Minerva Journal
ISSN-E: 2697-3650 Vol.3, Spec. Issue N°1, (pp. 76-85)

https://doi.org/10.47460/minerva.v1iSpecial.82

Protección de datos para el uso de bring your own device

García Suarez Yaira Anabel
https://orcid.org/0000-0002-4204-1981
e1313676312@live.uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Chone – Ecuador

Arteaga Lucas Kassandra Elizabeth
https://orcid.org/0000-0002-9545-1212
e1313827592@live.uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Chone – Ecuador

Castillo Bravo Eliecer Francisco
https://orcid.org/0000-0003-0108-7526
eliecer.castillo@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Chone – Ecuador

Zambrano Villegas Yenny Alexandra
https://orcid.org/0000-0002-4203-5848
yeny.zambrano@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Chone – Ecuador

Mendoza Navarrete Martha Lorena
https://orcid.org/0000-0001-9135-5963
martha.mendoza@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Chone – Ecuador

Recibido(20/06/2022), Aceptado(31/09/2022)

Resumen. - Bring Your Own Device (BYOD), en español "trae tu propio dispositivo" se trata de una política empresarial que aporta flexibilidad y productividad en los colaboradores de las compañías, organizaciones o establecimientos que la adoptan. En este trabajo se efectuó un estudio con el objetivo de conocer el uso de manera formal de los dispositivos móviles personales para actividades laborales, utilizando técnicas de recolección como encuestas y entrevistas. En este sentido, se analizó si las personas emplean o no de manera oficial el BYOD, los principales resultados mostraron que un importante número de trabajadores si emplea la tendencia de forma informal, desde su smartphone, mientras que otros no lo están usando, pero tienen la disponibilidad de hacerlo. Finalmente, se propone elaborar un plan de acción que ayude en la utilización del Bring Your Own Device con la protección de datos y mitigación en la pérdida de la información adecuadas.

Palabras clave: Bring Your Own Device (BYOD), seguridad móvil, protección de datos.

Data protection for the use of bring your own device

Abstract. - Bring Your Own Device (BYOD), in Spanish "bring your own device" is a business policy that provides flexibility and productivity to the employees of the companies, organizations, or establishments that adopt it. In this work, a study was carried out with the objective of knowing the formal use of personal mobile devices for work activities, using collection techniques such as surveys and interviews. In this sense, it was analyzed whether or not people officially use BYOD, the main results showed that a significant number of workers use the trend informally, from their smartphone, while others are not. using, but they have the availability to do so. Finally, it is proposed to develop an action plan that helps in the use of Bring Your Own Device with adequate data protection and mitigation in the loss of information.

Keywords: Bring Your Own Device (BYOD), mobile security, data protection.

I. INTRODUCCIÓN

Bring Your Own Device es una política empresarial que le permite a los trabajadores utilizar su dispositivo móvil para acceder a las fuentes de datos corporativas, como correos electrónicos, datos empresariales, entre otros. El riesgo de perder datos e información valiosa al momento de utilizar BYOD, hace que las empresas, instituciones y organizaciones no quieran adoptar Bring Your Own Device, pero un arma valiosa es la seguridad de la información que ayuda a mitigar los riesgos que afectan la confidencialidad, integridad y disponibilidad de los recursos de Tecnología de la Información (TI) [1].

Según el Ministerio de Telecomunicaciones, tres de cada diez ecuatorianos tienen un smartphone y el 90,8% tiene acceso a la tecnología móvil 3G y 4G, pero es común que estos sean vistos como un dispositivo de comunicación e incluso de entretenimiento, y en algunas compañías los consideren como distractores. En este sentido, uno de los principales desafíos para las empresas es aprovechar esa tecnología en lugar de aislarla, ya que puede constituir un activo importante para su operación, tanto en productividad como en infraestructura. La tendencia Bring Your Own Device se ha mantenido latente en los últimos años [2].

La implementación de Bring Your Own Device requiere de un análisis de todos los departamentos y responsabilidades de los empleados, y luego decidir que recursos son accesibles mediante dispositivos móviles, incorporar medidas de seguridad para cubrir una variedad de dispositivos móviles contra amenazas y ataques, por último, capacitar y educar a los empleados sobre la seguridad BYOD, las soluciones implementadas y el cumplimiento de las políticas de seguridad es fundamental [3].

Este trabajo se centró en conocer el uso de Bring Your Own Device en el Hospital Napoleón Dávila Córdova del Cantón Chone siendo el principal problema la protección de los datos. En este apartado se muestran cinco secciones: la introducción; el desarrollo donde esta una breve descripción de BYOD y protección de datos; la metodología utilizada para la investigación; la explicación de los resultados obtenidos con un plan de acción para implementar Bring Your Own Device de forma segura; finalmente, se indican las conclusiones en base al análisis del hallazgo.

II. DESARROLLO

Bring Your Own Device es una iniciativa relativamente nueva, adoptada por empresas que permiten que sus colaboradores utilicen dispositivos móviles privados (pueden ser teléfonos inteligentes, tabletas y computadoras portátiles e incluso pueden incluir dispositivos de Internet de las cosas (IoT), que son integrados a la red empresarial) para completar el trabajo de una manera conveniente y flexible [4]. La política BYOD trae consigo un impacto positivo tanto a la empresa como a los colaboradores, los principales beneficios de BYOD son: aumenta la productividad y la satisfacción laboral de los colaboradores; mejora la eficiencia de los empleados; mejora la movilidad de los dispositivos y aumenta la accesibilidad y flexibilidad laboral; ahorra coste de organización mediante reducción de los gastos de TI en la provisión de dispositivos, software y mantenimiento; al utilizar sus propios dispositivos, el empleado se cuidará y cumplirá con las políticas y prácticas de seguridad, que se encuentren establecidas en la empresa, organización o institución [5].

Las empresas, organizaciones e instituciones dependen absolutamente de sus programas de TI para capturar, almacenar, procesar y distribuir su información, y con la llegada de BYOD ha aumentado el riesgo en la pérdida de datos, la seguridad de la información es la disciplina necesaria para mitigar los riesgos que afectan la confidencialidad, integridad y disponibilidad de los recursos de TI [6].

Si no se puede tener un buen control acerca de los riesgos estos se convierten en amenazas que se pueden materializar, entre las principales están:

- Malware: Un dispositivo infectado con algún software malicioso puede conducir a la fuga de información confidencial, el uso de servicios adicionales como llamadas y envío de mensajes de texto no programados, interrupción parcial o completa del correcto funcionamiento del dispositivo.
- Spam: Mensajes de correo electrónico no deseado que se reciben de fuentes desconocidas los cuales generan consumo del dispositivo en recursos como ancho de banda y memoria.

- Phishing: Esto puede llegar a presentar a través de un correo electrónico o un mensaje de texto para engañar al usuario e ingresar a un sitio web falso solicitándole información sensible de la organización.
- Bluetooth y Wi-Fi: Al conectarse a diferentes redes o compartir archivos el dispositivo puede verse fácilmente infectado lo cual daría paso a la interceptación de datos que viajan desde o hacia los dispositivos móviles.
- Amenazas persistentes avanzadas: Es una amenaza inteligente y cuidadosa que la utilizan con el fin de extraer y filtrar datos confidenciales importantes de las empresas.
- Ingeniería social: Manipulan a la víctima para obtener información acerca del sistema para proceder con sus objetivos de extraer o compartir los datos de la empresa.

La protección de los datos hace referencia a la seguridad, buenas prácticas y principios elementales para salvaguardar la información de una determinada persona ya sea en su vida privada o pública [7]. En otras palabras, se refiere a los derechos fundamentales de las personas, es decir, el individuo decide si desea o no compartir ciertos datos, quién puede tener acceso a los mimos, por cuánto tiempo, por qué razones, tener la posibilidad de modificarlos y mucho más. Y para esto un aspecto muy importante es que se deben considerar las obligaciones legales y éticas [8].

Se consideran medidas de seguridad existentes a redes privadas virtuales (VPN), firewall y filtrado de correo electrónico, que son ideales para proteger los recursos dentro de las redes y cuando los dispositivos móviles ya están involucrados en BYOD antes de la aplicación de políticas formales [9]. Las VPN facilitan las conexiones de red exclusivas con los dispositivos y permiten el acceso a los recursos en un entorno controlado, mientras que los cortafuegos protegen las redes al monitorear el tráfico de la red y negar el acceso a solicitudes sospechosas y por último el filtrado de correo electrónico detecta y advierte a los usuarios de los correos electrónicos infectados. Los dispositivos móviles pueden sincronizar aplicaciones de correo electrónico, lo que beneficia al dispositivo cuando el filtrado de correo electrónico esta activo [10].

III. METODOLOGÍA

Se obtuvo información del personal que labora en el Hospital Napoleón Dávila Córdova del Cantón Chone, para establecer la muestra para las técnicas de recolección.

Tabla 1. Personal del Hospital Napoleón Dávila Córdova del Cantón Chone.

FUNCIÓN	CANTIDAD
• GERENTE	1
• ADMINISTRATIVOS	67
• ENFERMEROS/AS	400
• MÉDICOS	116
TOTAL	**584**

Se utilizó la fórmula de población finita para obtener el tamaño de la muestra. Esta fórmula se aplicó por motivo de que la población es menor a 100.000 habitantes.

$$n = \frac{(Z)^2 * p * q * N}{e^2(N-1) + Z^2 p * q} \qquad (1)$$

Donde n= Tamaño de la muestra, N= Tamaño de la población. (584), p = Probabilidad a favor. (0,5), e = Error de muestra. (10%=0,1), q= Probabilidad en contra. (0,5), Z = Nivel de confianza. (90%=1,64). Obteniendo un valor de n=60 para la muestra. La muestra seleccionada estuvo compuesta por 1 gerente, 6 personas del área administrativa, 41 enfermeras y 12 médicos.

Se utilizó el método bibliográfico para la revisión profunda de investigaciones realizadas, el analítico para seleccionar contenidos relevantes de investigaciones verídicas referente al tema planteado, el inductivo ayudó a concluir gracias al dominio del tema, el deductivo para realizar una posible propuesta, el de campo porque fue necesario ir hasta el hospital para realizar el estudio y el sintético se lo utilizó para considerar cada información relevante y hallazgo como un todo para realizar el resumen de la investigación. En la recolección de la información se utilizaron técnicas como la encuesta y entrevista, la primera para conocer el uso del dispositivo móvil personal para las actividades laborales con un cuestionario de diez preguntas variadas y la segunda se realizó a la gerente y al director de Tecnología de la Información para conocer el uso formal de BYOD.

IV. RESULTADOS

A continuación, se presenta un diagrama de barras con los porcentajes mayoritarios obtenidos en cada una de las diez preguntas aplicadas en la encuesta.

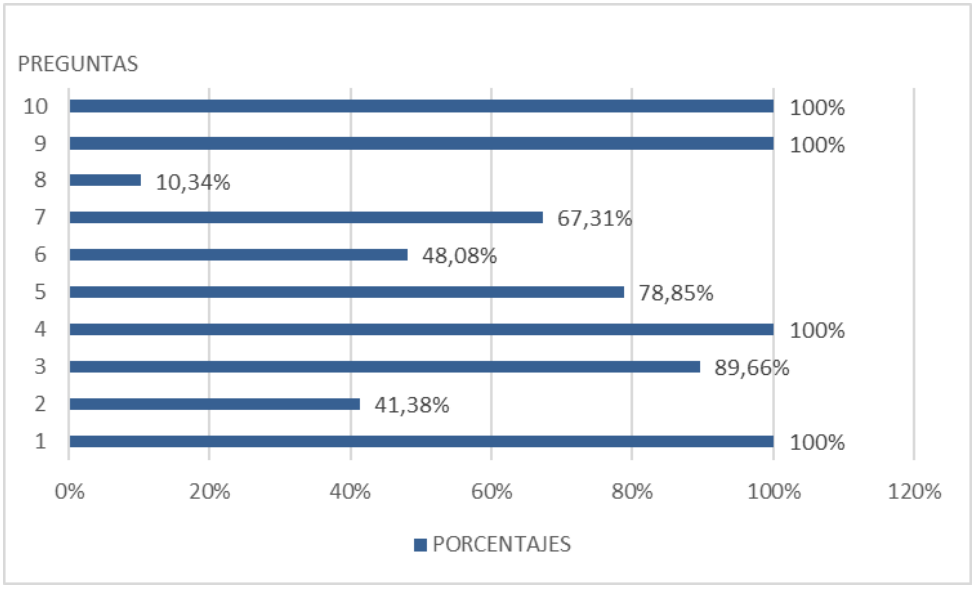

Fig. 1. Diagrama de respuestas con su porcentaje mayoritario.

El ítem 1 de la encuesta, corresponde a la totalidad del uso de un dispositivo móvil inteligente, mientras que el ítem 2 muestra la prevalencia del sistema operativo android, por otro lado el ítem número 3 a la utilización del móvil personal en lo laboral, el siguiente a la no utilización de protocolos de seguridad, el 5 al consentimiento del uso del smartphone para el trabajo por parte del departamento de TI, seguidamente en el ítem 6 la frecuencia de la utilización del móvil en lo laboral correspondiente a 4 horas diarias, en el 7 el principal problema que han presentado ha sido el ataque de phishing. Finalmente, desde el ítem 8 se les atribuye a las personas que contestaron que no usan el móvil personal para laborar, en el 9 manifestaron que no lo hacen por el miedo a la posibilidad de comprometer los datos, y en el 10 aceptaron que con un plan de seguridad lo harían.

En la entrevista realizada a la gerente y director de TI ambos manifestaron que en esta casa de salud no hacen uso de BYOD como tal, pero que si sería factible su implementación por las visitas del Ministerio de Salud y si estaría establecido BYOD podría acelerarse el trabajo usando directamente el móvil y de la misma manera el personal tendría mayor flexibilidad a la hora de laborar por el tamaño del dispositivo.
En base a estos resultados se propone un plan de acción que ayude a proteger los datos cuando se vaya a utilizar el Bring Your Own Device (Figura 1).

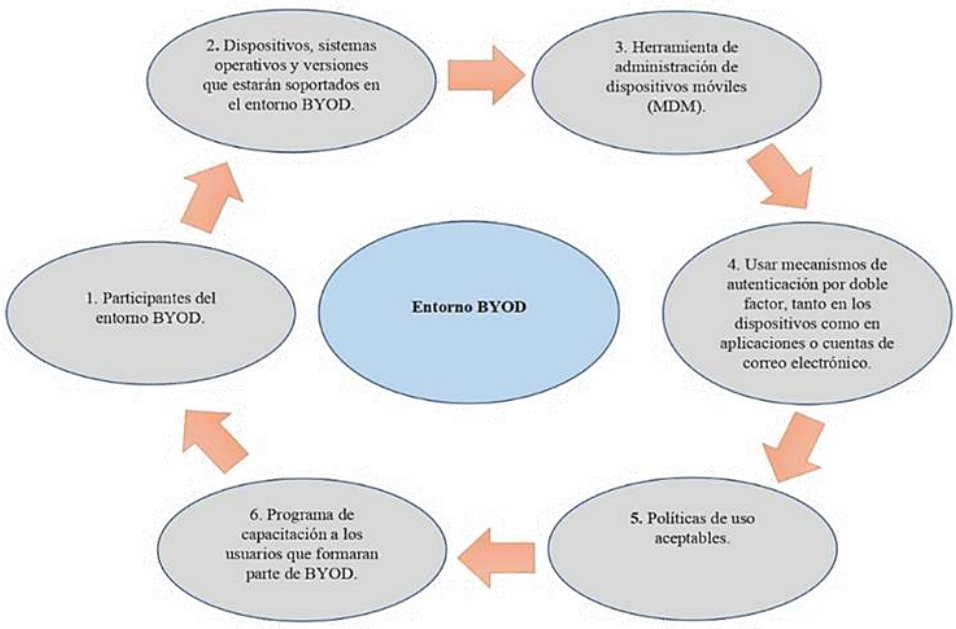

Fig. 2. Pasos para la implementación de BYOD

A. Participantes del entorno BYOD

Como es una tendencia relativamente nueva, es importante delimitar las personas que entraran al entorno BYOD, en este caso se podrían considerar a 60 colaboradores del Hospital Napoleón Dávila Córdova del Cantón Chone que cumplan con las especificaciones necesarias en sus móviles personales, empezando como una prueba piloto para ir monitoreando su funcionamiento.

B. Dispositivos, sistemas operativos y versiones que estarán soportados en el entorno BYOD.

En el entorno BYOD se deben considerar dispositivos con sistemas operativos y versiones que reciban actualizaciones para mejoras en el funcionamiento y en la seguridad del software permitiendo solucionar errores y vulnerabilidades, se pueden considerar; móviles con Android hasta Android 12; móviles con iOS hasta iOS 15.

C. Herramienta de administración de dispositivos móviles (MDM)

Es importante tener el entorno de trabajo BYOD controlado, una de las opciones recomendadas para minimizar riesgos es implementar un sistema que permita gestionar y administrar los dispositivos móviles (Mobile Device Management o MDM). Existen muchas herramientas en el mercado que realizan esta función, pero en este caso se recomienda a Mobile Device Manager, porque permite lo siguiente:

Gestión de dispositivos móviles que permite:

- Agregar dispositivos rápidamente: brinda la facilidad de agregar múltiples dispositivos móviles simultáneamente.
- Dashboard intuitivo: permite ver el ecosistema de dispositivos disponibles en la institución.
- Perfiles de configuración: configuración de perfiles para imponer políticas tales como WIFI y VPN.
- Vigila los activos: permite el seguimiento completo de la visibilidad de los dispositivos en la red.

Gestión de aplicaciones:

- Fácil distribución de aplicaciones: distribuye y administra aplicaciones internas y de la tienda iOs, Android, Mac OS, Chrome OS y Windows.
- Permite solo las aplicaciones aprobadas en los dispositivos: con un modo Kiosco bloquear dispositivos para ejecutar una sola aplicación o un conjunto de aplicaciones.
- Gestiones el inventario de aplicaciones: con esta opción se obtiene los datos detallados y permite administrar licencias de aplicaciones en dispositivos móviles.
- Separa las aplicaciones corporativas de las personales: mantiene la integridad de los datos en los dispositivos separando los perfiles de trabajo de la empresa de los perfiles personales.
  Permite gestionar la seguridad de la siguiente manera:
- Realiza acciones como limpieza de datos, bloqueo remotos e informe.
- Permite acceder de una manera rápida y segura a los emails de la empresa.
- Acceso seguro a la red con los permisos de uso de los dispositivos según el rol y acceso selecto a cuentas corporativas.

D. Mecanismos de autenticación por doble factor

Para aumentar la seguridad del entorno BYOD en el Hospital Napoleón Dávila Córdova del cantón Chone la autenticación por doble factor cumple un rol fundamental, el colaborador al ingresar a la aplicación de trabajo debe autenticarse. Estos son los pasos para la autenticación por doble factor.

- Se solicita al colaborador acceder a las aplicaciones de la empresa.
- El colaborador ingresa su nombre de usuario y la contraseña, con lo que cumple con el primer factor de seguridad.
- Después de que la aplicación reconoce al colaborador, se le solicita que inicie el segundo paso del proceso de acceso. En esta etapa el colaborador debe probar que tiene algo, ya sea una tarjeta de identificación o un teléfono inteligente, para cumplir el segundo factor de seguridad.
- En la mayoría de los casos se le puede enviar a los colaboradores un código de acceso de seguridad único que pueden usar para confirmar su identidad.
- Finalmente, el colaborador ingresa la clave de seguridad y, después de que la aplicación la haya autenticado, se le otorga acceso.

E. Políticas de uso aceptable

Las políticas de uso aceptable que se pueden considerar en un principio para implementar BYOD en el Hospital Napoleón Dávila Córdova, van a ayudar a controlar la seguridad de los datos, estas pueden ser:
Políticas en caso de robo o pérdida del dispositivo móvil.

- Si el dispositivo móvil es robado o perdido automáticamente se debe realizar un borrado de datos remoto al contenedor BYOD de manera inmediata.
- Mantener siempre encendido la localización mediante GPS, wifi o la información de la antena de telefonía con la que esté conectado el dispositivo.
- Tener siempre activado el bloqueo de pantalla del terminal. En caso contrario se bloqueará de manera remota.

Políticas para el control del acceso a la red.

- El acceso a la red corporativa a través de dispositivos personales debe estar integrado en el sistema de control de accesos (autenticación, doble factor). De esta forma el empleado debe acreditar su identidad antes de acceder a los servicios de la red corporativa.
- Proporcionar a los colaboradores acceso mediante red privada virtual (VPN).

Políticas de uso de dispositivos manipulados.

- Los dispositivos rooteados (Android) o con Jailbreak (iOS) tienen estrictamente prohibido acceder a la red.
- Los dispositivos móviles que no están en la lista de los dispositivos compatibles de la institución no pueden conectarse a la red.

Políticas para el uso del móvil en horarios de oficina.

- El dispositivo BYOD será monitorizado en horas laborables dependiendo del contrato de trabajo establecido.
- El dispositivo BYOD debe tener encendido el antivirus en horarios laborales.

Políticas de gestión de contraseñas para el entorno BYOD.

- Las contraseñas de los dispositivos BYOD deberán ser mayor o igual a ocho caracteres.
- Tener una combinación de números, letras minúsculas y mayúsculas, incluir caracteres especiales.
- Las contraseñas se rotarán cada 90 días y la nueva contraseña no puede ser una de las 15 contraseñas anteriores.

Políticas para realizar copias de seguridad.

- Deben realizarse copias de seguridad diarias en cada uno de los contenedores de los dispositivos BYOD.
- El departamento de Tic es responsable de hacer copias de seguridad de los datos de los dispositivos, pero solo se permite usar un disco duro encriptado.

Políticas de aplicaciones permitidas.

- El director de Tic será el encargado de definir las aplicaciones con las que se va a trabajar en el entorno BYOD.

Políticas de seguridad del dispositivo.

- El dispositivo que este inactivo durante 5 minutos deberá bloquearse automáticamente.
- Después de 5 intentos fallidos de inicio de sesión al entorno BYOD, se bloqueará y deberá comunicarse con el departamento de Tic para su recuperación.
- Los dispositivos BYOD deberán estar protegidos mediante métodos de autenticación por doble factor, por ejemplo, claves, lectores biométricos, SMS, email, etc.

Políticas para el usuario BYOD.

- El usuario será responsable exclusivo de mantener a salvo su identificación que le permita acceder al entorno BYOD.

- El perfil asignado es de uso único al responsable, si llegase a compartir o difundir su identificador será penalizado
- En caso de que se violen las políticas, el usuario no podrá acceder al espacio de trabajo BYOD y debe pasar por un proceso con el departamento de Tic's para proceder al desbloqueo.
- El usuario tiene prohibido copiar y pegar contenido entre el espacio de trabajo corporativo y personal.
- El usuario no podrá permitir el acceso al contenedor de trabajo BYOD a terceros.
- Cuando el usuario usa BYOD, debe tener la precaución de que los datos no sean leídos por personas no autorizadas.
- El usuario no podrá descargar software sin licencias en el contenedor.
- El usuario está de acuerdo en que el espacio de trabajo creado en su dispositivo será monitorizado en horas laborables.
- El usuario solo tendrá acceso al entorno de trabajo BYOD cuando se conecte a la red empresarial destinada al ambiente Bring Your Own Device.
- El usuario está de acuerdo que si el dispositivo móvil es robado o perdido automáticamente se debe realizar un borrado de datos remoto al contenedor BYOD de manera inmediata.
- El usuario tiene que asistir a las reuniones de capacitación antes de entrar al ambiente BYOD y después mensualmente.
- Si el usuario BYOD cesa sus funciones en la institución su perfil y rol será eliminado, y se realizará un borrado de información en el entorno de trabajo de manera inmediata.
- El usuario deberá notificar al responsable de seguridad antes de eliminar, vender o entregar el dispositivo BYOD a terceros para su reparación.
- El usuario no podrá descargar e instalar software que estén en la lista de aplicaciones prohibidas para BYOD dentro del contenedor.
- El usuario es el encargado de utilizar su dispositivo de manera ética en todo momento y se adhiera a las políticas de uso aceptable.
- El usuario es personalmente responsable de todos los costos asociados con su dispositivo.

Políticas para el cumplimiento de la Normativa.

- Se asegurará que los empleados conocen la normativa corporativa y se comprometen a cumplirla antes de la incorporación de sus dispositivos personales al entorno de trabajo.

F. Programa de capacitación a los usuarios que formaran parte de BYOD.

Es importante un exitoso programa de capacitación BYOD, ya que puede significar la diferencia entre una fuerza de trabajo más productiva y una violación de datos desafortunada. La mejor manera de comunicar con claridad sus políticas para todas las partes es mediante la inversión en la formación de los empleados mediante cursos. Es por eso que se debe realizar seminarios de capacitación regulares, crear una guía detallada o programar sesiones. La formación permite a los empleados utilizar sus dispositivos de forma segura y eficaz y los educa sobre los riesgos de las personas y de toda la institución de no cumplir.

CONCLUSIONES

De acuerdo con el análisis de los resultados obtenidos gracias a las encuestas y entrevistas, se concluye que en el hospital Napoleón Dávila Córdova del cantón Chone el término Bring Your Own Device no es conocido del todo, sin embargo, hacen uso del dispositivo móvil para laborar en una mayoría. La respuesta de los encuestado permitió comprender la importancia de contar con un protocolo de seguridad que proteja los datos al momento de laborar con el smarthpone, porque el desconocimiento de los riesgos puede llegar a materializar la pérdida de información.

Por otro lado, es importante realizar un diagnóstico profundo de las áreas que van a formar parte del entorno BYOD y con ello que tipo de sistemas operativos usan en sus móviles personales para determinar si poseen las características necesarias, definir los roles y perfiles de los seleccionados, crear usuarios únicos y políticas de uso aceptable para el compromiso de los participantes de esta tendencia. Por lo antes explicado, se realizó un plan de acción para implementar Bring Your Own Device de manera segura en el hospital Napoleón Dávila Córdova del cantón Chone, mismo que puede ser usado y adaptado a las necesidades de la Institución. El principal objetivo de este plan es proteger los datos cuando se use el móvil para laborar sin pasar por alto la intimidad del propietario.

REFERENCIAS

[1] B. Alotaibi y H. Almagwashi, «Una revisión de los desafíos y las soluciones de seguridad de BYOD,» IEEE, p. 6, 2018.
[2] Revista Transformación Digital, «Los peligros del Bring your own device (BYOD),» 2021. [En línea]. Available: https://www.revistatransformaciondigital.com/2021/06/16/los-peligros-del-bring-your-own-device-byod/.
[3] T. W. Ahmad , A. Mendoza y K. Gray, «Desafíos y soluciones de seguridad para el hospital "Traiga su propio,» JMIR MHEALTH Y UHEALTH, vol. 8, p. 13, 2020.
[4] C. Galván, «Bring Your Own Device (BYOD) en el ámbito de la salud,» 2016. [En línea]. Available: https://www.hospitalitaliano.org.ar/#!/home/infomed/noticia/131102.
[5] K. Downer y M. Bhattacharya, «Seguridad BYOD: un nuevo desafío empresarial,» IEEE International Conference on Smart City/, p. 6, 2016.
[6] E. Gil, Big data, privacidad y proteccion de datos., Mdrid: IMPRENTA NACIONAL DE LA AGENCIA ESTATAL, 2016.
[7] L. Mejia, «Diferencia entre privacidad de datos y seguridad de datos,» 2021. [En línea]. Available: https://escuelasciberseguras.com/blog/diferencia-entre-privacidad-de-datos-y-seguridad-de-datos/.
[8] J. P. Murga Fernández, Proteccion de datos, responsabilidad activa y técnicas de garantía, Reus, 2018.
[9] G. Peter, Seguridad de dispositivos móviles y BYOD, John Wiley & Sons, Ltd, 2011.
[10] A. Sara, Q. Muhammad y A. Abdul, «Analysis of BYOD security frameworks,» 2015. [En línea]. Available: https://www.researchgate.net/publication/304406382_Analysis_of_BYOD_security_frameworks.
[11] Revista Transformación Digital, «Los peligros del Bring your own device (BYOD),» 2021.
[12] F. Rivadeneira y G. Rodriguez, «Traiga su propio dispositivo: una encuesta de amenazas y modelos de gestión de seguridad,» Revista Internacional de Negocios Electrónicos, p. 15, 2018.
[13] B. Alotaibi y H. Almagwashi, «Una revisión de los desafíos y las soluciones de seguridad de BYOD,» IEEE, p. 6, 2018.
[14] J. Choi, «Detección de dispositivos BYOD mal configurados en redes Wi-Fi,» Ciencias Aplicadas, p. 16, 2020.
[15] C. Tamayo y I. Silva , «TÉCNICAS E INSTRUMENTOS DE DATOS,» 2018. [En línea]. Available: https://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/23.pdf.
[16] J. L. Abreu, «El Método de la Investigación,» 2014.
[17] Microsoft, «www.microsoft.com/,» 2019. [En línea]. Available: https://www.microsoft.com/es-es/microsoft-365/business-insights-ideas/resources/how-mobile-data-protection-can-help-keep-intruders-out.

Ecuatoriana, recientemente graduada de la carrera de Ingeniería en Sistemas de la Universidad Laica Eloy Alfaro de Manabí, con experiencia en proyectos de vinculación, investigativos y ponencias.

Ingeniera en Sistemas de la Universidad Laica Eloy Alfaro de Manabí, con experiencia de asistente de procesos académicos escolares para aportar beneficios en la construcción progresiva del saber en el alumnado.

Ecuatoriano nacido en Chone, Ecuador. Licenciado en Ciencias de la Educación mención Computación, Comercio y Administración de la institución que actualmente trabaja y con Maestría en Pedagogía de la Universidad Técnica Particular de Loja. Actualmente se desempeña como docente y presidente de la Comisión de Vinculación de la ULEAM Extensión Chone.

Ecuatoriana, nacida en Chone, Manabí. Licenciada en Ciencias de la Educación mención Físicas y Matemáticas. Magister en Educación y Desarrollo Social, especialista en Diseño Curricular por competencias. Docente de la Universidad Laica Eloy Alfaro de Manabí, actualmente Decana de la ULEAM extensión Chone.

Ecuatoriana, nacida en Chone, Manabí. Licenciada en Ciencias de la Educación especialidad Comercio y Administración. Magister en Docencia Mención Gestión en desarrollo del currículo. Actualmente se desempeña como Coordinadora del Área Técnica de la Universidad Laica Eloy Alfaro de Manabí extensión Chone.