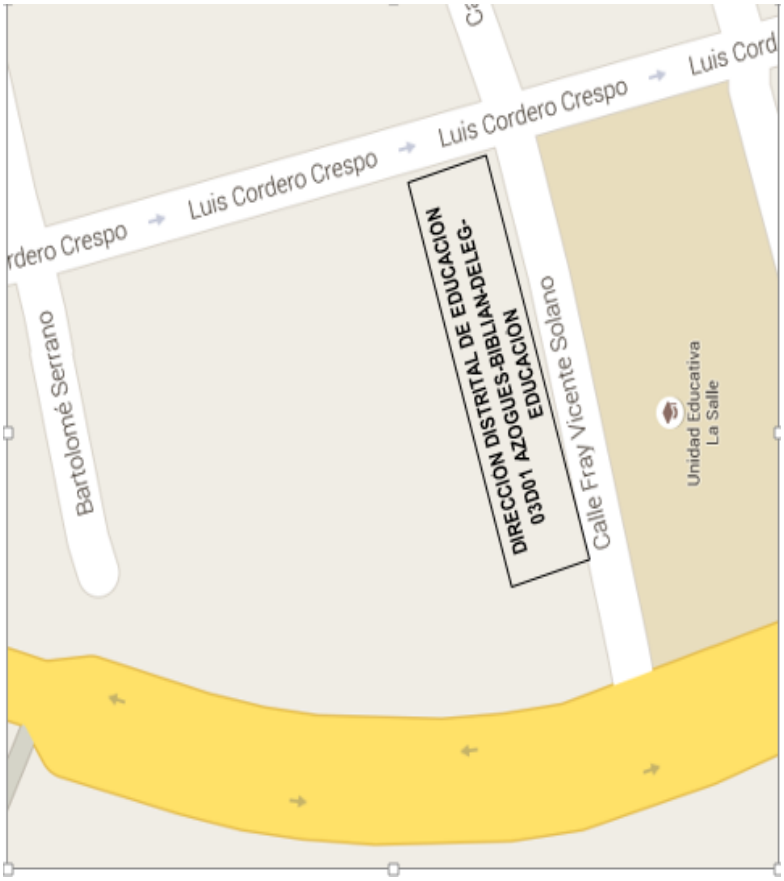


Figura 3.1: Croquis de Ubicación

Atribuciones y Responsabilidades de la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación.

Garantizar una oferta y distribución adecuada de recursos educativos de calidad con la participación de los actores educativos y, adicionalmente, coadyuvar para el fortalecimiento de una cultura de gestión de riesgo en el territorio correspondiente al distrito bajo su jurisdicción [8].

El Distrito se encuentra dividida en los siguientes departamentos y número de funcionarios:

Tabla 1: Estructura del Distrito

DEPARTAMENTO	PERSONAL QUE LABORA
Dirección Distrital	1
Departamento de Secretaria	1
Departamento de planificación	4
Departamento de asesoría jurídica donde labran	2
Departamento de Informática	1
Departamento de Contabilidad	5
Oficina de atención ciudadana	2
Departamento de regulación y seguimiento escolar	4
Departamento de inventarios y bodega	2
Total	22

3.2. Definición de los Activos.

En la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, es una empresa pública sin fines de lucro, dedicada a la supervisión y a la planificación de la educación fiscal y particular de Azogues, Biblián y Déleg. La importancia radica en el correcto manejo de información, donde el área de informática es de vital importancia ya que desde aquí se maneja toda la información, por ello se debe garantizar la seguridad, el manejo oportuno y eficiente de la información.

3.3. Clasificación de la Información.

En el Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación al ser una entidad pública tiene el siguiente manejo de información:

Los oficios y circulares son recibidos a través del departamento de atención ciudadana, personal que escanea los oficios, los archiva y los direcciona con el Sistema de gestión de documentos o Quipux a los demás departamentos que van dirigidos, para que sean procesados y se dé una respuesta. Es importante recalcar que el sistema de Gestión de Documentos o Quipux funciona acorde a un cronograma de respuesta establecido, en donde a través de correos y seguimiento por parte del Director Distrital se establecerá su funcionamiento eficiente y a tiempo. Para dar respuesta a cualquier oficio siempre se le direccionará a la Autoridad de la Institución misma que enviará o imprimirá la respuesta o contestación al oficio dirigida tanto para el docente, institución o persona natural a quien vaya dirigido.

Para ello utilizan el internet, mismo que es manejado desde el departamento de informática, que está constituido por una red de topología de cascada con cable Rj45 interconectados con Switch 2924 – SFP Plus 3CBLG24, los servicios de internet son prestados por la empresa TELCONET, misma que mucha de las veces ha dejado mucho que desear en cuanto a sus servicios ya que se han interrumpido por varias horas dificultando el trabajo en la Dirección. Un servidor de Windows

NT server 2003 que se encuentra aún en funcionamiento, el cual direcciona la red en toda la institución. Cabe señalar que para el control de navegación cuenta con un X5 Digital vaccine, mismo que fue configurado por planta central es decir desde el departamento de informática del Ministerio de Educación cede en Quito, Ingenieros que se encargaron de la implementación tanto de la red como del control, instalación del Servidor, cabe destacar que el personal de Informático no tuvo injerencia ni intervención en la instalación de estos equipos.

A continuación se muestra como está la topología de Red del Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación y las características de sus equipos.

Topología en Cascada

Se trata de un punto de partida en el desarrollo de una red de almacenamiento. Para conseguirlo fácilmente sólo hay que conectar los switches entre sí con un único ISL, utilizando un E-Port o un puerto dedicado a la extensión de la red de almacenamiento. La mayor ventaja de la tecnología en Cascada es su veloz y fácil desarrollo. Su desventaja radica en la carga que recae sobre el nodo central. La cantidad de tráfico que deberá soportar es grande y aumentará conforme vayamos agregando más nodos periféricos, lo que la hace poco

recomendable para redes de gran tamaño. Además, un fallo en el nodo central puede dejar inoperante a toda la red.

Figura 3.2: Estructura de la Red

3 COM X5 Digital vaccine.- Proporciona un filtro de control de ataques., de vulnerabilidades, protocolos, anomalías de tráfico y permite configurar puertos, enlaces y direcciones no deseados. Una de las desventajas es que su actualización dura solo un año en cuanto a las vulnerabilidades.

Figura 3.3: Filtro de Control

Base Switch 2924 – SFP Plus 3CBLG24 Este es el encargado de la interconexión de equipos dentro de la red, que junto al cableado constituyen las redes de área local o LAN.

Figura 3.4: Base Switch

Equipos de Oficina

Cada uno de los empleados del Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación poseen un ordenador con sistema operativo Windows 8, y un hardware de una memoria de 500GB, memoria RAM de 4 GB un procesador Intel Core i3, todos están conectados a la red mediante cables de red RJ45 y por cada oficina comparten una impresora.

3.4. Análisis de los requerimientos del Usuario

3.4.1. De los Administradores del Departamento Informático.

En la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, se ha realizado un análisis del departamento de informática, donde se encontrado que uno de los principales requerimientos de los administradores es el delimitar acciones de contingencia en caso que la red falle, en especial por que no ha sido instalada por ellos. Además se ve en la necesidad de realizar políticas claras para el manejo tanto del software como del hardware.

Es indispensable que se realice un mantenimiento de equipos, debido a que no se ha realizado desde su instalación desde el año 2003.

No existen medidas de contingencia en caso de que exista cualquier tipo de siniestro, como robos, perdida de información, incendios, etc.

3.4.2. Del Usuario

En la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, los usuarios carecen de políticas claras en cuanto al manejo y uso de la información. Se debe desarrollar procedimientos estandarizados para el mantenimiento, mejora y remplazo de equipos informáticos así como la importancia del mantenimiento del Software.

3.5. Análisis de las vulnerabilidades.

Dentro de las vulnerabilidades detectadas dentro de la institución son:

a) Políticas de seguridad en la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, no existen ningún tipo de políticas de seguridad de los activos de la información.

b) Seguridad en el Hardware y software.- Se analizado de que no existe ningún tipo de políticas para el manejo de los equipos, su mantenimiento o remplazo.

   En cuanto al Software se observa que no existe ninguna política de ingreso al sistema por parte del usuario como de los administradores, no hay impedimentos sobre la instalación de programas o ingreso de memorias a los equipos que eviten posibles vulnerabilidades de la información.

c) Seguridad de Recursos Humanos no existe evidencia, que se haya realizado algún tipo de simulacro en caso de algún tipo de siniestro, lo que existe son las adecuadas señalizaciones dentro de la institución.

d) En cuanto al uso de la Gestión de Comunicaciones y Operaciones no existen normativas claras en cuanto al proceso que se debe dar cuando sucede un daño o percance con los equipos informáticos.

e) No existe registro de incidentes contra la seguridad de la información ni medidas de contingencia.

3.6. Análisis de las Amenazas.

a) Software

No existe ningún tipo de políticas de se seguridad, actualización ni mantenimiento del softwares en cuanto lo externo no se detecta un antivirus eficiente y con las debidas licencias para que los sistemas estén bajo un buen resguardo.

En cuanto a la instalación externa de cualquier tipo de programas no se registra ningún tipo de restricción ni control

b) Hardware

Se observa que en cuanto a mantenimiento externo y seguridad física de los equipos no se ha tomado ningún tipo de medidas, no ningún tipo de mitigación para una eventualidad o calamidad en su entorno físico.

c) Activos de la Información.

No existe una alarma en toda la instrucción ni ningún tipo de control cuando las oficinas se encuentran cerradas en caso de algún siniestro, tanto la información física como digital se perdería. Tampoco se detectaron medidas de contingencia en caso de robo de información, no hay el debido control.

No hay ningún tipo de medidas para la gestión de activos de la información.

d) Seguridad de Recursos Humanos.

En cuanto a la seguridad de recursos humanos se ha detectado varias falencias, por cuanto los administradores de Informáticos son los únicos encargados del laboratorio de informático, mismos que no fueron capacitados en el momento de la implementación de la red.

Lo mismo sucede en cada departamento donde cada usuario es el encargado de manejar la información en caso de que alguno faltara no existiría continuidad en los procesos.

e) Seguridad Física y Ambiental

A nivel físico se ha detectado que los equipos no tienen la adecuada seguridad en caso de un siniestro, la institución no cuenta con seguro contra robos, incendios, etc.

La institución no posee guardia ni alarma, las únicas seguridades detectadas son el cerramiento.

En cuanto las instalaciones eléctricas como el edificio es antiguo su construcción es de adobe todas las conexiones y tomas son antiguas y no se ha refaccionado o mejorado de ninguna manera. En cuanto al cableado no está correctamente estructurado ni protegido debido a que los departamentos han sido trasladados de una oficina a otra, las canaletas se encuentran rotas y en otras en total mal estado.

Ante cualquier sobrecarga eléctrica los equipos se encuentran bajo riesgo.

f) Gestión de Incidentes de Seguridad de la Información

Al tener un contrato con la empresa TELCONET, la operatividad del internet no es continua, cuando el sistema de internet falla se detienen todos los procesos debido a que se trabaja con el sistema de QUIPUX

CAPÍTULO 4

4.1. Definición del proceso de Aseguramiento Informático

El Diseño del aseguramiento del entorno Informático de la Dirección Distrital De Educación 03d01 Azogues-Biblián-Déleg-Educación, a través de un levantamiento de información, que se basar primero en crear políticas claras en de manejo de la información, se establece que uno de los principales riesgos son una adecuada instalación eléctrica y de redes de la información.

Crear políticas claras en cuanto al uso de los equipos Informáticos de la empresa realizando políticas de uso y manejó tanto de software como hardware.

Se solicitará al distrito que se ha las gestiones adecuadas para mejorar la seguridad física y ambiental.

Se debe tener una medida de contingencia en caso de que uno de los Departamentos deje de trabajar o uno de los empleados falte.

4.2. Relación de los Activos con el Proceso

En la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación. Al implementar el aseguramiento del entorno informático se garantizará la seguridad, el manejo oportuno y eficiente de la información en caso de cualquier eventualidad.

En caso de que uno de los administradores de los usuarios falte, se garantizará continuidad en los procesos y respuestas.

Cada una de las políticas y de las observaciones en cuanto como se viene desenvolviendo los servicios en el Distrito, ayudara a garantizar tanto la seguridad y continuidad de los procesos.

4.3. Análisis de los Riesgos

4.3.1. Vulnerabilidades

Al no existir ningún tipo de políticas de seguridad ni de mantenimiento en la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, en cuanto al uso del hardware ni software los sistemas, se encuentran siempre en riesgo de amenazas tanto internas como externas. Ya que no existe el debido control de que programas o accesos a la red pueden tener o descargarse.

En cuanto a la seguridad de Recursos Humanos se evidencia que no existe ninguna medida de prevención contra siniestros, a nivel físico se ve que el edificio es poco convencional y no está correctamente distribuido ni diseñado para el funcionamiento que tiene.

4.3.2. Amenazas

En cuanto tanto para el Software como hardware las amenazas externas, son siempre latentes debido a que no tiene las actualizaciones para el sistema operativo, ni antivirus. La continuidad del proceso de la información se ve afectada en el momento de que el servicio de internet falla.

La falta de mantenimiento tanto al cableado de electricidad como de la red, puede ocasionar que el Distrito deje de funcionar.

Al no contar con seguridad física como una alarma o contratar un guardia de seguridad o seguro contra incendios siempre estará latente un robo o un incendio.

Cuando la empresa TELCONET tiene alguna eventualidad y se suspende el servicio de internet, se detienen todos los procesos dentro del Distrito.

4.4. Diseño de la matriz de Riesgos

Tabla 2: Matriz de Riesgos

RIESGO	DESCRIPCIÓN	CAUSAS
Mal uso del software y hardware	1. Tener un software que cubra en parte las necesidad del Distrito 2. Poco de mantenimiento en los equipos	1. No existe un verdadero estudio de las necesidades y requerimientos del Distrito. 2. Falta de conocimiento del uso de los recursos tanto en software como en hardware.
Uso ilícito de la información	1. Riesgos de que se manipule o divulgue la información	1. Nada de control al acceso a la información. 2. No existen políticas de control de la seguridad. 3. Falta de control de acceso a la información.
Sistemas de información Vulnerables	1. Por la falta de control, es posible el ingreso de personal externo a que tengan acceso a la información del Distrito.	1. El control al acceso a la información es escasa. 2. Cortafuegos desactualizado.
Deterioro, pérdida o daño de los recursos tecnológicos	1. Recursos tecnológicos con falta de mantenimientos, obsoletos o que causen perdida de información.	1. Control, protección y mantenimiento. 2. Recursos obsoletos. 3. Factores externos 3. Uso no adecuado. 4.No existe capacitación
Softwares deficientes	1. Software que no garanticen la eficiencia de la información.	1. Carece de recursos para la adquisición de nuevos softwares 2. Falta de mantenimiento y actualización de los sistemas 3. Recursos tecnológicos obsoletos

Uso inadecuado del QUIPUX	1. Inadecuado uso del QUIPUX del portal del Ministerio de Educación	1. Poca capacitación 2. No existe un buen seguimiento y control del sistemas 3. Falta de actualización de los recursos del sistema QUIPUX.
Redes internas y externas defectuosas tanto eléctricas como de información	1. Existe poco mantenimiento de las Redes tanto eléctricas como de telecomunicaciones.	1. Internet defectuosa 2. Sistema eléctrico con poco o nada de mantenimiento 3. Sistema de Redes tanto internas como externas con poco o nada de mantenimiento. 4. No existe el control adecuados de los técnicos del sistema eléctrico y de sus falencias.
Control de acceso al Departamento Informático y áreas tecnológicas.	1. No existen restricciones al ingreso del Departamento Informático y áreas tecnológicas.	1. Falta de control de las instalaciones. 2. Alarma y rejillas dañadas.

4.5. Definición de Probabilidades

Tabla 3: Probabilidad

RIESGO	DESCRIPCIÓN	ALTA	MEDIA	BAJA
Mal uso del software y hardware	1. Tener un software que cubra en parte las necesidad del Distrito	X		
	2. Poco de mantenimiento en los equipos	X		
Uso ilícito de la información	1. Riesgos de que se manipule o divulgue la información		X	

Sistemas de información Vulnerables	1. Por la falta de control, es posible el ingreso de personal externo a que tengan acceso a la información del Distrito.		X	
Deterioro, pérdida o daño de los recursos tecnológicos	1. Recursos tecnológicos con falta de mantenimientos, obsoletos o que causen perdida de información.	X		
Softwares deficientes	1. Software que no garanticen la eficiencia de la información.		X	
Uso inadecuado del QUIPUX	1. Inadecuado uso del QUIPUX del portal del Ministerio de Educación		X	
Redes internas y externas defectuosas tanto eléctricas como de información	1. Existe poco mantenimiento de las Redes tanto eléctricas como de telecomunicaciones.	X		
	2. Incendios	X		
Control de acceso al Departamento Informático y áreas tecnológicas.	1. No existen restricciones al ingreso del Departamento Informático y áreas tecnológicas.		X	

4.6. Definición del Impacto

Tabla 4: Impacto de Riesgos

RIESGO	IMPACTO
Mal uso del software y hardware	Perdidas económicas Parálisis del sistema de información Inestabilidad de los procesos - fallas en la red de datos
Uso ilícito de la información	Mala imagen, Toma de decisiones no adecuadas.
Sistemas de información Vulnerables	Perdidas económicas. Inestabilidad de los procesos. Fuga de información
Deterioro, pérdida o daño de los recursos tecnológicos	Equipos dañados, desaprovechamientos de los recursos tecnológicos
Softwares deficientes	Cambios de precios de compras, perdida de garantías
Uso inadecuado del QUIPUX	Desinformación del Distrito
Redes internas y externas defectuosas tanto eléctricas como de información	Demora en los procesos, perdida de la imagen de la entidad ante el público, perdida de información,, información inoportuna, Incumplimiento del proceso, alteración de la operación. Perdidas físicas en el caso de incendio.
Control de acceso al Departamento Informático y áreas tecnológicas.	Perdida, daños, manipulación, robos en la infraestructura tecnológica

CAPÍTULO 5

Definición de los Esquemas y el Plan de Mitigación.

Planificación e implementación de las políticas de aseguramiento del entorno INFORMATICO DE LA DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DÉLEG-EDUCACIÓN

Tabla 5: Plan de Mitigación

RIESGO	MITIGACIÓN
Mal uso del software y hardware	Crear políticas de seguridad de Software y Hardware.
Uso ilícito de la información	Generar políticas de seguridad de la información y establecer responsabilidades.
Sistemas de información Vulnerables	Realizar un manual de uso de las tecnologías para los trabajadores del distrito.
Deterioro, pérdida o daño de los recursos tecnológicos	Realizar un manual de políticas en caso de daño, deterioro o pérdida de los recursos tecnológicos.
Softwares deficientes	Con respecto a los problemas de ausencia o deficiencia de software el Administrador del departamento de informática deberá dar los informes sobre las posibles consecuencias de no adquirir estos a los Directivos.
Uso inadecuado del QUIPUX	Informar y mantener actualizados a los usuarios sobre el uso del QUIPUX. Con los manuales

	existentes.
Redes internas y externas defectuosas tanto eléctricas como de información	Realizar un seguimiento sobre las fallas que se han detectado en la red, por causa del servidor de internet con la empresa TELCONET. Realizar un informe completo sobre la necesidad de la restructuración de la Red, el cambio de cables que sean necesarios, las acometidas que no están e correcto estado. Generar un informe sobre el estado del cableado eléctrico y sus posibles consecuencias si no se cambia y reestructura por completo.
Control de acceso al Departamento Informático y áreas tecnológicas.	Se debe generar un informe a las Autoridades del distrito, sobre la falta de seguridad física del distrito.

5.1. Políticas De Seguridad De Información De La Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación

5.1.1. Protección de información

Política: Para el mejor uso y mantenimiento de la información, teniendo en cuenta que es un activo, para garantizar su confidencialidad e integridad se generan las siguientes políticas.

Encaminada a: Todos

5.1.2. Revisión de la política de seguridad de la información

Política: Se debe realizar un seguimiento continuo de las políticas aquí establecidas, con el fin de detectar nuevos requerimientos y necesidades; tanto a nivel de seguridad de Software como Hardware.

Encaminada a: Todos

5.1.3. Coordinación de la seguridad de la información

Política: El departamento de Informática será el encargado, de la coordinación y el seguimiento de las políticas implementadas de realizar un registro, para luego establecer los lineamientos que sean necesarios ser adecuados.

Encaminada a: Todos

5.1.4. Proceso de autorización para nuevos medios de almacenamiento de información

Política: El departamento de informática será el encargado de determinar cuáles son los medios idóneos, para el almacenamiento de información, bajo que resguardo y responsables debe encontrarse.

Encaminada a: Todos

5.1.5. Acuerdos de confidencialidad

Política: El departamento de informática debe ser el encargado de realizar actas de compromiso de confidencialidad, para aquellos usuarios que tengan a acceso a información estratégica y de un alto grado de importancia. Al mismo tiempo deber realizar socializaciones sobre la importancia de la restricción a la información de que cada departamento maneja y sobre su responsabilidad.

Encaminada a: Todos

5.1.6. Clasificación de la información

Política: El departamento de informática, conjuntamente con las autoridades del Distrito determinará cuales son las áreas estratégicas, que manejarán los activos de la información determinando los responsables en caso de cualquier tipo de inconveniente presentado.

Encaminada a: Todos

5.1.7. Uso de información

Política: El Distrito determinará y clasificara por departamentos el uso que se dé a los activos de la información, determinando cuáles serán las posibles sanciones en caso de un mal manejo.

Encaminada a: Todos

5.1.8. Manejo de información, acceso y uso

Política: Desde el Ministerio de educación viene ya dado las políticas y normas de cuáles son las acciones y departamentos, que manejaran y darán proceso a la información. Así como las sanciones en caso de incumplimiento.

Encaminada a: Todos

5.1.9. Eliminación de derechos de acceso

Política: El departamento de informática será el encargado de ejecutar las restricciones y reformas necesarias, para evitar el acceso a la información en caso, de que se haya terminado cualquier tipo de contrato o cese de funciones de un empleado o compañía.

Encaminada a: Todos

5.1.10. Devolución de activos

Política: El Departamento de Informática será el encargado de que una vez cesado cualquier tipo de contrato con una empresa o empleado, de solicitar cualquier activo de la empresa que maneje información sea hardware o software.

Encaminada a: Todos

5.1.11. Procedimientos de operación

Política: El Departamento de Informática debe tener un registro de operaciones y actividades que se desarrollan en cada departamento, con respecto al manejo y actividades que desarrollan con los activos de la información, para dar continuidad en los procesos ante cualquier eventualidad al igual que del mismo departamento.

Encaminada a: Todos

5.1.12. Segregación de responsabilidad

Política: El Departamento de Informática, conjuntamente con la Autoridad del Distrito debe delimitar cada una de las actividades de los empleados por departamento, con el objetivo de definir responsabilidades

Encaminada a: Todos

5.1.13. Ambientes de prueba, desarrollo y operacionales

Política: El Ministerio de Educación pone en marcha nuevos sistemas o los actualiza, por lo cual el encargado de Sistemas, debe tener siempre un respaldo o un equipo de pruebas para evitar cualquier inconveniente con la continuidad de los procesos.

5.1.14. Reclamos por datos y programas

Política: El Departamento informática no tendrá ningún tipo de responsabilidad, en caso de daño o pérdida de información. Es importante recalcar que el Ministerio de Educación debe generar un ambiente de trabajo propicio, entregando los equipos con sus respectivas licencias, los softwares puestos en marcha deben ser garantizados por cualquier eventualidad. Los usuarios también deben seguir las políticas y normas establecidas para el uso de los programas y datos.

Encaminada a: Usuarios finales

5.1.15. Control contra software malicioso

Política: El Ministerio de Educación es quien garantiza la compra, actualización de los Antivirus del mercado. El departamento de informática será el encargado de implementarlos y de darles mantenimiento.

Encaminada a: Todos

5.1.16. Control contra dispositivos móviles

Política: Dentro del Distrito está permitido el uso de dispositivos móviles, siempre y cuando no tengan virus o sea para pasar información que no esté relacionada con sus labores.

Encaminada a: Todos

5.1.17. Procedimientos de manejo de la información

Política: El Distrito ha establecido según sea el cargo o su función, sobre la responsabilidad del acceso y manejo de la información.

Encaminada a: Todos

5.1.18. Intercambio de información

Política: Cada uno de los empleados son responsables de los activos de la información que manejan, de ser necesario el intercambio de información, serán los responsables de su uso correcto, en caso de cualquier eventualidad será el Director quien determine responsabilidades en base a investigaciones.

Encaminada a: Todos

5.1.19. Uso de Certificado Digitales

Política: Acorde a la Ley solo el Director Distrital es el que posee un Certificado Digital mismo que es el responsable de su uso y manejo.

Encaminada a: Todos

5.1.20. Comercio electrónico

Política: Desde el Departamento de Bodega es el encargado de cualquier solicitud al Ministerio de Educación, quienes son los responsables de cualquier eventualidad.

5.1.21. Transacciones en línea

Política: El Departamento de Bodega es el encargado de realizar cualquier tipo de transacción en línea, por lo que ellos serán los responsables directos.

5.1.22. Información disponible de forma pública

Política: Para cualquier tipo de publicación para conocimiento de la población, el departamento de informática será el responsable de publicarle en la página Web de la institución, misma que será protegida de cualquier tipo de vulnerabilidad o amenazas.

5.1.23. Control de legalidad

Política: Las políticas de seguridad de la información fueron generadas acorde a las necesidades y requerimientos del Distrito, por lo que se debe garantizar un continuo seguimiento y en caso de necesidad de actualización de las mismas.

5.1.24. Excepciones a las políticas

Política: Las policías son para el cumplimiento por parte de todos los actores del Distrito de Educación, se tomara como referencia la única excepción que puede ser por causa económica debido a cualquier eventualidad que no haya sido garantizada por el Ministerio de Educación.

Encaminada a: Todos

5.1.25. Control de las transgresiones

Política: El Departamento de Informática es quien a través de diferentes formularios ya sea en línea o digitales tendrá constancia de todas las transgresiones detectadas por los otros departamentos, mismos que serán los encargados de realizar cada trimestre a la Autoridad en caso de que sean transgresiones leves. En caso de transgresiones grabes se tendrá que realizar el debido informe de manera inmediata

Encaminada al: Director Distrital

5.1.26. Revocación de privilegios de acceso

Política: La revocatoria de acceso será potestad únicamente de la máxima Autoridad al detectar una trasgresión grave, donde el Departamento de informática será el encargado de ejecutarlo.

Encaminada a: Usuarios finales

5.1.27. Estándares específicos para la seguridad de información

Política: Todo el personal de Informática en base a los informes y solicitudes sobre fallas tanto en el software o en hardware, desarrollara un esquema de procedimientos para solucionar de manera urgente cualquier tipo de eventualidad detectado. Si es error del usuario tendrá que realizar una capacitación al mismo para evitarlo.

Encaminada a: Personal técnico

5.1.28. Uso de políticas de seguridad de información y procedimientos

Política: El presente documento de nomas y procedimientos es desarrollado para ser aplicado únicamente dentro de la Dirección Distrital De Educación 03d01 Azogues-Biblián-Déleg-Educación

Encaminada a: Todos

5.1.29. Operación de controles de seguridad

Política: El Departamento informático será el encargado de la socialización y puesta en marcha de las políticas y normas de unos de los activos de la información.

Encaminada a: Administración y personal técnico

5.2. Infraestructura de seguridad de información

5.2.1. Administración de seguridad de la información:

5.2.1.1. Control de seguridad de información

Política: El Departamento de Informática es el encargado de garantizar con sus políticas y normas establecidas acorde a las necesidades del Distrito, el normal funcionamiento, garantizando la confidencialidad e integridad de la información

Encaminada a: Administración y personal técnico

5.2.2. Coordinación De Seguridad De Información

5.2.2.1. Riesgos significativos de seguridad de información

Política: El Departamento de informática establecido políticas y normas para los riesgos detectados dentro de la empresa para los activos de la información.

5.2.3. Asignación De Responsabilidades De Seguridad De Información

5.2.3.1. Control de asignación de responsabilidades de seguridad de la información

Política: Cada uno de los empleados según el papel que desempeñen serán los responsables de la administración de la información que se les confía. Ellos serán sancionados según la ley en caso de cualquier tipo de una mala manipulación de la información.

Encaminada a: Administración

5.2.3.2. Cambios de estatus

Política: Se notificara de forma inmediata por parte de la Autoridad, al departamento informático, en caso de que un empleado haya cambiado de funciones o que se haya contratado a personal externo, y que necesiten acceso a los activos de la información.

5.2.3.3. Enfoque a la administración de la seguridad

Política: El Departamento de informática debe realizar campañas de concienciación y de capacitación a los usuarios de forma periódica. Así mismo debe realizar un seguimiento a las políticas y normas para actualizarlas o modificarlas de ser necesario.

5.2.3.4. Evaluaciones de riesgos

Política: Esta evaluación de riesgos es desarrollada por los bomberos, personal de la empresa eléctrica y por informes de los diferentes departamentos que conforman el distrito.

Encaminada a: Administración

5.2.3.5. Aprobación de cambios en los sistemas de información

Política: Cualquier tipo de cambios en el sistema de la información o manejo de activos de la Información, están dictados o reglamentados por el Ministerio de Educación quien es el encargado de gestionar los medios económicos y personal técnico para ser implementados.

5.2.3.6. Seguridad de información centralizada

Política: El Ministerio de Educación es quien dicta sus reglas y políticas del manejo de la información, las posibles sanciones y correcciones. El Distrito es el encargado de ejecutarlas y de velar que se cumplan.

5.2.3.7. Responsabilidades del área funcional de seguridad de información

Política: El Departamento con la finalidad de establecer reglas claras y concisas ha establecido sus propias normas y políticas

del manejo de los activos de la información, con el fin de garantizar continuidad en los procesos.

Encaminada a: Usuarios finales

5.2.3.8. Misión del área funcional de seguridad de información

Política: El Departamento de informática está encargado de que la información este siempre a la mano del usuario garantizando su confiabilidad y disponibilidad.

Encaminada a: Departamento de Informática.

5.2.3.9. Estándares y procedimientos de seguridad de información

Política: En base a los requerimientos, fichas y problemas detectados tanto por el departamento de sistemas como parte de los usuarios serán los encargados de ir actualizando y mejorando las políticas y estándares de seguridad de la información.

Encaminada a: Todos

5.2.3.10. Planes de seguridad de información

Política: Trabajando en forma trimestral se debe realizar un planes de contingencia ante problemas y vulnerabilidades detectados.

Encaminada a: Administración

5.2.3.11. Manual de seguridad de información

Política: El Departamento de Informática es el encargado de realizar un manual de políticas de seguridad de la Información.

5.2.3.12. Contacto de seguridad de información

Política: Conjuntamente el Departamento de Recursos Humanos con el de Sistemas serán los responsables de socializar las políticas y normas de manejo de los Activos de la Información a los empleados y nuevos trabajadores.

5.2.3.13. Asignación de propiedad de la información

Política: Los activos de la información deben estar bien distribuidos acorde a las necesidades del usuario estableciendo sus respectivas responsabilidades.

5.2.3.14. Responsabilidad de propiedad en el área informática

Política: Se reconocerá únicamente como activos del área de informática aquello que esté debidamente inventariado por el departamento de bodega del Distrito de educación.

5.2.3.15. Custodio de la información

Política: Cada usuario será el responsable directo de la información que maneja, mismo que será amonestado según dicte la ley.

Encaminada a: Todos

5.2.3.16. Responsabilidades del custodio de la información

Política: El Departamento de informática es el encargado de que la información este presta y activa para garantizar los procesos del Distrito de Educación.

5.2.3.17. Responsabilidades del usuario de información

Política: Los Activos de la información están bajo resguardo exclusivo de los empleados acorde a sus funciones en caso de un daño técnico tendrán que comunicar al departamento informático.

Encaminada a: Todos

5.2.3.18. Delegación de propiedad de la información

Política: No se podrá dentro del Distrito delegar funciones a ningún compañero previa autorización del Director Distrital en caso de cualquier siniestro

Encaminada a: Todos.

5.2.3.19. Políticas de acceso de información

Política: En base a los lineamientos del Ministerio de Educación se procederá a establecer cuáles son las políticas de acceso a la información.

Encaminada a: Departamento Informático.

5.2.4. CONTROL DE ACCESOS A LA INFORMACIÓN Y SISTEMAS

5.2.4.1. Administración de accesos de los usuarios

Política: La administración de los activos de la información será registrada por el departamento de Informática. Delimitando el acceso según la necesidad del usuario.

Encaminada a: Todos

5.2.4.2. Registro de usuarios

Política: El Departamento de Informática tendrá un registro de todos los Usuarios del sistema.

Encaminada a: Todos

5.2.4.3. Gestión de privilegios

Política: El Departamento de Informática en base a disposiciones de la Autoridad dará los privilegios y servicios de la información.

Encaminada a: Todos

5.2.4.4. Revisión de derechos de acceso del usuario

Política: El Departamento de informática revisara los permisos y accesos siempre y cuando sea por petición de la Autoridad Distrital.

Encaminada a: Todos

5.2.4.5. Acceso al ambiente de producción

Política: El ingreso al Departamento Informático, para los usuarios está totalmente restringido.

Encaminada a: Todos

5.2.4.6. Protección del equipo informático de trabajo

Política: Cada uno de los usuarios serán los encargados de emitir un informe en caso de fallas tanto de Hardware como de software al departamento de Informática, quienes tendrán que dar una solución oportuna.

Encaminada a: Todos

5.2.4.7. Administración de controles de acceso a la red

Política: El Acceso de la Red será determinada por el Departamento de Informática, quienes serán los encargados de dar los privilegios a los usuarios del Internet.

Encaminada a: Todos

5.2.4.8. Control de acceso al software de los sistemas operativos

Política: La Dirección distrital tiene software propios y especializados que serán manejados exclusivamente por los Departamentos pertinentes. Se les dará el debido seguimiento y en caso de fallas se notificara a planta central, es decir el Ministerio de Educación.

Encaminada a: Todos los Departamentos

5.2.4.9. Administración de contraseñas

Política: En caso de las contraseñas cada usuario tendrá la facultad de poner su propia contraseña, previa solicitud al departamento informático, quienes tendrán un registro.

Encaminada a: Todos

5.2.4.10. Seguridad en acceso físico a áreas no autorizadas

Política: El ingreso a las áreas de acceso no autorizado, está indicado solo por la Autoridad Distrital quien dispondrá quien dispondrá quien tiene acceso a ellos.

Encaminada a: Todos

5.2.4.11. Restricciones de acceso

Política: Los accesos al estar controlados por la Autoridad Distrital a lugares restringidos, será quién establezca responsabilidades en caso de pérdida física o de información.

Encaminada a: Todos

5.2.4.12. Accesos y uso de sistemas de monitoreo

Política: Los accesos a la información se encuentran registrados en el Servidor del sistema, se dará un informe solo cuando el Director Distrital lo requiera, o el Departamento de Informática crea pertinente.

Encaminada a: Todos

5.2.4.13. Acceso a los archivos y documentos

Política: El acceso a los activos de la información. En caso de ser requeridos será entregado solo con permiso de la Autoridad Distrital.

Encaminada a: Todos

5.2.4.14. Controles de acceso a sistemas de alto riesgo

Política: El acceso a la información de alto riesgo como es el registro de actividades tendrá solo acceso el Jefe de talento humano y el personal de informática. Quienes tendrán prohibida su divulgación y realizarán el informe a la Autoridad Distrital.

Encaminada a: Todos

5.2.4.15. Identificación del equipo en red

Política: El departamento de Informática será el encargado de ingresar en cada dispositivo del sistema una dirección IP para ser reconocido.

Encaminada a: Todos

5.2.4.16. Protección del puerto de diagnóstico remoto

Política: El departamento de informática es el encargado de autorizar la conexión de equipos remotos.

Encaminada a: Todos

5.2.4.17. Segregación en redes

Política: El Departamento de informático es el encargado.

Encaminada a: Todos

5.2.4.18. Control conexión en redes

Política: Solo el departamento de informática es el encargado de permitir la conexión de nuevos equipos en red.

Encaminada a: Todos

5.2.4.19. Sesión inactiva

Política: Las sesiones se desactivara después de 5 minutos que el equipo no detecte una actividad.

Encaminada a: Todos

5.2.4.20. Limitación del tiempo de conexión

Política: En caso de equipos externos solo se restringirá la conexión borrando su MAC de acceso.

Encaminada a: Todos

5.2.4.21. Computación móvil y comunicaciones

Política: Los equipos móviles y de comunicación tendrán acceso solo previa autorización de la Directora Distrital en caso de la Red de Internet.

Encaminada a: Todos

5.2.4.22. Control al acceso remoto de usuarios

Política: El control de acceso remoto se realiza el seguimiento a través de usuario y contraseña que son intransferibles.

Encaminada a: Todos

5.2.5. PERSONAL DE SEGURIDAD DE INFORMACIÓN

5.2.5.1. Conocimiento de políticas:

Política: Las políticas del Distrito de Educación conocen cada uno de los integrantes del distrito

Encaminada a: Todos

5.2.5.2. Cumplimiento con las políticas y estándares de seguridad

Política: El Departamento de Sistemas y de Recursos Humanos son los encargados de dar seguimiento y hacer cumplir con las políticas y normas de los activos de la información.

Encaminadas a: Todos

5.2.5.3. Capacitación para la administración de los sistemas

Política: El departamento de Sistemas es el encargado de dar las capacitaciones a los nuevos administradores del sistema.

Encaminada a: Usuarios finales

5.2.5.4. Entrenamiento en los servicios informáticos

Política: El departamento informático es el encargado de la capacitación de los servicios informáticos, con charlas y manuales de usuarios., a los nuevos empleados

Encaminada a: Todos

5.2.5.5. Manual de prácticas de seguridad de información

Política: El departamento informático es el encargado de entregar un folleto sobre las políticas y normas de los activos de la información y su adecuado uso.

Encaminada a: Todos

5.2.5.6. Responsabilidades y procedimientos

Política: El Departamento de Informática tiene su manual de responsabilidades y procedimientos dentro del Distrito

Encaminada a: Todos

5.2.5.7. Aprendizaje de los incidentes en la seguridad de información

Política: El departamento de Informático se manejará con una bitácora de eventos, para registrar todo tipo de eventualidades detectadas y hacer el debido seguimiento y correcciones.

5.2.5.8. Conocimiento de políticas

Política: Las políticas serán socializadas a todos los empleados del Distrito con cursos, folletos, seminarios de concienciación sobre el uso correcto de los recursos informáticos.

Encaminada a: Todos

5.2.5.9. Cambios a las políticas de seguridad de información

Política: En caso de modificaciones a las políticas de seguridad el departamento de informática será el encargado de notificar.

Encaminada a: Todos

5.2.5.10. Responsabilidad sobre la capacitación formal

Política: Toda Capacitación será previamente planificada y planeada desde el departamento de informática, donde se generará manuales y folletos para los usuarios en caso de nuevos software o uso de nuevas tecnologías.

Encaminada a: Todos

5.2.5.11. Tiempo de capacitación

Política: El departamento de Informática realizara un cronograma de capacitación para el conocimiento de las normas y políticas del manejo de los activos de la Información.

Encaminada a: Todos

5.2.5.12. Consentimiento de políticas

Política: Todos el personal externo contratado por el Distrito tendrá que cumplir con las normas y políticas establecidas, para el manejo correcto de la información.

Encaminada a: Contratos externos

5.2.5.13. Entrenamiento en sistemas de producción

Política: El Departamento de Informática en caso de cualquier cambio en el sistema implementado por el Ministerio de Educación, serán los primeros en ser capacitados y luego ellos serán los precursores del cambio.

5.2.5.14. Educación técnica y capacitación

Política: El Personal del Departamento Informático, serán personas instruidas y de una gran calidad y calidez humana, con el fin de que puedan trasmitir sus conocimientos al usuario.

Encaminada a: Personal técnico

5.2.5.15. Responsabilidad de seguridad de información

Política: Desde el departamento de Informática hasta cada uno de los usuarios serán los responsables de la seguridad y del control de los activos de la información.

Encaminada a: Todos

5.2.6. SEGURIDAD FÍSICA Y AMBIENTAL

5.2.6.1. Áreas de seguridad

Política: Cada uno de los departamentos del Distrito debe restringir el acceso a su información tanto a nivel física como electrónica, para ello deben notificar al guardia en caso de cualquier incidente y si es grabe al departamento de Informática.

Encaminada a: Todos

5.2.6.2. Seguridad perimetral

Política: La Seguridad del Distrito está determinada por un guardia un sistema de alarma.

Encaminada a: Todos

5.2.6.3. Controles a entradas físicas

Política: En la puerta del Distrito se encuentra un guardia de Seguridad mismo que es el encargado de la seguridad del ingreso solo a personal autorizado.

Encaminada a: Todos

5.2.6.4. Trabajando en áreas restringidas

Política: Todos los Activos de la Información se encuentran centralizados en una base de datos en Quito por lo que es difícil su acceso, es importante recalcar que el área informática se encuentre restringida al usuario como al público.

Encaminada a: Todos

5.2.6.5. Seguridad del equipo

Política: Cada uno de los equipos del departamento de informática se encuentra bajo el cuidado y responsabilidad de sus usuarios. En caso de daño o robo se tendrá que informar al Departamento de Informática.

Encaminada a: Todos

5.2.7. ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

5.2.7.1. Actualizaciones de seguridad

Política: Todas las actualizaciones tanto del sistema informático como de los antivirus, está regido por el Ministerio de Educación y será implementado una vez sea establecido por el mismo.

Encaminada a: Personal técnico

5.2.7.2. Planes de atención de contingencias informáticas

Política: En caso de que el sistema tenga algún tipo de dificultad, se comunicara al Departamento de Informática, quienes llevaran un registro en su bitácora, quienes tratarán de solucionar el problema.

Responsable: Departamento de Informática.

Encaminada a: Todos

5.2.7.3. Equipo de atención de emergencias informáticas

Política: Los equipos que tenga un daño de Software o Hardware serán llevados al departamento de informática, para ser examinados, se arreglaran y serán devueltos a sus usuarios. Caso contrario se darán de baja y se les solicitara que pidan a la Autoridad la restitución del mismo.

Responsable: Departamento de Informática.

Encaminada a: Todos

5.2.7.4. Prueba de equipos de atención de emergencias informáticas

Política: Trimestralmente se realizar pruebas de equipos de la red y de internet para estar preparados en caso de algún contingente o daño.

Responsable: Departamento de Informática.

Encaminada a: Todos

5.2.7.5. Detección de intrusión en los sistemas

Política: En caso de que un sistema haya sido vulnerado se deberá notificar al departamento Informático, quienes darán el debido seguimiento. Se realizará los informes respectivos a la Autoridad del Distrito y se anotará en la bitácora de sucesos.

Responsable: Departamento de Informática.

Encaminada a: Todos

5.2.7.6. Identificación de puntos de ataque

Política: Si se ha identificado al equipo que ha vulnerado la información y detectado al usuario responsable será debidamente notificado a la Autoridad Distrital. Para que sea sancionado según la ley.

Responsable: Departamento de Informática.

5.2.7.7. Procedimientos de atención de intrusiones

Política: En el caso de que ingrese un intruso en el sistema se notificar al Departamento de Informática luego de ellos se realizara conjuntamente un informe de los daños detectados o robo, a la Autoridad Distrital. Además de ello se escribirá en la bitácora de sucesos.

Encaminada a: Todos

5.2.7.8. Avisos de vulnerabilidades

Política: El personal de informática deberá revisar las vulnerabilidades detectadas por el sistema y emitir reportes. Además de ellos se deberá realizar modificaciones y cambios para evitarlas.

Encaminada a: Departamento de informática.

5.2.7.9. Comunicación de incidentes de seguridad de información

Política: Se debe hacer lecturas de los reporte de los sistemas acerca de los incidentes detectados, establecer los lineamientos para evitarlos y mantener un registro en la bitácora de sucesos.

Encaminada a: Departamento de informática.

5.2.7.10. Problemas de acceso no autorizado

Política: Si se ha logrado ingresar al sistema de red a una usuario no registrarlo se anotara en la bitácora de sucesos y se procederá de inmediato a desconectarlo de la red.

Encaminada a: Departamento de informática.

5.2.7.11. Resolución de problemas de seguridad de información

Política: Todos los incidentes de seguridad detectados, que sean de un alto grado de ataque debe ser notificado a la Autoridad Distrital y anotado en la bitácora de sucesos.

Encaminada a: Todos

5.2.7.12. Roles y responsabilidades en el manejo de incidentes

Política: en general todos las vulnerabilidades, ataques, pérdidas de información, equipos defectuosos o dañados serán notificados al departamento informático quienes tendrán una Bitácora de sucesos.

Encaminada a: Departamento de informática.

5.2.8. DESARROLLO Y MANTENIMIENTO DE SOFTWARE

5.2.8.1. Manejo de librerías de programas ejecutables en producción

Política: Las librerías serán ejecutadas conjuntamente con el usuario, en un ambiente seguro para realizar las pruebas pertinentes y determinar su correcto funcionamiento.

Encaminada a: Departamento de informática.

5.2.8.2. Manejo de librerías de programas fuente

Política: Serán tratados conjuntamente con el usuario y puestos en marcha una vez en funcionamiento se le pedirá al programador que nos realice visitas periódicas para dar seguimiento al sistema.

Encaminada a: Departamento de informática.

5.2.8.3. Análisis y especificación de los requerimientos de seguridad

Política: Para la instalación de nuevos programas se debe estipular cuales son los requerimientos para su correcto funcionamiento tanto en especificaciones de software como de hardware

Encaminada a: Departamento de informática.

5.2.8.4. Control de cambios durante el desarrollo de software

Política: El departamento informático será el encargado de autorizar cualquier tipo de cambio de software o hardware del sistema, lo instalara y lo pondrá en marcha.

Encaminada a: Todos.

5.2.8.5. Revisión técnica después de cambios en aplicaciones y sistemas operativos

Política: Cuando se realiza un cambio del sistema el departamento de informática será el encargado conjuntamente con el usuario de notificar su correcto desempeño o sus fallas.

Encaminada a: Todos

5.2.8.6. Control de software operacional

Política: El departamento de informática será el encargado de instalar cualquier tipo de software operacional entregado por el Ministerio de educación. Además de ello de dar las capacitaciones requeridas en caso de ser necesarias.

Encaminada a: Todos

5.2.8.7. Desarrollo de software por proveedores

Política: En caso de instalar un software desarrollado para el Distrito se dará el debido seguimiento para observar si el aplicativo funciona correctamente, el técnico de sistemas o monitoreará al usuario y le pedirá informes.

Encaminada a: Departamento de Informática

5.2.8.8. Control de vulnerabilidades técnicas

Política: Se debe realizar un seguimiento a la bitácora de sucesos y de ir encontrando las soluciones a las notificaciones de vulnerabilidades encontradas para mejorar el sistema informático del distrito.

Encaminada a: Departamento de Informática

5.2.8.9. Control de listas de programas y sistemas operativos

Política: Las actualizaciones serán implementadas bajo la dirección del Ministerio de Educación.

Encaminada a: Departamento de Informática

5.2.8.10. Control de versiones de programas

Política: El departamento de informática conjuntamente con los usuarios serán los encargados de mantener los equipos en buen funcionamiento y los programas actualizados. Previa indicaciones del Ministerio de Educación o desembolso del mismo.

Encaminada a: Todos

5.2.8.11. Desarrollo de software

Política: En caso de ser necesario el Ministerio de Educación es el encargado de proporcionar los instaladores, código fuente de los programas desarrollados para uso exclusivo de ciertos departamentos mismos que están en constante actualización. Que serán implementados y puestos en marcha por el departamento de informática.

Encaminada a: Todos

5.2.8.12. Correcciones de emergencia al software

Política: El Ministerio de Educación desde su departamento de sistemas es el encargado de corregir cualquier tipo de fallas o errores en los sistemas implementados, estos serán ejecutados por el departamento de Informática.

Encaminada a: Todos

5.2.8.13. Autorización de cambios al sistema

Política: Todo cambio en el software es de autorización exclusiva del Ministerio de Educación.

Encaminada a: Todos

5.2.8.14. Desarrollo de nuevos sistemas o aplicaciones

Política: El desarrollo de nuevos aplicativos está regido por el Ministerio de Educación quienes son los encargados de distribuir a todos los usuarios de los diferentes distritos del País.

Encaminada a: Todos

5.2.8.15. Ambiente de desarrollo y ambiente de producción

Política: El ambiente de desarrollo y de producción de nuevos software se encuentra en el Ministerio de Educación.

Encaminada a: Todos.

5.2.9. Prueba y Entrenamiento

5.2.9.1. Pruebas al software antes de pasar a productivo

Política: La puesta en marcha y ejecución de un nuevo software será conjuntamente con el Departamento a quien va dirigido y con el de informática.

5.2.9.2. Planear capacitación y pruebas del nuevo sistema

Política: El Ministerio de Educación es el que indica quien o quienes se van a las capacitaciones para la incorporación de nuevos sistemas, mismos que tendrán que socializar en el distrito.

5.2.9.3. Ejecución en paralelo

Política: El Ministerio de Educación se encarga de poner en prueba los sistemas en diferentes Distritos, mismos que notifican cualquier tipo de errores o problemas encontrados.

Encaminada a: Todos

5.2.9.4. Capacitación en el nuevo sistema

Política: El Ministerio de Educación es el encargado de capacitar a los usuarios del nuevo sistema según al departamento que esté diseñado.

5.2.9.5. Documentación del sistema

Política: En caso de que ya en puesto en marcha el sistema presente múltiples errores y problemas será el departamento de informática quien notifique al Ministerio de educación, para que se hagan los correctivos necesarios

5.2.10. Administración De La Continuidad De Operatividad Del Distrito De Educación

5.2.10.1. Requerimientos de apoyo ante emergencias y desastres

Política: En el evento de una emergencia o desastre se debe poner en operación equipos y programas de cómputo, políticas y procedimientos relacionados adecuados para recuperar los procesos críticos, de acuerdo con el plan de recuperación de desastres establecido.

Dirigida a Personal técnico

5.2.10.2. Incluir seguridad de la información en el proceso de gestión de continuidad de negocio

Política: En caso de que se tenga inconvenientes en la continuidad de los procesos es necesario que se ponga en acción el plan de contingencia establecido en la bitácora de suceso.

5.2.10.3. Continuidad operacional y evaluación del riesgo

Política: El departamento de informática ha delimitado que uno de los riesgos puede ser delimitado don el plan establecido en la bitácora de sucesos.

5.2.10.4. Accesibilidad del plan de contingencia

Política: En caso de cualquier inconveniente se deberá poner en práctica el plan de contingencia antes establecido para ello se podrá contar con la bitácora de sucesos.

5.2.10.5. Asignación de recursos para apoyo a los planes de continuidad de operatividad

Política: En caso de que los recursos o procesos se vean afectados, el personal de informática será el encargado de gestionar ante el Ministerio de Educación los recursos conjuntamente con la Autoridad del distrito.

5.2.11. ANÁLISIS DEL IMPACTO Y CONTINUIDAD DE NEGOCIO

5.2.11.1. Evaluación de la criticidad de aplicaciones multiusuario

Política: El departamento de informática debe está preparado para una carga de multiusuarios de sus sistemas.

5.2.11.2. Esquema de clasificación de criticidad de aplicaciones de cinco categorías

Política: La bitácora de sucesos debe establecer normas y políticas para mitigar problemas de categoría postergarles, no críticas, moderadamente críticas, críticas y altamente citicas.

Encaminada a: Departamento de Informática

5.2.11.3. Análisis de impacto

Política: En la Bitácora de sucesos se tendrá que realizar un estudio de mitigación de forma anual para estar listos para cualquier imprevisto.

Encaminada a: Departamento de Informática

5.2.11.4. Evaluación de la prioridad de recuperación de aplicaciones multiusuario

Política: La Bitácora de sucesos permitirá al personal de informática restablecer los recursos y aplicaciones para poner en marcha la operatividad del Sistema.

Encaminada a: Departamento de Informática

5.2.11.5. Preparación y mantenimiento de planes de continuidad de la operatividad del distrito de educación

Política: Los planes de contingencia para determinar que los procesos y actividades continúen dentro del distrito, serán implementados según lo establecido en la bitácora de sucesos.

Encaminada a: Departamento de Informática

5.2.12. Esquema De Planificación De Continuidad De Operatividad Del Distrito De Educación

5.2.12.1. Planificación de continuidad de operatividad e informática

Política: Los planes de continuidad y de operatividad de los procesos, serán aplicados una vez sean detectados los inconvenientes realizando las pruebas pertinentes. Teniendo en cuenta la bitácora de sucesos.

Encaminada a: Departamento de Informática

5.2.12.2. Expectativas de los funcionarios respecto a la recuperación de la operatividad.

Lineamiento: Una vez detectado el inconveniente dentro de los procesos por parte del departamento de informática se procederá a activar el plan de contingencia y realizar el uso correcto del sistema dentro del distrito.

Encaminada a: Usuarios finales

5.2.13. Pruebas, Mantenimiento Y Re-Evaluación De Planes De Continuidad De Operatividad Del Distrito De Educación

5.2.13.1. Operación con procedimientos manuales

Política: El plan de contingencia cuando ocurra un evento imprevisto debe ser reportado y escrito en la bitácora de sucesos con el fin de encontrar de la forma más rápida la solución al inconveniente. Ponerlos en marcha y garantizar la continuidad de los procesos.

Encaminada a: Departamento Informático

5.2.13.2. Rotación de personal bajo el modelo de contingencia

Política: Los miembros del departamento de informática deben estar siempre actualizados con cada uno de los sucesos de

vulnerabilidades detectados, con el fin de que cada uno de ellos sepa como mitigarlos.

Encaminada a: Departamento Informático

5.2.13.3. Niveles de apoyo durante la interrupción de la operatividad del Distrito

Política: Ante un evento o desastre se debe realizar un reporte que ira a la bitácora de sucesos, donde se informará detalladamente los pasos a seguir para corregir el problema.

Encaminada a: Departamento Informático

5.2.13.4. Pruebas de los planes de contingencia

Política: Se debe realizar pruebas documentadas de cada una de las soluciones planteadas, contra las vulnerabilidades que se pudieron solucionar en el distrito. Para garantizar la continuidad de los procesos

Encaminada a: Departamento Informático

5.2.13.5. Pruebas de información de contacto

Política: Los técnicos del departamento informático de la Dirección Distrital son los encargados, de mantener actualizado los registros de los empleados de forma periódica

Encaminada a: Departamento Informático

5.2.13.6. Roles y responsabilidades en la planificación de contingencias y recuperación de sistemas

Política: Los técnicos de informática para mantener los sistemas y aplicativos en funcionamiento deberá realizar un seguimiento y monitoreo permanente con el fin de encontrar los posibles defectos o falencias mismos que se registraran en la bitácora de sucesos del Distrito

Encaminada a: Departamento Informático

5.2.14. Cumplimiento Con La Legislación Y Los Requerimientos De Las Políticas

5.2.14.1. Identificación de la normativa vigente

Política: El Departamento informático a través de las normativas establecidas dentro del distrito y dictadas por el Ministerio de Educación, realizaran las revisiones gerenciales en conjunto con sus jefes departamentales actualizando la bitácora de sucesos, de manera mensual.

Encaminada a: Departamento Informático

5.2.14.2. Protección de data y privacidad de la información

Política: El departamento de informática debe garantizar la continuidad de los procesos y los activos de la información.

Delimitar cuales son las posibles consecuencias en caso de violación a la integridad de la información, establecidos en la Ley.

Encaminada a: Departamento Informático

5.2.14.3. Cumpliendo con la legislación de protección de datos y activos equivalentes

Política: La Dirección Distrital, al ser una entidad gubernamental regidas por las leyes del estado esta normada por las Leyes del Estado Ecuatoriano, que garantiza y defiende la confidencialidad e integridad de la información.

Encaminada a: Departamento Jurídico

5.2.14.4. Cumplimiento con la ley general de derechos de autor

Política: La Dirección Distrital, al ser una entidad gubernamental regidas por las leyes del estado esta normada por las Leyes del Estado Ecuatoriano, garantiza el derecho de autor.

Encaminada a: Departamento Jurídico.

5.2.14.5. Legislación de protección contra el mal uso de los equipos de cómputo

Política: Se debe realizar a todos los empleados del distrito pruebas sobre el conocimiento de las normas y políticas de la

seguridad de la información. Luego de ello respaldar los conocimientos que se detectó que carecen.

Encaminada a: Departamento Jurídico.

5.2.14.6. Administrando los medios de almacenamiento y períodos de retención

Política: El Distrito de Educación garantiza el respaldo de la información a través de la nube de la red donde siempre está a la mano de todos los usuarios que lo requieren. Esto es de conocimiento general de todos los empleados.

Encaminada a: Departamento Informático.

5.2.14.7. Cumpliendo con las políticas de seguridad de información

Política: Dentro de las políticas y normas que garantizan los activos de la información estipula que los empleados externos del Distrito de Educación deben cumplir con ellas.

Encaminada a: Departamento Informático.

5.2.14.8. Uso de información y documentos relacionados a sistemas informáticos

Política: El Ministerio de Educación es el encargado de socializar cada uno de los manuales de usuarios de los sistemas informáticos incorporados y puestos en marcha. Por lo cual el Distrito no tiene competencia en realizar ninguna copia ya que esto violaría la ley.

Encaminada a: Departamento Informático.

5.2.14.9. Registro de evidencias de incidentes

Política: Toda vulnerabilidad o incidente debe estar registrado en la bitácora de sucesos, conjuntamente con el departamento de informática como con el usuario que lo detecto.

Encaminada a: Departamento Informático.

5.2.14.10. Renombrar dominio y sitios Web

Política: Es de conocimiento general que los sitios del Ministerio de Educación son únicos e irreproducibles.

Encaminada a: Departamento Informático.

CAPÍTULO 6

6. Análisis de Resultados.

6.1. Resultados de las acciones tomadas.

En la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, al poner en poner en práctica las políticas de Seguridad de Acceso a la Información, se ha visto que los Departamentos como los Administradores han ido tomado más conciencia de la importancia de la aplicación de las mismas, se ha visto reflejada en la acción más oportuna y evitado muchas pérdidas de información tanto digitales como físicas.

El desarrollo de actividades se han mejorado gracias a la implantación de políticas de control tanto para Usuarios como para el Departamento de Informática, se ha mantenido el

acceso y confiabilidad a los datos tanto a nivel de la Red como del funcionamiento de cada equipo.

6.2. Incidentes Reportados

Las políticas y directrices generales definidas en este documento son de cumplimiento obligatorio por cada una de las áreas de tecnología de la Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación y sus proveedores de servicios, como son las empresas encargadas del desarrollo, instalación, mantenimiento y actualización de los recursos de hardware y software correspondientes a los sistemas en ambiente de producción o en desarrollo.

Se deben identificar y revisar regularmente, los requerimientos de confidencialidad o los acuerdos de no divulgación, reflejando las necesidades de la Institución para la protección de sus activos. En donde al realizar la socialización y la puesta en marcha de las políticas no se han reportado incidentes o problemas en cuanto al manejo eficiente de los activos de la Información.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Al realizarla el estudio, levantamiento de información, generar y aplicar las políticas de Aseguramiento Del Entorno Informático La Dirección Distrital De Educación 03d01 Azogues-Biblián–Déleg-Educación, se ha visto que los procesos se llevan con mayor agilidad y rapidez, se informado al Distrito de los diferentes hallazgos encontrados, se han podido mitigar a través de políticas claras y fáciles de aplicar.
2. Dentro de los activos de la información se han definido medidas de contingencia para la estabilización y mantenimiento del entorno informático en la Dirección Distrital De Educación 03d01 Azogues-Biblián-Déleg-Educación.

3. Se ha logrado crear un cambio cultural en el ambiente en el departamento Informático, al aplicar políticas que afecten al personal, al uso de los recursos y a la forma de trabajo, además de una conciencia integral de la importancia de la seguridad del entorno informático y las implicaciones de las falencias en este tema, al establecer dentro del distrito las responsabilidades de los usuarios así como de los administradores.
4. A continuación se muestra un análisis estadístico, de cómo se han mejorado los proceso dentro del Distrito al incorporar políticas y normas claras para el manejo de los activos de la infamación:

Tabla 6: Estudio de los Riesgos Informáticos

RIESGOS INFORMÁTICOS		
Riesgo	**Sin políticas**	**Políticas Implementadas**
Inadecuado uso e instalación de software y hardware	70%	30%
Fallas en las telecomunicaciones y/o fluido eléctrico	85%	15%
Vulnerabilidad del sistema de información	90%	10%
Ausencia y/o deficiencia en los softwares y sistemas de información	75%	25%

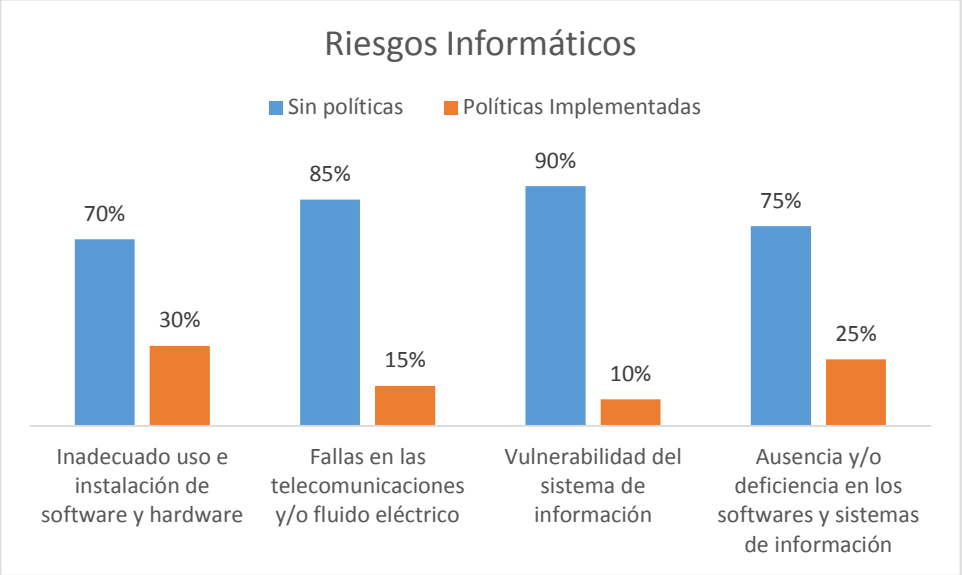


Figura 7.1: Riesgos Informáticos

En cuanto a los riesgos informáticos como se puede observar, al promover la implementación de políticas claras y estándares de manejo frente a ciertas amenazas se ha podido ir mitigando, como es el inadecuado uso e instalación de software y hardware al ser considerado como una actividad netamente de parte del encargado del departamento informático teniendo un 70% de incidencia antes de la implementación, bajando a un 30%. Al igual que el seguimiento de las fallas en las telecomunicaciones y/o flujo electico, es importante recalcar que se ha normado el uso adecuado de los recursos de la red por lo que se ha visto un índice de error del 15% frente a un 85%. En cuanto a la Ausencia y/o deficiencia en los softwares y sistemas de información se ha visto que el departamento informático ha dado el adecuado mantenimiento de los equipos y se ha tenido un especial

cuidado en la instalación de software dedicados a los usuarios según sus necesidades, por lo que se ve en los gráficos estadísticos que ha bajado la inconformidad a un 25% frente a un 75%.

Tabla 7: Estudio estadístico de los riesgos de los usuarios

RIESGOS DEL USUARIO		
RIESGO	**Sin políticas**	**Políticas Implementadas**
Daños, deterioro o pérdida de los recursos tecnológicos	90%	10%
Inadecuada utilización del QUIPUX	65%	35%
Uso indebido de la información	75%	25%
Accesos no autorizados a las instalaciones del área tecnológica	80%	20%

Sobre los riesgos de los usuarios presentamos los siguientes resultados

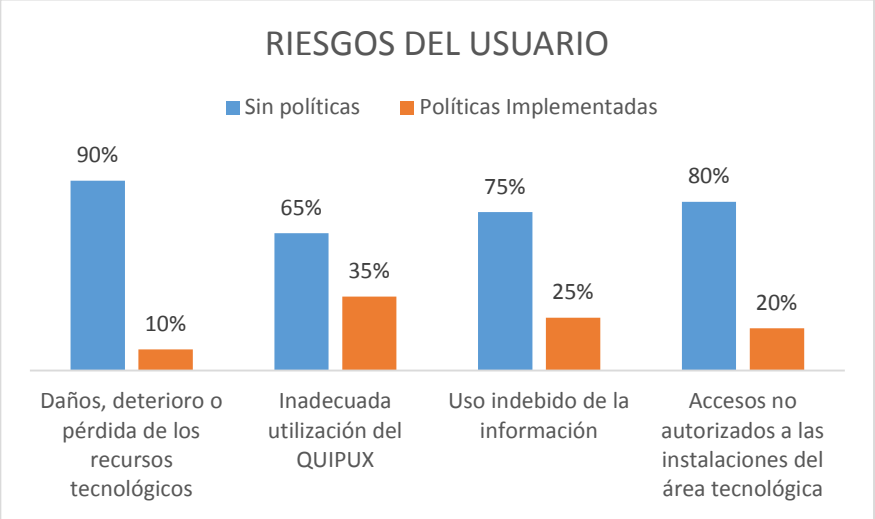


Figura 7.2: Riesgos del Usuario

La gráfica nos muestra que se está logrando mitigar el daño, deterioro o perdida de los recurso tecnológicos, ya que se ha definido los responsables, definiendo claramente sus políticas en cuanto al manejo eficiente y adecuado teniendo al inicio del estudio un 90% bajando a un 10%. En cuanto al uso inadecuado del sistema QUIPUX se ve que la mejora es considerable de un 65% a un 35%, pero no es la esperada debido a que los usuarios muestran un poco de apatía a los cambios en cuanto a los tiempos que este programa asigna por tarea. Como se puede observar en el gráfico se demuestra que existe mayor concienciación sobre el adecuado manejo de la información teniendo un 75% de incidencias antes del estudio frente a una mejora de un 25%. Sobre el acceso no autorizado a las instalaciones del área tecnológica se ha generado un gran cambio ya que se definido claramente que el encargado de este departamento es el único habilitado para realizar cualquier tipo de modificación, teniendo un 20% de incidencias frente a un

80%, la razón de no tener un reporte del 0% de incidencia es que mucha de las veces los encargados del departamento de informática, se encuentran habilitados en diferentes actividades fuera del distrito.

RECOMENDACIONES

Es importante mencionar que al ser, una entidad pública depende mucho de los recursos económicos que le asigne el Estado, por esto el análisis expuesto en el esquema de la matriz de riesgos, en cuanto a los problemas encontrados a nivel de red y de conexiones eléctricas, se debe a la ausencia de recursos lo cual impide intervenir en ellos, por lo que se solicitó que se trabaje únicamente en las políticas de aseguramiento de la información, donde no se necesiten gastos económicos. Por ello se recomienda al Distrito de Educación que gestionen los recursos necesarios para cambiar o mejorar totalmente sus instalaciones eléctricas y dar un buen mantenimiento a la red. Es importante continuar con la socialización y puesta en marcha por parte del Departamento de Informática, de las políticas de aseguramiento, para alcanzar a mitigar los riesgos detectados dentro de la institución. A demás de ello, es necesario realizar un análisis de las políticas a lo largo de su aplicación y determinar sus posibles mejoras y cambios que deban realizarse para que estén acorde a las nuevas necesidades detectadas.

5. Anexos

ENCUESTA SOBRE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

La siguiente encuesta va dirigida para obtener datos relevantes, sobre cómo se garantiza la seguridad Informática Tanto en Hardware como en Software dentro de la Dirección Distrital de Educación 03D01 Azogues – Biblián – Déleg – Educación, para realizar el plan de trabajo del "ASEGURAMIENTO DEL ENTORNO INFORMÁTICO EN LA DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DÉLEG-EDUCACIÓN. Dirigido al departamento Informático.

1. ¿Qué herramientas de seguridad usted reconoce para un aseguramiento Informático?

Firewall
Actualizaciones
Herramientas de autenticación de usuarios
Antivirus, Antispyware , Antimalware
Proxy
Herramientas de monitoreo de red
Políticas de seguridad
Ninguna

2. ¿Qué herramientas de seguridad usted usa en su entorno informático?

Herramientas de monitoreo de red
Antivirus, Antispyware , Antimalware
Actualizaciones
Herramientas de autenticación de usuarios
Proxy
Políticas de seguridad
Firewall
Ninguna

3. ¿Cuál sería el mecanismo eficiente para realizar el seguimiento de los equipos que forman parte de la red?

A través de una bitácora de control
Políticas de seguimiento y de seguridad en la red
Sistema automatizado
Inventario

4. ¿Qué tipo de políticas o normas de seguridad informática usted recomendaría aplicar?

Guías básicas enfocadas a estándares internacionales
Manejo de políticas de seguridad informática
Normativas internas

5. ¿Qué tipo de mecanismos usted recomendaría para poder evaluar políticas o normas de seguridad?

- Evaluación por parte del personal interno calificado
- No existen ningún tipo de sistemas de evaluación
- A través de algún tipo de aplicativo adaptado o enfocado a este fin
- Otro (por favor, especifique)

6. ¿Cómo usted recomienda llevar el proceso de control de los mecanismos de seguridad Informática?

- La labor es destinada al personal interno de la organización
- A través de políticas claras y realizadas en base a nuestras necesidades.
- No es necesario ningún tipo de control

7. ¿Cómo recomendaría usted poder validar y evaluar el rubro de la seguridad informática?

- Manualmente, y registrado a través de bitácoras en papel.
- A través de un sistema ligero creado por la empresa
- Con políticas claras tanto a nivel de seguridad Física como Lógica de los Sistemas informáticos.

8. ¿Usted considera importante el efecto que puede producir las políticas de administración de seguridades informáticas sobre el rendimiento de los recursos Informáticos?

- No importa el aspecto del rendimiento
- Depende del requerimiento de los usuarios
- Que el efecto sobre el rendimiento del sistema en general deba ser mediano
- Que el efecto sobre el rendimiento del sistema en general debe ser mínimo

9. ¿Cómo usted recomendaría poder verificar los resultados luego de un proceso de evaluación de la seguridad en los procesos Informáticos?

- No es necesario la emisión de un reporte, con los datos visualizados en tiempo real es suficiente
- A través de un reporte escrito
- A través de un reporte con ayuda de gráficos estadísticos emitido por la herramienta de administración digital
- A través de un reporte emitido por las políticas de administración de seguridad establecidas para la institución.

10. ¿Cómo usted recomendaría la elaboración de un manual de administración de seguridad informática?

- Muy detallado pero que se presente de una manera amigable al usuario sin la presencia de muchos tecnicismos
- Muy detallado, manejado a nivel muy técnico el análisis de la herramienta, y enfocado solo a personal operativo
- Manejado de una manera muy simple, sin profundizar mucho y con la ayuda de gráficos explicativos.
- Manejado de tal manera que se haga uso de un análisis simple, detallado y con una gran presencia de gráficos e imágenes de ayuda

11. ¿Hacia qué personal usted recomienda que deba ir enfocado el manual de uso de la herramienta de administración de seguridad informática?

- Exclusivamente a personal técnico y operativo del departamento de sistemas de la organización
- Manejado exclusivamente solo por aquella(s) persona(s) que operaran el aplicativo
- Enfocado al personal técnico, al operativo y también al personal administrativo del departamento o de la organización.

12. ¿Una vez detectadas cuales son las políticas de seguridad Informática que deben ser implementadas en la institución, usted recomendaría dar algún tipo de asesoría o capacitación junto con el manual de uso, de cómo funciona la herramienta de administración de seguridad informática?

- Si se recomienda dar dicha capacitación

- No es necesario recibir la capacitación, con el manual de uso de la herramienta es suficiente
- Se recomienda algún tipo de asesoría dada de manera personalizada a la(s) persona(s) que operaran el aplicativo
- Otro (por favor, especifique)

Gracias por su tiempo

ENCUESTA SOBRE LA SEGURIDAD INFORMÁTICA

La siguiente encuesta va dirigida para obtener datos relevantes, sobre cómo se garantiza la seguridad Informática Tanto en Hardware como en Software dentro de la Dirección Distrital de Educación 03D01 Azogues – Biblián – Déleg – Educación, para realizar el plan de trabajo del "ASEGURAMIENTO DEL ENTORNO INFORMÁTICO EN LA DIRECCIÓN DISTRITAL DE EDUCACIÓN 03D01 AZOGUES-BIBLIAN-DÉLEG-EDUCACIÓN. Dirigido al Usuario.

1. Existe personal de seguridad en la institución?

Si ____ No__

2. Usted como usuario, reporta daños en sistema al personal de Informática.

Si ____ No__

3. Usted en su equipo como mecanismo de seguridad tiene una clave de acceso.

Si ____ No__

4. El Edificio donde se encuentra la computadora está a salvo de :

Fuego ( )

Sabotaje( )

Inundaciones( )

Terremotos ( )

5. El centro de cómputo tiene salida al exterior
Si ____ No__
6. Existe un mecanismo de seguridad en la Institución:
Si ____ No__
Indique cuál _____
7. Existe extintores de fuego dentro de la institución
Si ____ No__
8. ¿Los interruptores de energía están debidamente protegidos, etiquetados sin obstáculos para alcanzarlos?
Si ____ No__
9. Su equipo tiene está conectado a un regulador de voltaje.
Si ____ No__
10. La Institución cuenta con políticas de seguridad Informática en cuanto al manejo de la información.
Si ____ No__
11. ¿Se ha adiestrado al personal sobre políticas de un buen manejo de la tecnología dentro de la institución?
Si ____ No__
12. ¿Cuándo se efectúa modificaciones en los equipos informáticos, a iniciativa de quién es?
Departamento Informático ( )
Particulares ( )
Usuario ( )
Otros por favor especifique_____
13. ¿Cuándo necesita algún tipo de mantenimiento su equipo informático lo hace de manera?
Oral ( ) Escrita ( )

14.¿El uso del Internet que Usted posee le restringe el ingreso a redes sociales como Facebook, correos electrónicos personales, etc.?
Si _____ No ____

15. ¿Cuál es el mecanismo de mensajería, en cuanto al manejo de la información usa
Quipux( )
Mensajería electrónica Gratuita (Gmail , Hotmail, Yahoo, etc.) ( )
Todo se lleva en forma impresa y registrada.( )

16. La conexión a la rede es vía
Inalámbrica ( )
Con cable( )

17.Tiene acceso libre al internet?

Si ( ) No( )

18.Existe alguna política en caso de que la conexión a internet se corte o sea deficiente en su velocidad.
Si _____ No ____

19.¿La institución cuenta con algún tipo de respaldo de la información en caso de que su equipo informático se dañe?
Si _____ No ____

20. ¿Existe control de los equipos informáticos cuando estos son sacados fuera de la institución?
Si _____ No ____

Indique
cuál_____

21. ¿Existe controles y medidas de seguridad sobre las siguientes operaciones?
( ) Archivos guardados en dispositivos de Almacenamiento masivo
( ) Operaciones del equipo de computación.
( ) En cuanto al acceso de personal
( ) Identificación del personal
( ) Políticas claras sobre el uso de los equipos informáticos y el acceso a la red
( ) Seguro contra robos e incendios
( ) Recepción de documentos
( ) Información Confidencial
( ) Captación de documentos
( ) Instalación de Programas.
( ) Documentos de Salida
( ) Otros por favor
especifique_____

Gracias por su tiempo

BIBLIOGRAFÍA

[1] Definicion. de (2008-2015) Seguridad Concepto; http://definicion.de/seguridad/

[2] Actualidad Tecnológica (2009). Control Interno y Auditoria Informática; http://tecno-actualidad.blogspot.com/2010/02/control-interno-y-auditoria-informatica.html

[3] © 2015 Unidad Editorial Información Económica S.L. Expansión; Pilar Yubero Hermosa 2015, Activo, http://www.expansion.com/diccionario-economico/activo.html

[4] Información Activo valioso para las empresas; Gabriel Alejandro Granados http://www.visionindustrial.com.mx/industria/desarrollo-industrial/informacion-activo-valioso-para-las-empresas.html

[5] ISO (International Standard Organization). “Estándar de Seguridad ISO 17799”

[6] ISO (International Standard Organization). “Estándar de Seguridad ISO 27002”

[7] ISO (International Standard Organization). “The Common Criteria for Information Technology Security Evaluation” v2.1

[8] Ministerio de Educación del Ecuador sobre las atribuciones y responsabilidades de las Direcciones Distritales, 23/07/2013 http://educacion.gob.ec/wp-content/uploads/downloads/2013/07/Atribuciones_y_responsabilidades_de_los_140_Directores_Distritales_de_Educacion.pdf