UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ABRIL 2022 – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

SISTEMA DE INFORMACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÒN

TEMA:

ANÁLISIS DE RIESGO QUE PRESENTAN LOS CORREOS INSTITUCIONALES EN EL DISTRITO DE SALUD 12D02 PUEBLOVIEJO-URDANETA.

ESTUDIANTE:

JONATHAN PATRICIO VILLAMAR SÁNCHEZ

TUTOR:

ING. FABIAN ALCOSER CANTUÑA

AÑO 2022

Resumen

El presente estudio de caso denominado análisis de riesgo que presentan los correos institucionales en el distrito de salud 12D02 “Puebloviejo-Urdaneta”, del 2022. Aplica es análisis a los correos institucionales en el programa Systools Simplifying Technology, este programa cuenta con un sin número de herramientas que nos ayudará a realizar el correcto análisis a los correos institucionales de la institución mencionada, esto nos permitirá saber si es seguro abrir un mensaje de correo electrónico, como ya sabes robar la información que contiene una empresa es un delito muy grave, ya que esta información puede poner en peligro a las personas e incluso a la misma institución, la manera de hurtar los datos de las empres se pueden hacer de varias maneras ya sea de forma física y de forma digital, la forma más sencilla es de manera digital mediante los correos electrónicos existen un sinnúmero de métodos por los cuales se pueden hurtan los datos, esto son phishing, publicidad engañosa, malware, ingeniería social, los ataques mencionados los hackers se hacen pasar por empresas importantes estas pueden ser ofertas de trabajos o con supuestas encuestas, un ejemplo claro es la publicidad engañosa en ella te salen anuncios falsos donde te dicen que te has ganado un celular último modelo o un vehículo 0 kilómetros, las personas que laboran en empresa o cualquier personas natural tiene que saber identificar cuáles son cada uno de ellos y así no poner en riesgo la integridad de ella ni la de la empresa, y así no ser una más de las personas que son estafadas en las redes sociales.

PALABRAS CLAVES: Phishing, Malware, Correo Electrónico, Ingeniería Social, Spam, Análisis de Riesgo.

Contenido

Planteamiento del problema 4
Justificación 6
Objetivos del estudio 8
Líneas de investigación 9
Marco conceptual 10
Marco metodológico 31
Resultados 33
Discusión de resultados ..... **¡Error! Marcador no definido.**
Conclusiones 39
Recomendaciones 40
Referencias 41
Anexos 42

Planteamiento del problema

Desde sus inicios el correo electrónico se volvió muy útil para las personas que se ejercen en el ámbito laboral o tienen familiares que viven en otras ciudades o en otros países, de esta forma nos permitió comunicarnos de manera directa con nuestros parientes. Nos encontramos en una era denominada la era de la información, gracias a la llegada del internet y nuevas tecnologías, la comunicación es muchísimo más fácil de como lo era antes, con más medios de comunicación masiva que nos permite estar conectados con los demás e informados del acontecer mundial.

La finalidad de la seguridad en los correos electrónicos es fundamental para evitar daños sea esta por el mal uso de los datos de la información. Actualmente existe una serie de causas o dudas potenciales que pueden ocurrir en los correos electrónicos debido a que no cuentan todas las compañías con la compra de un software que verifique los posibles datos maliciosos que puedan tener los correos electrónicos. Todas las compañías sean estas públicas o privadas deberán mantener información crítica y reservada en la que no tenga acceso los competidores o personas naturales.

El Distrito de Salud 12D02 Puebloviejo-Urdaneta siendo la institución de objeto de estudio para el presente desarrollo de caso se encuentra ubicado en el "Cantón Urdaneta" provincia de los Ríos. Teniendo en cuenta que forma parte de la cartera Estado que se encarga de planificar, coordinar, controlar y evaluar la implementación de la política pública sectorial y gestión del territorio de su competencia, actualmente está bajo la administración de la Dra. Maruixi Leonor Aguirre Zambrano.

Para la ejecución de este estudio de caso con respecto al análisis de riesgo que presentan los correos institucionales, se observó que la institución podría sufrir ataques o violación en lo que respecta a información interna. Distrito de Salud 12D02 Puebloviejo-Urdaneta posee actualmente correos institucionales o canales de comunicación que permiten

comunicarse con los otros distritos de salud, la información que posee es valiosa y esta es propiedad de la institución de salud. Considerando como un factor crítico la seguridad y la confidencialidad para proteger la información importante de la institución pública, debido a que los correos no solo informan a los usuarios, sino que también guardar la información que se maneja dentro de ella.

Justificación

En la actualidad la información juega un rol importante siendo uno de los activos primordial de mayor relevancia para toda institución, no obstante, es uno de los recursos mayor exposición a vulnerabilidades teniendo la necesidad de proteger y salvaguardar este valioso activo de amenazas y demás problemáticas que puedan existir tanto internas y externas. Hoy en día las empresas necesitan que la información y demás datos que se manejan esté siempre en absoluta reserva, integra sin que sufran algún tipo de alteraciones en sus datos y estas sean confiable en su procesamiento.

Es de suma importancia tener un amplio conocimiento en lo que respecta a las vulnerabilidades en los correos electrónicos, incluyendo todos sus componentes y demás información necesaria para su adecuado manejo, y desde luego se tiene que tener el conocimiento necesario para poder controlar los accesos a los correos electrónicos de la institución, llevando así un análisis exhaustivo de los problemas de vulnerabilidad en los correos electrónicos para poder tomar decisiones certeras y precisas.

Para el Distrito de Salud 12D02 Puebloviejo-Urdaneta siendo una institución de carácter pública que ofrece servicios a la ciudadanía en general, en su parte interna gestiona y administra información privada y con total confidencialidad con lo que respecta a sus labores o actividades que ejecutan, por ende, es adecuado realizar un análisis de riesgo que presentan los correos institucionales para su buen funcionamiento, y disponibilidad de la misma.

El análisis de riesgo en los correos electrónicos ayudara a conocer si existen algún tipo de riesgo en los correos electrónicos, para que exista acciones preventivas dentro de la institución, para evitar que se exponga en divulgación datos confidenciales. Una vez expuesto los problemas que presentan los correos electrónicos en la institución se procederá a realizar un análisis de riesgos que ocurre con los correos, mediante el

programa llamado “Systools Simplifying Technology” este programa nos ayudara a comprobar si existen algún riesgo o amenazas en los correos de la institución.

Objetivos del estudio

Objetivo general

- Realizar un análisis de riesgo a los correos institucionales del Distrito de Salud 12D02 Puebloviejo-Urdaneta con el programa Systools Simplifying Technology.

Objetivos específicos

- Examinar el problema actual que presentan los correos institucionales del Distrito de Salud 12D02 Puebloviejo-Urdaneta.
- Proporcionar lineamientos con respecto a la seguridad para de esta manera garantizar la confidencialidad, disponibilidad e integridad de la información del Distrito de Salud 12D02 Puebloviejo-Urdaneta.
- Emplear bibliográficamente estudios relacionados a distintos tipos de ataques a correos institucionales.

Líneas de investigación

El presente estudio de caso se enmarca en la línea de investigación “Sistemas de información y comunicación, emprendimiento e innovación”, con su respectiva sub línea de investigación que es redes y tecnologías inteligentes de software y hardware.

Esta línea y sub línea de investigación tiene una correlación con la variable independiente sistema de información y la variable dependiente del análisis de riesgo que presentan los correos institucionales en el distrito de salud 12d02 Puebloviejo-Urdaneta.

Marco conceptual

Actualmente la seguridad informática o también llamada la seguridad en los sistemas de información, es la que representa el conjunto de medios y técnicas implementados para afianzar la integridad y que no se propaguen involuntariamente los datos de los informes o noticias de las instituciones que recorren dentro del sistema de información, entendiendo así como tal a la agrupación de datos que conceden el almacenamiento y la circulación de la información que el sistema contiene, además esta representa la red de actores que interactúan sobre él.

El correo tradicional (sea el envío de una carta, un documento, un telegrama, etc.) es una forma de expresarse a través de un papel escrito y las comunicaciones electrónicas son una forma de expresarse a través de una computadora o un teléfono inteligente (el papel y la computadora son medios distintos a través de los cuales una persona, empresa, institución, etc. Envía un mensaje a otra persona, empresa, institución). El envío de comunicaciones electrónicas a través de Internet, no deja de ser un intercambio epistolar, pero lo que cambia, es el medio a través del cual se efectúa el envío, la rapidez del mismo, la manera en que se efectúa (Granero, et al.,2019).

Hoy en día según (Vega, 2021) la seguridad de la información es un concepto que se involucra cada vez más en muchos aspectos de nuestra sociedad hiperconectada, en gran parte como resultado de nuestra adopción casi ubicua de la tecnología de información y comunicación en nuestra vida cotidiana, muchos de nosotros trabajamos con computadoras para nuestros empleadores, jugamos con computadoras en casa, vamos a la escuela en línea, compramos productos de los comerciantes en Internet, llevamos nuestras computadoras portátiles a la cafetería o al centro comercial y revisamos nuestro correo electrónico en distintos lugares.

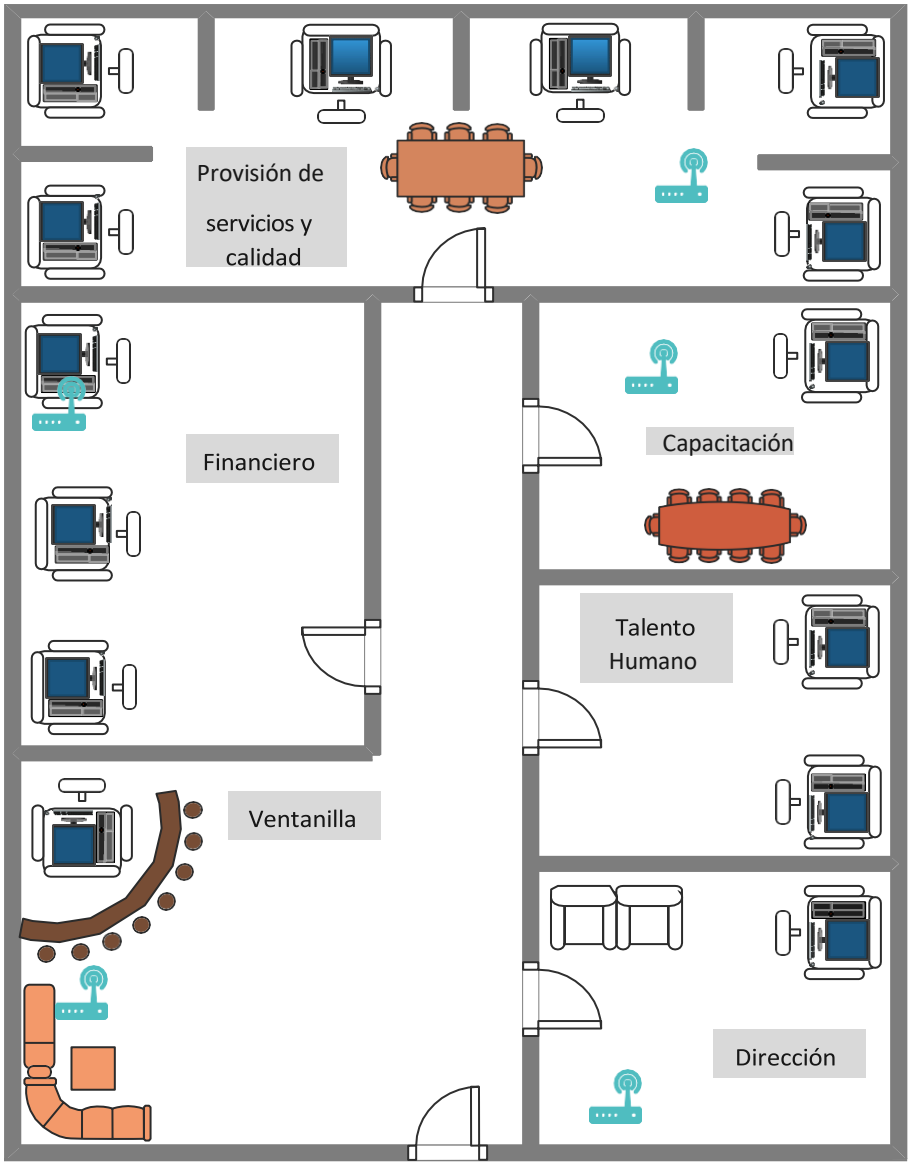
La tecnología nos permite ser más útil cuando trabajamos y nos ayuda acceder a una amplia cantidad de información con solo un clic del mouse, también conlleva una enorme cantidad de problemas de seguridad, la información sobre los sistemas utilizados por empleadores o directores encargados de las diferentes instituciones manejan un sin números de información que se encuentran almacenada en los CPU, correos electrónicos, almacenamiento en la red, estos datos pueden ser hurtados por hacker o ciberdelincuentes, por ende, las consecuencias pueden ser perjudiciales.

En el Distrito de Salud 12D02 Puebloviejo-Urdaneta existe actualmente la problemática en donde los correos institucionales sufren ataques de usurpación de datos debido a que a ellos les llegan mensajes maliciosos o correos spam, llegan un sin número de correos al día donde el personal del área de sistemas de la institución tiene que analizar de manera exhaustiva lo que en él está redactado o cualquier link que este anexado a él, si no se analiza de manera muy profunda el correo que se recibe este puede contener algún tipo de virus, spyware, gusano informático, malware, phishing, y estos ataques pueden ser muy peligrosos para la institución.

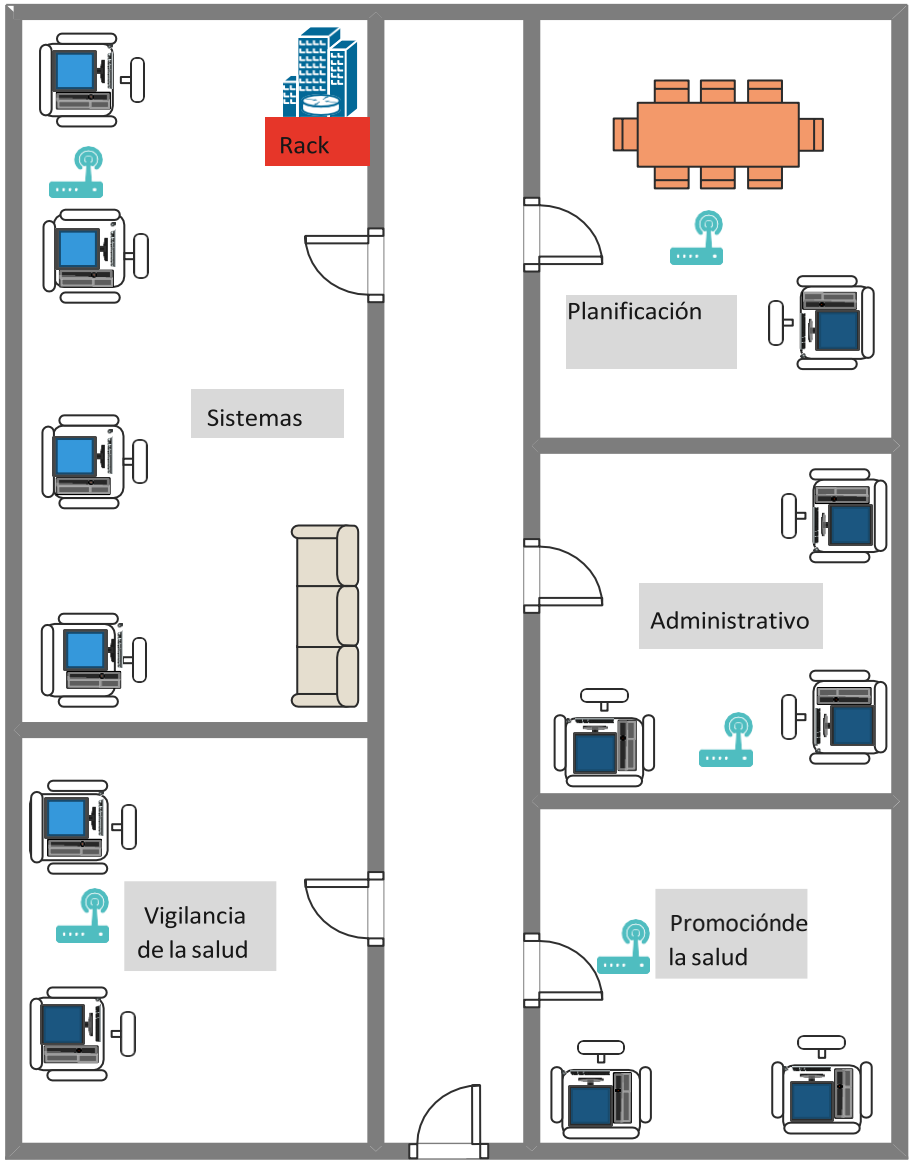
El día 30 de mayo del presente año uno de los empleados de la institución le llego un correo electrónico malicioso que tenía anexado un link, el trabajador de la institución ingreso a dicho link, luego al instante se produjo el ataque les llenaron el servidor de correos basura o mejor conocido como correos spam, el servidor de la institución colapso ya que tenía más de 380.000 mensajes en espera y esto produjo que el servidor colapse, el proveedor de servicio de internet de la institución les corto del servicio, luego tuvieron que enviar un oficio a sus proveedor diciendo que les devuelva el servicio de internet, la solución que se dio a este ataque fue identificar la IP del atacante y proceder a bloquearla mediante las iptables, así se logró dar fin a este ataque.

En el distrito mencionado el día 2 de julio del presente año les llego un correo electrónico del Centro de Respuestas a Incidentes Informáticos Nacional ECUCERT (de la Agencia de Regulación y Control de Telecomunicaciones), donde ellos les decían que en su dirección IP presentaba una vulnerabilidad, luego de recibir dicho correo de manera inmediata el equipo del área de sistemas realizaron una revisión completa a los computadores y equipos informáticos que se encuentran conectados al terminal de acceso a internet ya estos se encuentren conectados de manera alámbricas o inalámbricas para que así los hackers no puedan aprovechar esta vulnerabilidad.

Planta baja



Primer piso



Nº de Equipos	**Área**	**Características**
Pc 1	Provisión de servicios ycalidad	Procesador Core i3. Memoria RAM de 4 GB. Disco duro de 500 GB. Pantalla de 20 pulgadas.
Pc 2	Provisión de servicios y calidad	Procesador Core i3. Memoria RAM de 4 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 3	Provisión de servicios y calidad	Procesador Core i5. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 4	Provisión de servicios y calidad	Procesador Core i5. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 5	Provisión de servicios y calidad	Procesador Core i3. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 6	Provisión de servicios y calidad	Procesador Core i3. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 7	Financiero	Procesador Core i3. Memoria RAM de 8 GB.

		Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 8	Financiero	Procesador Core i5. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 9	Financiero	Procesador Core i5. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 10	Capacitación	Procesador Core i3. Memoria RAM de 4 GB. Disco duro de 500 GB. Pantalla de 20 pulgadas.
Pc 11	Talento humano	Procesador Ryzen 3. Memoria RAM de 8 GB. Disco duro de 1 Tb. Pantalla de 20 pulgadas.
Pc 12	Talento humano	Procesador Ryzen 3. Memoria RAM de 8 GB. Disco duro de 500 GB. Pantalla de 20 pulgadas.
Pc 13	Ventanilla	Procesador Ryzen 3. Memoria RAM de 4 GB. Disco duro de 750 GB. Pantalla de 20 pulgadas.
Pc 14	Dirección	Procesador Ryzen 5. Memoria RAM de 8 GB. Disco duro de 750 GB. Pantalla de 20 pulgadas.

Pc 15	Sistemas	Procesador Ryzen 7. Memoria RAM de 16GB. Disco duro de 1 Tb. Pantalla de 20 pulgadas.
Pc 16	Sistemas	Procesador Core i7. Memoria RAM de 16 GB. Disco duro de 1 Tb. Pantalla de 20 pulgadas.
Pc 17	Sistemas	Procesador Ryzen 7. Memoria RAM de 16GB. Disco duro de 1 Tb. Pantalla de 20 pulgadas.
Pc 18	Sistemas	Procesador Ryzen 7. Memoria RAM de 16GB. Disco duro de 1 Tb. Pantalla de 20 pulgadas.
Pc 19	Planificación	Procesador Ryzen 3. Memoria RAM de 4 GB. Disco duro de 500 GB. Pantalla de 20 pulgadas.
Pc 20	Administrativo	Procesador Core i5. Memoria RAM de 8 GB. Disco duro de 1 Tb. Pantalla de 20 pulgadas.
Pc 21	Administrativo	Procesador Core i5. Memoria RAM de 8 GB. Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 22	Administrativo	Procesador Core i5. Memoria RAM de 8 GB.

		Disco duro de 700 GB. Pantalla de 20 pulgadas.
Pc 23	Vigilancia de salud	Procesador Ryzen 3. Memoria RAM de 4 GB. Disco duro de 500 GB. Pantalla de 20 pulgadas.
Pc 24	Vigilancia de salud	Procesador Ryzen 5. Memoria RAM de 8 GB. Disco duro de 750 GB. Pantalla de 20 pulgadas.
Pc 25	Promoción de salud	Procesador Ryzen 3. Memoria RAM de 4 GB. Disco duro de 500 GB. Pantalla de 20 pulgadas.
Pc 26	Promoción de salud	Procesador Ryzen 5. Memoria RAM de 8 GB. Disco duro de 750 GB. Pantalla de 20 pulgadas.

En la actualidad en la institución manejan un sistema de base de datos MySql, ya que es un gestor de base de datos gratuito y de código abierto, es uno de los gestores de base de datos más utilizado a para los servidores web a nivel mundial, además es uno de los gestores más fácil de aprender a manejar, pero no es uno del más seguros ya que es de código.

La institución cuenta con un rack mejor conocido como servidores principales, el rack sirve para para tener todos los equipos informáticos ya estos sean de redes o de sistemas operativos, el servidor de la empresa se encuentra en el área sistemas y a mi parecer se encuentra bien ubicado en esa área, ya que cualquier anomalía que pueda ocurrir se procederá a solucionarla de manera inmediata por parte del personal del área de sistemas, lo que no me parece correcto es que se encuentra ubicado en un lugar muy pequeño esto hace que no se ventile de manera correcta, una sugerencia seria que se lo colocara en un lugar más amplio y así rack no sufra de sobrecalentamiento y funcione de manera correcta.

En los tiempos actuales existen un sin número de ataque informáticos que se realizan por medio de los corres electrónicos, analizar cada correo que llegan a nuestra bandeja de entrada y verificar que no tenga algún tipo de virus informático, cualquier link o archivo malicioso tomaría mucho tiempo a las personas que trabajan en un área de sistemas, por ende, existen también software que se encargan de analizar los correos electrónicos de una manera rápida y eficiente, uno de los más conocidos es Systools Simplifying Technology este programa detectara los correos electrónicos que contengan alguna información maliciosa.

Los ataques informáticos es una forma de poder ingresar a los equipos informáticos o servidores de una organización, los piratas informáticos ingresan a los equipos es mediante la implantación de un virus o archivo malware, con esto logran alterar el

funcionamiento de los equipos informáticos y producen daños o también pueden hurtar la información de la organización, los ataques suelen ser causados por personas ajenas a la organización, también existe la posibilidad de que los ataques sean provenientes de la misma organización de empleados actuales o empleados pasados que cuentan con acceso para poder sustraer o borrar la información.

Los riesgos informáticos se describen como la inseguridad que existe dentro de un sistema, programa o red, por el posible riesgo de realizar un suceso vinculado con la amenazas o daños a los bienes o servicios informáticos de una empresa u organización, estos pueden ser equipos informáticos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, los riesgos informáticos se encuentra asociado de activo amenaza y vulnerabilidad esto nos da a entender que nuestra información está siempre expuesta a riesgos.

Una vulnerabilidad informática es una debilidad que existe en un sistema, que puede ser aprovecha por los hackers para comprometer el sistema y la información que tiene en mismo, los tipos de vulnerabilidad que existen son de hardware, software y de procedimentales, estas pueden ser utilizadas por personas maliciosas, ellos podrán acceder a los datos y los hurtaran de manera inmediata o podrían robar la información y la empresa quedarse sin la información que tenía almacenada o en algunas ocasiones exigen cierta cantidad de dinero para que ellos devuelvan la información.

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de alguna forma de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica,

por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. (Arellano & Darahug, 2021).

El phishing es un ataque informático que hace mención al método que es utilizado por personas que se dedican a la ciberdelincuencia para engañar a las personas, el phishing su forma de operar consiste con el envío de un correo electrónico que simula la identidad de una organización de confianza en el cuerpo del mensaje del correo se invita a la persona a ingresar información personal con el propósito de obtener información como son los usuarios y contraseñas, datos de tarjetas de crédito o débito y numerosas cuentas bancarias, también el correo puede traer anexado un link a una página web facilita el ataque.

Un virus informático no es otra cosa que un programa con código malicioso que infecta la computadora con el objetivo de alterar el correcto funcionamiento de un equipo, cosa que logra contagiando los archivos mediante un código maligno. Se caracteriza porque necesita de la intervención del usuario para ser ejecutado; luego, hace copias de sí mismo y, de esta forma, se propaga a través de la red, el correo electrónico, los pendrives y todo elemento que pueda contener o enviar código (Ciccariello, 2022).

Spyware

Tras instalarse en un equipo víctima, permanece inadvertido dentro de él mientras recaba información del sistema para enviársela después al atacante sin ser detectado. Sus objetivos pueden ir desde el acceso a los ficheros almacenados en memoria, hasta la obtención de credenciales de usuarios. Dentro del Spyware, una de las funciones más extendidas es la de los Keyloggers, que almacenan las pulsaciones de teclado que se realizan en el sistema (MAÍLLO, 2022).

La seguridad de la información es utilizada para la protección de los datos que maneja una empresa, para esos es necesario que la empresa cumpla con los 3 pilares de la información, según Villalón (2020) “La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades” (Pag. 4).

Seguridad online personal tiene un carácter más individual y está relacionada con la protección de los equipos computacionales; dispositivos electrónicos con la privacidad, protección de los datos personales y con la seguridad en las transacciones económicas online. En todos los casos, que se refieren tanto a los equipos fijos como a los dispositivos móviles, existen herramientas de seguridad (Iñiguez, 2020).

El objetivo de la seguridad de software es proteger las aplicaciones y el software posibles amenazas exteriores estos podrían ataques maliciosos y virus, el mecanismo que más se utiliza al interior de este tipo de seguridad son los programas antivirus, estos programas detectan los archivos con virus que se encuentra en el software y se actualiza automáticamente y es capaz de eliminar los virus encontrados, otras opciones son los cortafuegos, filtros antispam, software para filtrar contenidos y contra publicidad no deseada.

La seguridad del hardware hace referencia a proteger las computadoras y dispositivos frente a ataques o amenazas, tenemos que perseverar no solo la protección del software si no también el hardware utilizamos a diario en nuestras actividades laborales o educativas, uno de los métodos que más se utiliza es el uso de cortafuegos o firewalls de hardware y servidores proxy, también Iñiguez (2020) nos dice que “El hardware es la parte física de la computadora, y es un elemento que necesita seguridad, por lo que los

fabricantes han creado herramientas que ofrecen este servicio, principalmente los cortafuegos y los firewalls de hardware" (Pag. 17).

Los archivos que van anexado a los correo electrónico algunos son enviados por hacker y estos proliferan y propagan virus en nuestras computadoras o equipos informáticos e incluso pueden hurtar nuestra información, por lo consiguiente existen en la actualidad software que escanean los correos electrónicos que nos llegan y los utilizamos para analizar y detectar eficazmente los virus de correo electrónico, analizan de forma automática los mensajes que nos llegan a nuestros correo electrónico en busca de virus, también existen software más específicos que eliminan el malware, los virus y bloquean el spam, programas son eficaces para combatir los virus de los correo electrónico.

Systools Simplifying Technology es un programa que cuenta con varias herramientas como son migración de datos, análisis forense de datos, centro de datos y seguridad de datos, que son objeto de análisis para el caso de estudio del Distrito de Salud 12D02 Puebloviejo-Urdaneta. Estas herramientas son totalmente capaces de ayudarnos a investigar y analizar correos electrónicos para adquirir cualquier información. ofrece servicios de análisis forense digital cubren correos electrónicos basados en la web, correos electrónicos basados en computadoras de escritorio, correos electrónicos basados en la nube y también correos electrónicos almacenados en unidades locales.

Los principios de confidencialidad no solo deben aplicarse para proteger la información sino todos aquellos datos e información de los que sea responsables, La información puede tener carácter confidencial no solo por ser de alto valor para la organización, sino por ejemplo porque puede estar amparada por legislación de protección de datos de carácter personal, un ejemplo de violación de la confidencialidad son las filtraciones sufridas por entidades bancarias, grandes empresas y gobiernos para exponer públicamente algunas de sus actividades (Romero, et al.,2018).

El principal objetivo de la confidencialidad evitar la divulgación no autorizada de la información sobre una empresa u organización, también la confidencialidad hace referencia a la privacidad de la información, mediante las medidas que la acogen para garantizar que la información está segura, con esto se garantiza que la información no llegue a manos equivocadas, se acceder a dicha información por una autorización y control, esto hace que los datos se mantengan ocultos y seguros, para que nadie pueda lograr ver los recursos de la empresa.

La integridad tiene como objetivo evitar las modificaciones de la información por personas no autorizadas, siempre deberá conservar la consistencia, precisión y confiabilidad de los datos mientras el ciclo de vida de la misma, garantiza que usuarios no autorizadas no puedan alterar los datos o eliminarlos, la información no se cambiará durante algún ataque informático que pueda suceder y por eso se mantendrá inalterada ante accidentes o intentos maliciosos. Según (Ferro J. , 2020) La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la Información.

La disponibilidad tiene como objetivo prevenir la interrupción no autorizada de los recursos informáticos, garantiza que la persona que es dueño de la información pueda acceder a ella pueda acceder a ella sin sufrir ninguna degradación en cuanto a accesos de su información y que él pueda acceder el día y la hora que desee o que se necesario para el usuario poder acceder a información, también así como la creación de respaldos en la nube, asegura que la disponibilidad de la red y la información de los usuarios autorizados. Según (Vega, 2021) la disponibilidad: significa que la información y los recursos están

disponibles cuando se los necesite. A menudo, la disponibilidad es el elemento más importante para una organización, sobre todo si está orientada a servicios. La pérdida de disponibilidad se logra mediante ataques de denegación de servicios. Estos ataques tienen como objetivo desactivar el acceso temporalmente, y son usualmente motivados por razones económicas o políticas.

Una vez que se ha evidenciado en conocimiento teóricos la confidencialidad, disponibilidad e integridad de la información es necesario proporcionar los lineamientos de seguridad informática que son directrices y tienen como finalidad el buen uso y cuidado de los recursos de la tecnologías de información para el personal encargado del área de sistemas del Distrito de Salud 12D02 Puebloviejo-Urdaneta dando a conocer las pautas de importancia en el presente documento y sirva de gran ayuda para los problemas que se susciten en el mismo.

A continuación, se detalla los lineamientos para la seguridad informática:

La seguridad informática en las instituciones tiene que ser robusta ya que las empresas contienen información muy confidencial de sus clientes, hace algunos años atrás algunas organizaciones caen siendo víctimas de ataques cibernéticos debido a las pocas medidas de seguridad cibernética propia de ella, momentos actuales utilizan tecnologías modernas y herramientas informáticas para llevar a cabo el funcionamiento correcto de la misma, estas ya sean para conferencias de larga distancia, comunicación con los clientes y proveedores, e incluso para la realización de transacciones bancarias, el almacenamiento en la nube se ha convertido en parte importante para el buen funcionamiento de las empresas, el internet puede ser una bendición, pero también tiene su parte de riesgos y vulnerabilidades.

Hoy en día, toda organización está concienciada en la custodia de dicha información. La tendencia actual es la de implementar a nivel institucional o empresarial sistemas de gestión de la seguridad de la información [SGSI). Se trata de sistemas con múltiples ventajas para las organizaciones, ya que minimizan los incidentes de seguridad que llegan a suponer grandes problemas para un negocio, como pueden serla afectación de la productividad, de la imagen corporativa, de los ingresos e incluso del rendimiento financiero (García, 2022).

El buen uso de los activos informáticos son los recursos tecnológicos del ambiente de la información comunicativa es decir el hardware y software de la institución, los activos informáticos son designado a cada persona por el directos principal de área y cada persona es responsable del uso del correcto del mismos, así como es la información almacenada en ellos, también García (2022) nos dice "La información es uno de los activos más importantes para una organización. Esta está constituida por los datos de sus clientes, el inventario del almacén, las facturas, los datos de sus trabajadores" (Pag. 69).

La clasificación de la información es una sucesión en el cual la institución evalúa los datos que tiene y el nivel de resguardo que cada una requiere, es una de las fases más complejas, pero sin duda es una de las más interesante, donde cada empleado es responsable del resguardo de información, él debe garantizar que la información esté protegida para que así asegurar su integridad y confidencialidad, de acuerdo a su clasificación. Ellos deberán utilizar los datos e información a la que posean acceso solamente con el propósito relacionado con el cumplimiento de sus funciones.

En la prestación de servicios por terceros el proveedor que provee su servicio informático a una institución y que posea acceso a información discreta y confidencial debe acogerse a los mandatos de la ley, reglamentos y demás mecanismos normativos con relación al acceso a la información pública y resguardo de datos personales, también debe contar con

tratados de no divulgación ni uso que pueda dañar a institución. El servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación.

La protección contra código malicioso algunas organizaciones están desprotegidas ante la acción de virus o troyanos, por esta razón es esencial incluir una agrupación de medidas, en la mayoría de instituciones contratan antivirus para solucionar los problemas, los antivirus no son de todo seguro, también pueden ser vulnerados, se recomienda capacitara los empleados de qué manera ellos deben actuar y, por supuesto, saber realizar procedimientos de recuperación y verificación de la información.

El uso de cuentas de usuario toda persona que trabaja en una institución necesita tener acceso a los servicios informáticos de la misma, requiere de una cuenta de usuario y contraseña, la misma que deberá ser entregada por el responsable del servicio, las solicitudes de alta, baja o cambio de privilegios de cuentas de usuario para acceder a los servicios informáticos agregado a su perfil de puesto de trabajo debe ser solicitada a través del sistema de mesa de servicios, y debe ser entregada al jefe de área demandante, con su debido justificado. Si algún empleado deja de laborar en la Institución o cambia de área de trabajo, el jefe de podrá pedir a la institución el acceso al equipo institucional que ésta tenía asignado, el cual deberá ser concedido para que el sustraiga la información pertinente que el allá tenido.

El uso del correo electrónico institucional es para solo el uso exclusivo de los empleados activos administrativos, este medio de comunicación deberá ser utilizado sólo para realizar actividades con respecto a sus funciones, como el uso de servicio de mensajería debe ser utilizado para el desarrollo de actividades concernientes al puesto del personal, a toda persona que sea despedida por la institución una vez recibida la notificación de baja por parte del Departamento de Talento Humano, se procederá a inhabilitar el servicio

de correo electrónico, luego que hayan transcurridos 30 días hábiles el contenido que posee en su cuenta de correo inhabilitada será eliminado sin que genere ningún respaldo del mismo. Es de suma responsabilidad de todo empleado que tenga correo electrónico institucional notificar al personal de la institución la sospecha del uso no autorizado de su cuenta.

La gestión del correo electrónico es una de la tarea en las que más tiempo se invierte en el ámbito empresarial, por lo que es recomendable desarrollar una serie de hábitos y buenas prácticas para que se lleve a cabo de una forma eficiente (Alvarez & Garcia, 2021).

Con la relación de emplear bibliográficamente estudios relacionados a distintos tipos de ataques a los correos institucionales y más aún en la institución que está siendo objeto de estudio se realiza los siguientes conceptos, definiciones que aportan información necesaria y coherente para conocimiento de las personas encargadas en el área de sistemas del Distrito de Salud 12D02 Puebloviejo-Urdaneta, además que sirven para la prevención, cuidado de las distintas modalidades que puedan suceder en cuanto a las amenazas que puedan sufrir los correos de carácter no solo laboral sino también en lo personal. A continuación, se detalla algunos tipos de amenazas que puedan suscitarse.

Fraude en correos empresariales:

Para (Ferro J. , 2020) en el argot técnico fraude "es un acto deliberado de abuso de confianza, el cual, aprovechándose de engaño, se realiza para obtener un beneficio sin consentimiento de la empresa afectada". El fraude puede ser cometido por un empleado de la empresa (fraude interno) o por un cliente o proveedor (fraude externo).

En cuanto a los fraudes en correos empresariales los estafadores se hacen pasar por empleados que laboran en la institución o aquellos que trabajaron en un periodo de tiempo y tienen conocimiento alguno de información o de las actividades que se desarrollan lo

hacen de una manera donde centran sus esfuerzos en los empleados que tienen acceso a los datos económicos, personales de la empresa, o a los departamentos de Recursos Humanos, existe una defensa de la bandeja de entrada basada en API sirve como un método de protección más seguro y eficaz frente a los ataques de fraude esta identifica un intento de suplantación basado en el historial de comunicaciones.

Alrededor del 80% de los correos electrónicos enviados en el mundo son correos no deseados. El correo no deseado es un mal económico "algo de lo que querrías consumir menos" y hay muchas externalidades negativas asociadas a él. Todo ese correo basura te hace perder tiempo, colapsa los buzones de correo y puede ocupar un valioso ancho de banda y provocar que el internet vaya más lento. Cuando se desea mandar correo basura los remitentes no tienen en cuenta los costes que imponen a los receptores o a otros usuarios de internet (Goolsbee, Levitt, & Syverson, 2018).

Entre las principales posibilidades de sufrir ataques a correos electrónicos está el correo no deseado, dada la conceptualización de los autores se hace relevancia a fraudes u obtención de información privada. Los remitentes envían un correo electrónico a distintas direcciones o a uno en específico, con la expectativa de que respondan al mensaje, además recopilan direcciones de correo electrónico de una variedad de fuentes para tratar y en ciertos casos acceder a la información, incluido el uso de software para obtener direcciones, es por ello que los encargados en el área de sistemas de la institución deben ser énfasis con el resto del personal a no caer en este tipo de engaño.

Para (Bottini, 2021) El termino malware se refiere a cualquier tipo de software que daña dispositivos, roba datos y genera caos, mal funcionamiento o molestia al usuario afectado. Hay muchos tipos de malware (virus, troyanos, spyware, ransomware, etcétera) de acuerdo a como se lo quiera catalogar por su peligrosidad por el tipo de ataque que realiza o por la manera en que se propaga.

Cabe mencionar que malware es otro tipo de posibilidades que puedan presentarse para la usurpación de datos, noticias, se menciona que el malware se encuentra oculto principalmente en el propio documento o a su vez en una secuencia de comandos incrustada lo descarga de un sitio web externo, existe una defensa del correo electrónico frente al malware que aporta a estar prevenido, la protección antimalware se efectúa de una manera en el nivel de la puerta de enlace, como precaución antes de que los correos lleguen a las bandejas de entrada.

La suplantación de la URL para (Ortega & Manuel, 2021) menciona que esta vulnerabilidad podría usarse como parte de una estafa de suplantación de identidad, al redirigir a los usuarios a un sitio malicioso, donde si no se aplica una validación, un usuario malintencionado podría crear un hipervínculo para redirigir a sus usuarios a un sitio web malicioso o no valido.

Mediante los ataques de suplantación de identidad o URL los ciberdelincuentes intentan de obtener información de carácter confidencial, personal o laboral, sean nombres de usuario, sus contraseñas o datos bancarios entre otras, para utilizarla con fines ilegales usan el correo electrónico para hacer que sus víctimas ingresen información personal o de sus trabajos en un sitio web falso que tiene similitud a uno legítimo, existe defensa del correo electrónico frente a la suplantación de URL esta defensa de la bandeja de entrada en los correos está basada en API complementa y completa la seguridad que ofrece una puerta de enlace. Las URL que son falsas o que muestran alguna evidencia de ataques de suplantación pueden ser bloqueadas.

La suplantación de dominios tiene como objetivo hacerse pasar por un dominio de una página web establecida, a esta técnica se la conoce como el “typosquatting” (errores tipográficos) los piratas informáticos reemplazar o colocan una letra demás como nombre de su dominio como, por ejemplo: Google pasaría hacer Gooogle, los usuarios caen en

este tipo de confusión, ellos acaban visitando el sitio web, sin querer, normalmente con el propósito de ataques fraudulentos, cuando intentan hacer el ataque los hackers se registran el dominio y lo compran para así pueden estafar a las personas.

Marco metodológico

A continuación, se describe la metodología de investigación empleada la cual ha sido seleccionada para la realización de este estudio, en la cual a través de técnicas o procesos han sido empleadas para alcanzar los objetivos antes planteados en el desarrollo del presente documento.

El presente trabajo se enmarca en una investigación cualitativa que permitió recabar datos mediante la entrevista a la persona encargada en el área de sistema del Distrito de Salud 12D02 Puebloviejo-Urdaneta con respecto a el riesgo que presentan los correos institucionales y de esta manera obtener la información necesaria y pertinente para el desarrollo de este estudio de caso, conociendo la problemática actual para aportar información a soluciones factibles para la institución en cuanto a la seguridad informática y el buen manejo de sus datos e informaciones de carácter privada de las distintas gestiones que ejercen en el trabajo de la salud pública.

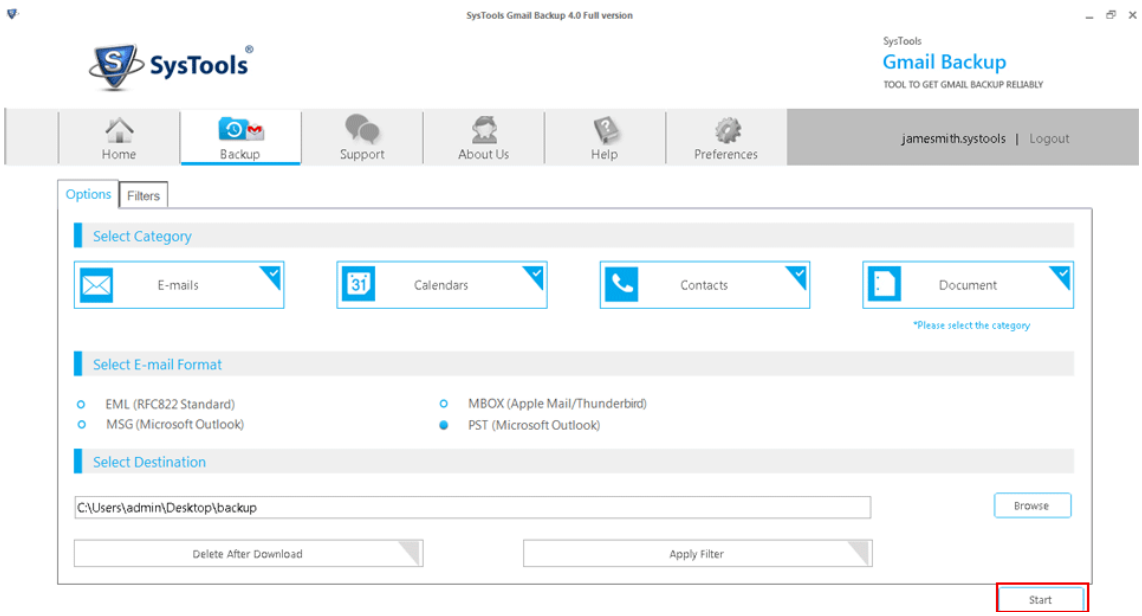
Entendiéndose a la investigación cualitativa que determina la realidad en un contexto de manera natural y en la forma que sucede, además de interpretar a los fenómenos de acuerdo con las personas involucradas en el desarrollo de la problemática de la investigación, además este tipo de investigación utiliza una variedad de instrumentos para recoger información, como las entrevistas, las observaciones, imágenes, entre otras.

Siendo la metodología inductiva una estrategia de razonamiento que se basa en la observación se evidencio la problemática actual de los riesgos que se suscitan en los correos institucionales en el Distrito de Salud 12d02 Puebloviejo-Urdaneta obteniendo como conclusión cual es la finalidad de los piratas informáticos para hurtar información o datos de la institución.

Además, la metodología bibliografía también forma parte en desarrollo de esta temática puesto que contribuye con información académica sobre el tema que está siendo objeto de investigación, encaminadas a localizar documentos e información relacionados con un tema o autores concretos basándose en libros, folletos, artículos de manera actualizada como se estipulan en las normas APA para la organización y presentación de información en este estudio de caso.

Resultados y Discusión de Resultados

Luego de haber recibido la autorización para realizar el análisis a los correos institucionales, la institución nos entregó un archivo MBOX, donde estaban las copias de seguridad de los correos electrónicos recibidos, procedimos a realizar el análisis con el programa SysTools Simplifying Technology el cual cuenta con varias herramientas para realizar el análisis respectivo, es uno de los más utilizados en la actualidad para el análisis forense.



Después que el programa terminó de realizar el análisis al archivo MBOX se encontraron los siguientes correos sospechosos los cuales los detallaremos como información importante se logró obtener:

1. Encontramos un correo electrónico con varias imágenes, esto nos dio una sospecha que podía ser un archivo malware, ya que dentro de los mensajes de correos electrónicos que traen anexado imágenes existe la posibilidad de algún tipo de archivo malware, lo examinamos con una mayor profundidad, con las herramientas del programa y sin un mayor esfuerzo podemos confirmar que efectivamente el correo recibido tenia anexado un archivo malware, si este archivo

se hubiera abierto fuera del programa este podría a ver puesto en ejecución de cualquier instrucción que en él estuviera programada para que el equipo afectado falle.

2. Se logró encontrar varios mensajes de con temática de Phishing donde decía “Su cuenta no está verificada, necesita verificar su cuenta” donde el emisor del correo electrónico le pedía al usuario nombres y apellidos completos, correo electrónico de respaldo, nombre de usuario, contraseña, verifique su contraseña, esto fue un claro ejemplo que era el mensaje que contenía el correo era parte de un ataque Phishing, además contenía una advertencia donde decía que si la información que ellos deseaban no era enviada dentro de 8 días hábiles su cuenta se eliminará y se perdería toda la información que contenga en él, esto se lo hace para que el usuario responda de manera inmediata y así ellos hurten los datos.
3. Se encontró correos con publicidad engañosa, donde decía “Has ganado el Iphone 13”, en la cual anexaba un link, el cual contenía un formulario donde pedían datos personas, la dirección del domicilio para poder enviar el premio que te ganaste, además tenías que pagar él envió del paquete, allí mismo te lo cobraban, tenías que colocar tus datos de tarjeta de débito o crédito, con las herramientas del programa fue muy fácil detectar y analizar que se trataba de un correo de publicidad engañosa.
4. Se logró localizar mensajes de correos electrónicos con la temática de ransomware, la herramienta del programa los detecto como correos spam, y los separo del demás correo, algunos de ellos contenían documentos en formato Pdf y Word otros tenían enlaces a diferentes páginas web, si ellos descargaban los archivos o daban clic en el enlace se descargaba de manera inmediatamente un tipo de malware que se lo conoce con el nombre de ransomware, este malware

impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos, los pagos se suelen realizar mediante criptomonedas o tarjetas de crédito.

Le realizamos una entrevista al jefe del área de sistemas donde le preguntamos las siguientes preguntas:

¿En cuántas ocasiones la institución ha sufrido algún ataque mediante correos electrónicos?

El señor Agustín respondió que la institución ha sido atacada mediante los correos spam 5 veces en los últimos 7 años, cuando los hackers intentan hackear la institución les llegan entre 80.000 a 120.000 mensajes spam, lo que es muy tedioso e incluso el proveedor de internet de la institución les suspenden el servicio, y para que este servicio sea devuelto tienen que enviarle un oficio a su proveedor diciendo que ellos se hacen responsables de que pueda ocurrir.

¿La institución cuenta con servicios en la nube?

Con relación a esta pregunta se conoció que actualmente la institución no cuenta con servicios en la nube, pero la institución se encuentra haciendo las gestiones necesarias para contratar este servicio, ya que dicho servicio es muy bueno y así ellos tendrá resguarda la información de la institución de manera segura.

¿Qué métodos utilizan para que el personal de la institución no habrá los mensajes maliciosos?

Nos respondió que en utiliza la ingeniería social les comunica en ciertos momentos del día al personal de la institución que están llegando mensajes sospechosos y que no los habrá si es posibles que eliminen dichos mensajes o bloqueen al usuario que los envía,

también se hacen capacitación cada bien de mes con temas actualizados sobres los ataques cibernéticos.

¿Qué métodos de seguridad utiliza la institución para el exceso de correos spam?

Su respuesta fue utilizamos lo que se conoce como BlackList para negar la recepción de mensajes, mayormente la utilizamos para los correos spam, también usamos las WhiteList para autorizar él envió y la recepción de mensajes. Si esto no llegase a funcionar contamos con las IpTables estas nos permiten bloquear la dirección ip del atacante de nuestro servidor de correos y que este siga funcionando de manera normal.

¿La institución está preparada para afrontar cualquier tipo de ataque informático mediante correo electrónico?

Respondió que la institución si está preparada para afrontar cual tipo de ataques informáticos mediante correos electrónicos, ya que ellos se capacitan semanalmente leyendo libros y artículos sobre ataques informático.

El distrito 12D02 Puebloviejo-Urdaneta, es una institución de salud pública que tiene a cargo 13 subcentro de salud y un hospital, la institución mencionada maneja de la información de cada subcentro y del hospital, la cual requiere ser guarda de manera segura y confidencial, el personal que trabaja en los subcentros y hospital, cada persona tiene un correo electrónico institucional, que es proporcionado por el Ingeniero Agustín Torres el cual es el encargado de la administración de los correos y de los servidores de la empresa, actualmente cuenta con 320 correos institucionales creados, y los administra a través de un gestor de correos electrónicos llamado Zimbra.

En la obtención de resultados del análisis de riesgo que presentan los correos institucionales en el Distrito de Salud 12D02 Puebloviejo-Urdaneta ayudarán a la institución a la implementación de buenas prácticas en el manejo de sus datos e

información logrando mitigar las distintas vulnerabilidades y amenazas que han sido identificadas y que sufren constantemente sus correos electrónicos institucionales. El centro objeto de estudio fue el del área de Sistemas que sirve como un soporte fundamental en el manejo y almacenamientos de información y que interactúan permanentemente con las demás áreas que tiene el distrito al surgir inconvenientes.

Los resultados del análisis de riesgos que presentan los correos instituciones de la institución dio a entender que la empresa está expuesta a ataques mediante correos electrónicos día a día ya que encontramos los siguientes tipos de ataques:

1. Se encontró mensajes con imágenes este tipo de ataque se lo conoce como malware.
2. Se encontró varios mensajes de con ataques Phishing.
3. Se logró localizar mensajes de ataque ransomware.
4. Se encontró mensajes con publicidad engañosa.

El Distrito de Salud 12D02 Puebloviejo-Urdaneta se encuentra con un elevado índice de inseguridad puesto que se ha evidenciado en el contexto de este documento las diferentes vulnerabilidades en las actividades diarias que realizan los funcionarios. Una debida aplicación de controles basadas en buenas prácticas de seguridad aportara de forma adecuada y convincente a una gestión correcta en el manejo de seguridad de sus datos, y así poder eliminar o reducir el riesgo a la cual están expuesto diariamente.

Teniendo como buenas prácticas los controles de seguridad para mitigar la inseguridad existente, con la persona encargada en el área de sistemas de la institución que permita estar constantemente involucrado en las problemáticas que se presenten monitoreando y dar seguimiento a los incidentes ocurridos. Además, mejorar la cultura organizacional en

temas de seguridad mediante la implementación de charlas sobre el uso y correcto funcionamiento, también mediante políticas en materia para salvaguardar la información.

Con base en lo expuesto en este trabajo de investigación se da a conocer lo importante que es realizar un análisis en cuanto al manejo de información en la seguridad de los correos institucionales y las dificultades que puedan presentarse en caso contrario, manteniendo la sostenibilidad y garantizar la seguridad de datos.

El reforzar los controles para la seguridad en los sistemas de información, conlleva a obtener datos de manera clara y precisa de los sistemas, según esto lo requiera la institución y sus funcionarios, y así minimizar incidentes de seguridad como daños o afectaciones a aplicaciones, equipos, en ciertas ocasiones hurto o alteración de información, que puede ocasionar inconvenientes a la institución.

Con el fin de obtener resultados en la problemática que en la actualidad posee la institución en temas de seguridad de la información, se elaboró un manual de preguntas de entrevista a la persona encargada en el área de sistema en donde se obtuvo respuestas en lo que realmente preocupa a los colaboradores de las áreas cuando estas presentan problemas de ataques y tienen que recurrir a ella para poder solucionar el inconveniente que se haya suscitado, evidenciándose en archivos que se tienen en registro que han sufrido anteriormente.

Cabe mencionar además que el Distrito de Salud 12D02 Puebloviejo-Urdaneta no cuenta con un manual de políticas en lo que respecta a la seguridad de la información. Es decir que no existe una política formal en la que se detalle los controles o procesos a implementar para así poder evitar la divulgación, salida o violación de información, lo que se ha implementado como medida de seguridad es la desactivación de todos los medios removibles de almacenamiento. (modificar o eliminar).

Conclusiones

Luego de haber realizado el análisis se concluyó lo siguiente:

El Distrito de salud 12D02 Puebloviejo-Urdaneta tiene un alto índice de riesgo es sus correos institucionales ya que en el análisis realizado a la institución se encontramos el envío masivo de correos spam, esto es muy riesgoso ya que corre el riesgo de que pueda ser infectado con un malware y este puede encapsular la información de la institución y la podría hurtar.

La institución no cuenta con lineamientos de seguridad de la información, donde se deben detallar las medidas preventivas para resguardar la información, ya que la mayoría de instituciones y organizaciones tienen estos lineamientos de seguridad porque ellos manejan un gran volumen de información confidencial que son recogida en todas las áreas de la institución.

Los funcionarios que laboran en la institución no tienen conocimiento de los tipos de ataques que se pueden realizar mediante los correos institucionales, el Distrito de Salud corre el riesgo que alguna persona que labora en ella envié información confidencial a los atacantes pensando que es una organización de gran jerarquía y así estos puedan hackear la institución.

Recomendaciones

Luego de haber realizado el análisis se recomienda lo siguiente:

Se recomienda la aplicación de un software de firewall, este podría reducir el impacto o mitigar los riesgos que presentan los correos electrónicos que son enviado por los piratas informáticos, ya que los firewalls proporcionan herramientas claves en los sistemas de protección de datos, también se podría implementar (DLP) o mejor conocido como una protección contra pérdida de datos.

Se sugiere que la institución mínima cada 3 meses cree una sala de capacitación para el personal que labora en ella, para que ellos tengan conocimiento de los tipos de ataques que puedan ocurrir estos serían los virus informáticos, malware, phishing y las demás modalidades que tiene los piratas informáticos tienen para hurtar la información, y así ellos no puedan caer en estos tipos de riesgo que podrían comprometer la información de la institución.

Implementar los lineamientos de seguridad que se propusieron en este proyecto debido a los riesgo y vulnerabilidades que se presentaron en él, estos van a salvaguardar la información respetiva si estos se implementan, así se podrá conocer cuáles son los riesgos que estarán presente y como solucionarlos de manera remota he inmediata, para salvar los datos de la institución.

Referencias

Alvarez, A., & Garcia, J. (2021). *Comunicacion empresarial y atencion al cliente.* Editex.

Arellano, L., & Darahug, M. (2021). *Manual de informática forense: Bases metodológicas: Científica, Sistémica, Criminalística, Tecnológica-Pericial y Marco Legal.* Errepar.

Bottini, C. (2021). *Elimina el malware sin instalar programas.* RedUsers.

Ciccariello, P. (2022). *MALWARE: Los más peligrosos y cómo enfrentarlos.* RedUSERS.

Ferro, J. (2020). *Curso Superior en jefe/inspector de servicios y auxiliares de servicios.* José Manuel Ferro Veiga.

Ferro, J. (2020). *Investigacion operativa del fraude interno y externo empresarial.* Jose Manuel Ferro Veiga.

García, B. (2022). *Transmisión de información por medios convencionales e informáticos.* Editorial Paraninfo.

Goolsbee, A., Levitt, S., & Syverson, C. (2018). *Microeconomia.* Reverte.

Granero, H., Molina, E., & Bielli, G. (2019). *E-Mails, chats, WhatsApps, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías: Validez probatoria en el proceso civil, comercial, penal y laboral.* elDial.com.

Iñiguez, H. (2020). *SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES.* Hector Giusepphe Iñiguez Estrada.

MAÍLLO, J. (2022). *Hackers: Técnicas y herramientas para atacar y defendernos.* Ediciones de la U.

Ortega, C., & Manuel, J. (2021). *Ciberseguridad. Manual práctico.* Editorial Paraninfo.

Romero, M., Figueroa, G., & Vera, D. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* 3Ciencias.

Vega, E. (2021). *Seguridad de la información.* 3Ciencias.

Villalón, A. (2020). *Seguridad en Unix y redes. Versión 2.* Nau Llibres.

Anexos

Aceptación de la realización del caso de estudio en la institución.

República del Ecuador

Ministerio de Salud Pública
Coordinación Zonal 5 - Salud
Dirección Distrital 12D02 – PueblovieJo – Urdaneta - Salud
Despacho Distrital

Urdaneta, 29 de julio de 2022
Oficio. Nro. DD-12D02-2022-104

Lcdo. Eduardo Galeas Guijarro, MAE
DECANO DE LA FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

En referencia al oficio nro. D-FAFI-UTB-0225-2022, en el cual la *Facultad de Administración, Finanzas e Infomática* de la Universidad Técnica de Babahoyo, solicita la autorización para realizar un Caso de Estudio en esta dependencia del Ministerio de Salud Pública, previa la obtención del titulo de tercer nivel, de la carrera Ingeniería en Sistemas de Información, al Sr. VILLAMAR SÁNCHEZ JONATHAN PATRICIO con CC. 1250177266, estudiante de la Escuela de Sistema de la facultad antes mencionada. *Con este antecedente:*

La Dirección Distrital 12D02 – PueblovieJo – Urdaneta – SALUD, *Autoriza*: Al Senor. VILLAMAR SÁNCHEZ JONATHAN PATRICIO con CC. 1250177266, realizar el Caso de Estudio, titulado: **ANÁLISIS DE RIESGO QUE PRESENTAN LOS CORREOS INSTITUCIONALES DEL DISTRITO 12D02 PUEBLOVIEJO - URDANETA.**

Particular que informo para los fines pertinentes.

Atentamente,

Firmado electrónicamente por:
MARIUXI LEONOR
AGUIRRE ZAMBRANO

Obstra. Mariuxi Leonor Aguirre Zambrano
DIRECTORA DISTRITAL DE SALUD 12D02 - PUEBLOVIEJO - URDANETA

Original: Facultad de Administración, Finanzas e Infomática - UTB
Copia: Archivo

Dirección: Calles. Eduardo Obando y Bartolomé, Código postal: 120651 / Ricaurte - Ecuador
Teléfono: 593-5-3700200 – www.salud.gob.ec

Gobierno del Encuentro

Ejemplo de Phishing

Verificar tu cuenta de correo electrónico

De : Administrador de correos <romina.faiola@isprambiente.it> jue., 30 de jun. de 2022 14:31

Asunto : Verificar tu cuenta de correo electrónico

Responder a : Administrador de correos <marvinuwadia@gmail.com>

Estimado usuario
Ha sido informado de amenazas en curso en el servidor, le solicitamos que valide los detalles de su correo electrónico para una verificación adecuada con el proveedor de servicios del servidor de correo web.
Por la presente, se le advierte que valide su correo electrónico de inmediato y no ignore este mensaje, de lo contrario, su correo electrónico será considerado y marcado para actividades de phishing.
VALIDA SU CORREO ELECTRÓNICO AQUÍ
Las pruebas y el mantenimiento del servidor están en curso y debe volver a validar su cuenta una vez que reciba este aviso.
Una cosa que todos podemos hacer para evitar ataques cibernéticos generalizados es fortalecer la seguridad de nuestro servidor.
Gracias por su comprensión.

Administrador del servidor
Cc: Soporte Sistemas

Ejemplo de Phishing

CUENTA verificación / actualización

De : ZIMBRA WEBMAIL ADMIN <renatosales@pgj.campeche.gob.mx> vie., 29 de jul. de 2022 08:58

Asunto : CUENTA verificación / actualización

Para : Recipients <renatosales@pgj.campeche.gob.mx>

Responder a : webmasterzimbra1@gmail.com

Su cuenta no ha pasado por el proceso de verificación / actualización. Los titulares de cuentas deben actualizar sus cuentas dentro de los 5 días hábiles posteriores a la recepción de este aviso. El incumplimiento de este aviso dentro de la fecha límite puede no ser capaz de enviar o recibir todos los mensajes y el propietario correrá el riesgo de perder su cuenta.

Confirme los detalles de la cuenta a continuación.

1. Nombre y apellido:
2. Correo electrónico completo en:
3. Nombre de usuario:
4. Contraseña:
5. Vuelva a escribir la contraseña:

NOTA !!! Si no actualiza su cuenta, su cuenta se eliminará automáticamente de nuestro sistema.

Nos disculpamos por cualquier inconveniente causado.

Sinceramente
Atención al cliente
Equipo de soporte técnico de Zimbra.

Analizando los resultados

Discusión de resultados