UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LAS COMPUTADORAS DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UTMACH

GUAMAN POMA CINDY ABIGAIL
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LAS COMPUTADORAS DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UTMACH

GUAMAN POMA CINDY ABIGAIL
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LAS COMPUTADORAS DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UTMACH

GUAMAN POMA CINDY ABIGAIL
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 26 DE AGOSTO DE 2019

MACHALA
26 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LAS COMPUTADORAS DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UTMACH, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: lunes 26 de agosto de 2019 - 12:58

URKUND

Urkund Analysis Result

Analysed Document:	CINDY GUAMAN.docx (D54764205)
Submitted:	8/10/2019 7:36:00 AM
Submitted By:	jgonzalez@utmachala.edu.ec
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, GUAMAN POMA CINDY ABIGAIL, en calidad de autora del siguiente trabajo escrito titulado AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LAS COMPUTADORAS DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UTMACH, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

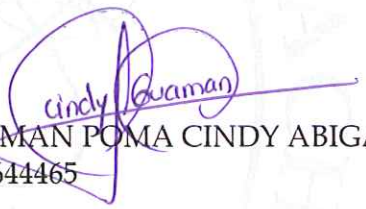
La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 26 de agosto de 2019



GUAMAN POMA CINDY ABIGAIL
0706644465

RESUMEN

La auditoría en los sistemas informáticos es una ciencia intrínseca en toda organización, permite analizar todos los aspectos relevantes referentes a automatización, solventar servicios, seguridad, protección, gestión y gobierno tanto de recursos tangibles como intangibles. La Universidad Técnica de Machala al ser una entidad de educación superior, debe maniobrar inmensas cantidades de datos, hacer fluir en forma holística una serie de procesos, tareas, servicios e implementos para ejercer sus funciones cotidianas dentro de la sociedad; su estructura compuesta por unidades académicas, departamentos, autoridades, consejos, unidades como la de bienestar estudiantil y centro de educación continua (C.E.C) que se encarga de organizar cursos, instituto de idiomas, capacitaciones, publicidad, convenios estratégicos, entre otras mociones para mantener la actualidad en conocimientos de todos los involucrados en su ámbito corporativo. Este caso de estudio comprende la descripción y explicación de todas las medidas que acata el C.E.C para mantener niveles de seguridad/protección aceptable en sus ordenadores, siendo abordada desde una perspectiva abductiva de carácter exploratorio y pragmático, a fin de proponer mejoras e inferencias favorables al desempeño del área analizada.

Palabras Clave: Auditoría informática, controles, centro de cómputo, educación.

ABSTRACT

The audit in the computer systems is an intrinsic science in every organization, it allows to analyze all the relevant aspects related to automation, solve services, security, protection, management and governance of both tangible and intangible resources. The Universidad Técnica de Machala, being an entity of higher education, must maneuver immense amounts of data, make a series of processes, tasks, services and implements flow in a holistic manner to exercise its daily functions within society; its structure composed of academic units, departments, authorities, councils, units such as the student welfare center and continuing education center (C.E.C) that is responsible for organizing courses, language institute, training, advertising, strategic agreements, among other motions to maintain the current knowledge of all those involved in their corporate environment. This case study includes the description and explanation of all the measures that the C.E.C abides to maintain levels of security / acceptable protection in their computers, being approached from an abductive perspective of an exploratory and pragmatic nature in order to propose improvements and favorable inferences to the performance of the area analyzed.

Keywords: Computer audit, controls, computer center, education.

ÍNDICE DE CONTENIDOS

ÍNDICE DE CUADROS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

El uso de las Tecnologías de comunicación e información ha transformado todos los aspectos relevantes de la sociedad, desde la educación hasta la competitividad empresarial; gracias a la prestación/alquiler de bondades como accesibilidad, manejo, versatilidad e integridad de datos gestado en sistemas computacionales; sin embargo, en nuestro país que no produce ni administra dichas potencialidades, es imperioso analizar los riesgos, desventajas o consecuencias adversas en especial para la seguridad personal y organizacional (CARVAJAL, 2018).

La auditoría informática es verificar, evaluar, revisar en el desempeño de todos los sistemas de información de una organización, con el objeto de mejorar su rendimiento, seguridad, e integrar controles para interactuar eficientemente con su entorno a la par de sus fortalezas y debilidades (Arcentales Fernández & Caycedo Casas, 2017).Los principios de este proceso son:

- Evaluar los sistemas, procedimientos, programas y activos en la red.
- Proponer mejoras para equilibrar vulnerabilidades vs controles de seguridad.
- Mantener la integridad de los datos.
- Automatizar procesos secuenciales, manuales u ofimáticos.
- Realizar un diagnóstico del estado del sistema en su totalidad.
- Informar mediante reportes todas las anormalidades detectadas.
- Analizar los flujos de procesos, flujos monetarios, uso de equipos u ordenadores.
- Gestar en forma interdisciplinaria políticas de seguridad digital (Lsi. María Elena Guevara Toscano, Ing. Tanya Magaly Recalde Chiluiza, Ing. Jennifer Alexis Avilés Monroy, & Balarezo, 2018).

El presente estudio pretende auditar en forma exploratoria y cognitiva al centro de cómputo del Centro de Educación Continua, para describir el estado de seguridad en sus sistemas, explicar qué medidas aplican al gestionar la integridad de sus datos, cuales percances se han detectado, cómo han respondido ante ellos; además se aplica el método analítico sintético, observación mediante una investigación documentada y entrevista al personal para dirimir los criterios necesarios en el caso propuesto.

1. FUNDAMENTACIÓN TEÓRICA

Es relevante en toda indagación, sustentar las opiniones a través de investigaciones similares, que cuenten con el rigor académico necesario al argumentar la perspectiva del autor, al explicar los conceptos o terminologías referente a la temática abordada.

1.1 Centro de Educación Continua

Es una dependencia administrativa, encargada de gestionar la oferta de cursos, congresos, capacitaciones, conferencias, seminarios u otros medios destinados a satisfacer las necesidades en conocimientos y requerimientos de la sociedad en general; dentro de sus responsabilidades se tiene:

- Elaborar cursos, capacitaciones, talleres, entre otros, de educación continua presencial, sean estos de las modalidades presencial, semipresencial y a distancia.
- Ejecutar el Plan Anual de Educación Continua, las cuales serán aprobadas por el Consejo Universitario.
- Administrar el Instituto de Idiomas de la Universidad Técnica de Machala.
- Ofertas y demandas de investigación y estudios sobre capacitación profesional en nivel básico, medio y avanzado.
- Conservar un registro actual sobre la participación en capacitación continua de estudiantes, profesionales, etc.
- Mantener un registro actual de capacitadores de los programas elaborados.
- En general todos los que se encuentran en conformidad con la Ley Orgánica de Educación Superior, Reglamentos Generales e internos, además del presente estatuto (UTMACH, 2017).

Ilustración 1. Sitio web del Centro de Educación Continua UTMACH
Fuente: (UTMACH, 2017).

1.2 Seguridad de sistemas

Es un proceso continuo que garantiza la operación de todos los activos informáticos a un costo rentable para la organización, mantiene a un margen aceptable los riesgos y efectúa políticas, controles, e integra metodologías enfocadas a salvaguardar la calidad de los datos, correcto desempeño computaciones y evitar daños a la infraestructura digital (Quiroz-Zambrano, 2017).

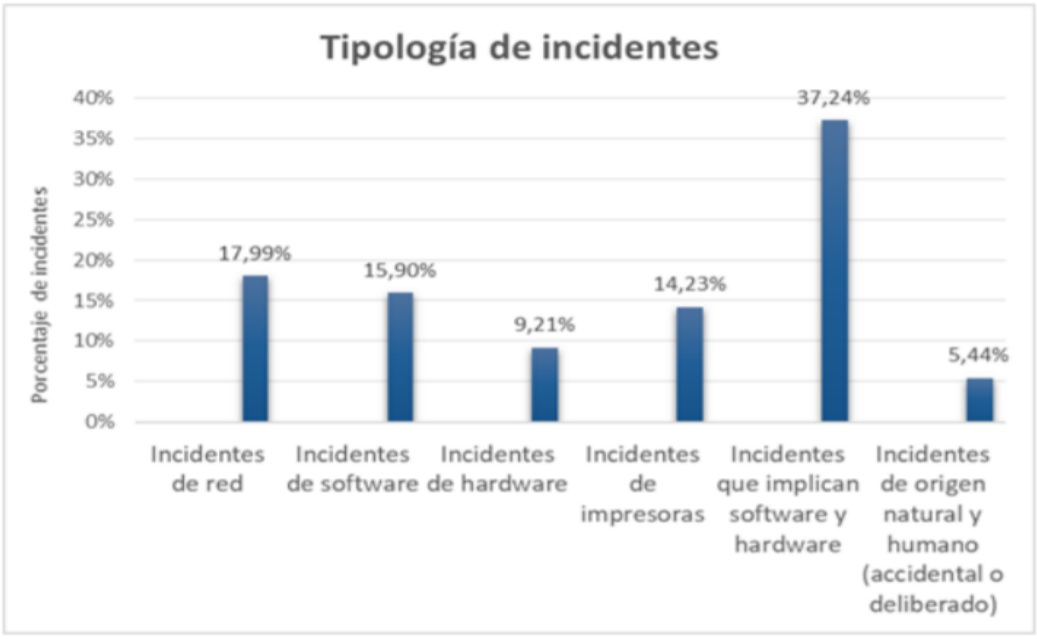


Ilustración 2. Incidentes informáticos más comunes en Universidades
Fuente: (Romero, Anchundia, & Loor, 2018)

1.3 Auditoria Informática

La auditoría como tal es un proceso complejo y de carácter continuo, que tiene por objeto monitorear, evaluar, retroalimentar e implementar medidas proactivas en favor de incrementar las potencialidades de la institución; su alcance es sistemático comprendiendo todos los aspectos de la organización, analiza toda tarea u operación relacionada a los activos informáticos sin importar si son tangibles e intangibles; una diferencia es su filosofía de mejora constante como medio para alcanzar la competitividad y desarrollo, gestado a través de medios computacionales armonizando riesgos/costos/beneficios (Montaño, 2016).

1.4 Vulnerabilidades

En un sistema digital son todas las debilidades desatendidas que producen aberturas, en las cuales una amenaza efectúa acciones dañinas a los activos del entorno; generalmente

son las falencias latentes en los requisitos del usuario y del sistema, debido a que su convergencia facilita irregularidades como:

- Inyección SQL, configuración incorrecta
- Conexión insegura, certificados web vulnerables
- Pérdida, robo o hurto de datos, edición/alteración de información
- Secuestro de sesiones, entidades externas XML y hackeos (Benitez & Nemury, 2018)

1.5 Amenazas

Son la presencia de factores adversos a la seguridad, derivados de las vulnerabilidades y falta de respuesta en las organizaciones; en los sistemas informáticos a nivel nacional las mayores amenazas son la falta de *auditoría a entidades públicas*, poca designación de presupuesto para actualizar/alquilar activos digitales de vanguardia, *falta de cultura en protección de datos*; es decir la población no toma conciencia en resguardar su información personal ni respaldar adecuadamente sus datos en los medios computacionales; tampoco se compra licencias ni paga a personal especializado en *medias de control* para garantizar la solvencia de las redes e implementos lógicos tan apreciados en toda institución, particularmente en las universidades por su responsabilidad social en pertinencia científica y epistemológica (Anchundia-Betancourt, 2017).

1.6 Controles en sistemas computacionales

Comprenden todas las medidas e implementaciones de seguridad física y lógica, para mantener los activos digitales seguros, minimizar riesgos o afectaciones graves al sistema, también son el conjunto de medios para regular el comportamiento del personal, respaldar datos y gestionar en forma correcta la información sin comprometer su integridad o accesibilidad (Calero Ordoñez , 2019); los más destacados en centros computacionales son:

- Cámaras de seguridad.
- Dispositivos biométricos para marcar e identificar personal.
- Gestión de privilegios y responsabilidades en el sistema.
- Contraseñas fuertes y cifrado de claves.
- Respaldo de información en medios físicos o virtuales.
- Antivirus, cortafuegos, software de escaneo de archivos.
- Configuraciones de redes e internet.
- Software para escaneo, monitoreo, visualización de tráfico en red.
- Puertos de servidores y certificados de seguridad.
- Políticas internas o sanciones disciplinarias en la institución.

2. METODOLOGÍA

En esta sección se destacan las técnicas implementadas al recopilar, procesar e interpretar conocimientos con la finalidad de demostrar científicamente la veracidad de las apreciaciones expuestas en este texto.

2.1 Investigación Documentada:

Consiste en compilar información sobre el tema, revisar datos e inferencias en forma hermenéutica dentro de publicaciones indexadas o artículos que faciliten explicar la estructura del proyecto con simplicidad, concisión y claridad (González, 2017).

2.2 Analítico Sintético:

Es un proceso sistemático que integra dialécticamente al todo investigado; mediante el análisis descompone el objeto de estudio para contrastar las relaciones entre variables, deducir sus implicaciones y luego sintetizar las partes para obtener una visión clara del entorno, tanto en forma contextual como puntual al explicar las inferencias denotadas en forma organizada e interdisciplinaria en lo referente al C.E.C de la UTMACH (Jiménez & Jacinto, 2017).

2.3 Observación:

Es un proceso ampliamente usado tanto en análisis cualitativos como cuantitativos, gracias a que permite abstraer de la realidad las características de un objeto estudiado; utiliza los sentidos como medio principal para extraer datos, deducir el comportamiento e inferir relaciones del entorno en forma de apreciaciones que luego se concatenan en forma lógica y holística (Risso, 2017).

3. DESARROLLO

En este apartado se resumen los hallazgos, valoraciones, consideraciones e implementación de medidas afines a la auditoría de sistemas realizada al Centro de Educación Continua, cuya función es servir de nexo entre capacitaciones constantes y todos los involucrados con la UTMACH tanto a nivel local como provincial.

En el *cuadro 1* se resumen los resultados de la auditoría, en general el nivel de seguridad es *aceptable* gracias a que su fortaleza es el recurso humano, confiabilidad, pericia y asistencia por medios computacionales bajo una política de calidad que empodera a toda la dependencia analizada.

Cuadro 1. Controles en respuesta a vulnerabilidades en el C.E.C

Vulnerabilidades	Controles Físicos	Controles Lógicos
Pérdida o robo de datos	Guardado en unidades externas	Respaldos virtuales online
Conducta del personal	Identificación biométrica, políticas de seguridad, sanciones	Privilegios en el sistema, directrices de la dirección de TIC`s
Malware o virus	Revisión de ordenadores	Antivirus NOD 32
Ataques o hackers	Personal profesional en seguridad de sistemas	Cortafuegos, configuraciones de redes y monitoreo del estado en las plataformas virtuales
Fallos en programación o configuraciones de equipos/software	Auditorías regulares, responsabilidades de la Dirección de TIC`s	Compilación de códigos fuente, revisión y análisis de los sitios web/Siutmach/servicios
Ordenadores, recursos y activos físicos	Guardado bajo llave, cámaras de vigilancia y guardián	Inventarios, registro de usuarios, documentos de los equipos

Fuente: Elaboración Propia

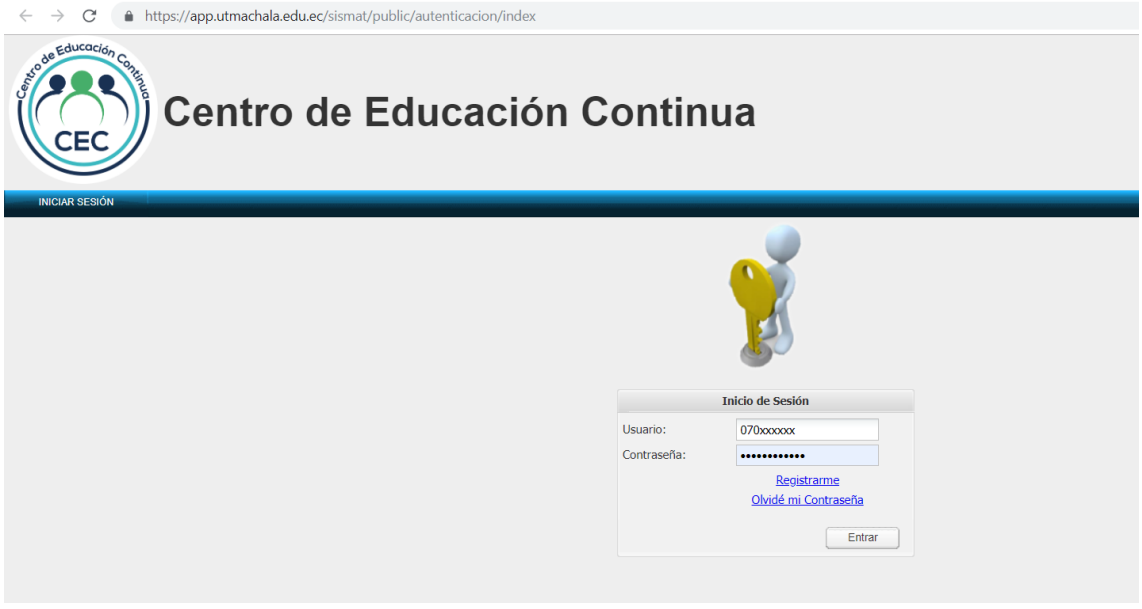


Ilustración 3. Plataforma para el usuario del C.E.C (SISMAT)
Fuente: (Universidad Tècnica de Machala, 2015)

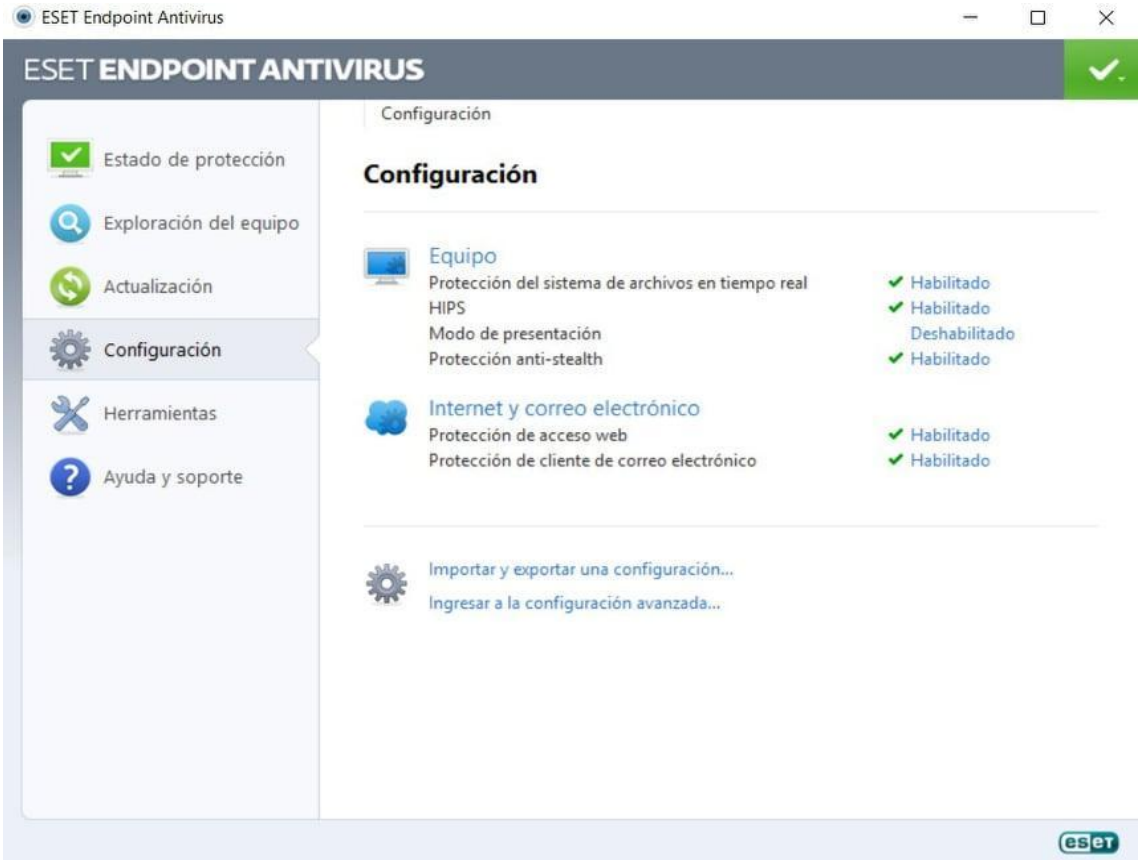


Ilustración 4. Configuración de Antivirus en los ordenadores
Fuente: Elaboración Propia

En forma holística se imponen las consideraciones de la Dirección de TIC`s por ser el organismo interno designado para velar por la seguridad informática, gestión de recursos digitales y auditoría de los sistemas; sus políticas principales son:

- La correcta administración del correo institucional, contraseña, mensajería, uso corporativo recae directamente sobre el usuario de forma exclusiva.
- El ordenador es de competencia inherente a las labores institucionales, instalar o alterar su configuración por software no está permitido, debe ser notificado cualquier percance a los superiores inmediatos.
- Es responsabilidad del personal, gestionar la seguridad en su área de trabajo, realizar informes regulares e implementar las políticas citadas en el presente texto.
- Las contraseñas deben ser fuertes, cambiadas periódicamente, no darse a terceros ni ser ingresadas o anotadas en forma imprudente.
- Las copias/respaldos son responsabilidad de la dirección de TIC`s, sus mecanismos, revisión, almacenado en servidores virtuales y espacios físicos seguros.

- Los acuerdos de confidencialidad regulan el comportamiento y buen uso de información institucional al abandonar la UTMACH bajo respeto mutuo en orden legal (Universidad Técnica de Machala, 2015)

3.1 Análisis en respuesta a eventualidades.

Es relevante la organización, al responder oportunamente ante cualquier hecho o acto mal intencionado, entrevistando al personal del C.E.C las secretarias y encargadas del sistema se destacan los siguientes acontecimientos:

Se han registrado dos intentos de ataques, uno fue en la Unidad Académica de Ingeniería Civil que supuestos hacker cobraban dinero para mejorar las notas, pasar supletorios e incluso alterar las actas en el SIUTMACH; no obstante, pese a ser una novedad entre estudiantes el rector político informe de auditoría a la dirección de Tics, quienes verificaron no se realizó ninguna alteración ni se violó la seguridad del sistema.

En cierta ocasión se notificó la alteración de matrículas en el Instituto de Idiomas, por parte de los administradores, sin embargo, las encargadas evidenciaron no ser las responsables; pese a cambiar la contraseña y revisar los privilegios de usuario no se pudo identificar al culpable, tampoco hubo acciones significativas.

En ambos casos no se produjeron daños relevantes; pero se demostró que se cuenta con la destreza para responder en forma temprana; esto abre un historial ante los posibles ataques haciendo imperiosa la necesidad de mantener un perímetro seguro, ejercer las políticas de seguridad con rigurosidad y la permanente auditoría para detectar falencias o instrucciones al sistema.

4. CONCLUSIONES Y RECOMENDACIONES

- La seguridad informática e información en el C.E.C es alta, gracias a que posee un riguroso control al personal, activos digitales, servicios web y constante monitoreo a escala para garantizar un desempeño óptimo sin imprevistos o falencias inesperadas.

- La auditoría informática también abarca los flujos monetarios, debido al costo de la seguridad, como licencias, pago a profesionales, mantenimiento de redes e internet, aconsejando que sean incluidas en el presupuesto anual.

- Se reveló que existen intentos de vulnerar la información, abriendo un registro de los peligros latentes en el contexto de la UTMACH, por lo tanto, mantenerse alerta e implementar mejoras robustas en la seguridad del sistema, puede garantizar la protección de los datos que gestionan las operaciones sociales del C.E.C.
- Uno de los factores más intrigantes en la seguridad informática es la conducta humana, debido a descuidos o desatenciones que pasan desapercibidas pueden desencadenar actos nocivos, dando oportunidades para el ingreso de amenazas pese a todos los controles lógicos existentes; por ende, también se concluye que imponer una cultura en seguridad a través del empoderamiento institucional es tan importante como implementar tecnologías de vanguardia en protección virtual.

5. REFERENCIAS BIBLIOGRÀFICAS

Anchundia-Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias Vol. 3*, 200-217.

Arcentales Fernández, D., & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias Vol. 3*, 157-173.

Benitez, Y. N., & N. S. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas, Vol. 12*, 205-221.

Calero Ordoñez , C. I. (2019). *IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN SITIOS WEB CONTRA ATAQUES INFORMÁTICOS.* Machala: UTMACH-UNIDAD ACADÉMICA DE INGENIERÍA CIVIL.

CARVAJAL, E. T. (2018). Tecnologías, seguridad informática y derechos humanos. *IUS ET SCIENTIA (ISSN: 2444-8478), Vol.4, nº 1*, 19-39.

González, N. L. (2017). Algunas nociones y aplicaciones de la investigación documental denominada estado del arte. *INVESTIGACIÓN BIBLIOTECOLÓGICA, Vol. 31, Núm. 73*, 237-263.

Jiménez, A. R., & Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista EAN, No 82*, 179-200.

Lsi. María Elena Guevara Toscano, M., Ing. Tanya Magaly Recalde Chiluiza, M., Ing. Jennifer Alexis Avilés Monroy, M., & Balarezo, I. L. (2018). Importancia de realizar auditoria de sistemas preventiva en las Organizaciones. *Espirales revista multidisciplinaria de investigación*, 25-38.

Montaño, M. F. (2016). Nuevas tendencias en auditoría: análisis de datos y aseguramiento continuò. *Fides Et Ratio - Volumen 12,* , 193-208.

Quiroz-Zambrano, S. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, Vol. 3, núm. 4*, 137-156.

Risso, V. G. (2017). Estudio de los métodos de investigación y técnicas de recolección de datos utilizadas en bibliotecología y ciencia de la información. *Revista Española de Documentación Científica, Vol. 40, No 2*, 1-13.

Romero, M. G., Anchundia, R. E., & Loor, E. S. (2018). Plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM MFL. *Revista de las tecnologìas de la Informàtica y las Telecomunicaciones; Vol. 2, No. 1*, 24-30.

Universidad Tècnica de Machala. (2015). *Centro de Educaciòn Continua*. Obtenido de SISMAT: https://app.utmachala.edu.ec/sismat/public/autenticacion/index

Universidad Tècnica de Machala. (2015). *POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION.* Machala: Secretaria General de la UTMACH.

UTMACH. (2017). *C.E.C-UTMACH*. Obtenido de Centro de educaciòn continua: http://cec.utmachala.edu.ec/