Dom. Cien., ISSN: 2477-8818
Vol. 7, núm. 6, Octubre 2021, pp. 63-82

DOI: http://dx.doi.org/10.23857/dc.v7i6.2315

Ciencias sociales y políticas
Artículo de investigación

Propuesta de políticas de Ciberseguridad para el Teletrabajo. Caso de estudio Rectorado ESPOCH

Proposal of Cybersecurity policies for Teleworking. ESPOCH Rector's case study

Proposta de políticas de Cibersegurança para Teletrabalho. Estudo de caso do Reitor da ESPOCH

Galo Iván Vilcacundo-Reinoso [I]
galo.vilcacundo@espoch.edu.ec
https://orcid.org/0000-0001-8210-9111

Omar S. Gómez [II]
oscarsg@gmail.com
https://orcid.org/0000-0002-2951-3833

Correspondencia: galo.vilcacundo@espoch.edu.ec

*Recibido: 25 de agosto 2021 *Aceptado: 15 de septiembre de 2021 * Publicado: 06 de octubre de 2021

I. Maestrante, Pontificia Universidad Católica del Ecuador, Sede Ambato Técnico Docente, Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.
II. GrIISoft Research Group, Escuela Superior Politécnica de Chimborazo-Pontificia Universidad Católica del Ecuador, Sede Ambato, Ecuador.

Resumen

El distanciamiento social causado por la actual pandemia se ha hecho parte de la vida cotidiana de las personas, obligando a que las instituciones públicas y privadas opten por la modalidad de teletrabajo para cumplir sus actividades. Esto hace necesaria la práctica de políticas adecuadas de Ciberseguridad a toda persona que envía o recibe información por medio de Internet. En el presente trabajo se presenta una propuesta de políticas de ciberseguridad orientadas a personas que realizan teletrabajo. Para evaluar la propuesta antes mencionada se realizó un estudio de caso con personas que hacen teletrabajo y que pertenecen al rectorado de la Escuela Superior Politécnica de Chimborazo (ESPOCH). los resultados del estudio de caso sugieren que la implementación de políticas de ciberseguridad para el teletrabajo permite el uso adecuado de la información del Rectorado de la ESPOCH.

Palabras clave: Ciberseguridad; teletrabajo; políticas.

Abstract

The social distancing caused by the current pandemic has become part of people's daily lives, forcing public and private institutions to opt for teleworking to carry out their activities. This makes it necessary to practice adequate Cybersecurity policies for anyone who sends or receives information through the Internet. This paper presents a proposal for cybersecurity policies aimed at people who telework. To evaluate the aforementioned proposal, a case study was carried out with people who do telework and who belong to the Rector of the Higher Polytechnic School of Chimborazo (ESPOCH). The results of the case study suggest that the implementation of cybersecurity policies for telework allows the proper use of the information from the ESPOCH Rectorate.

Keywords: Cybersecurity; telecommuting; policies.

Resumo

O distanciamento social provocado pela atual pandemia passou a fazer parte do cotidiano das pessoas, obrigando instituições públicas e privadas a optarem pelo teletrabalho para o desempenho de suas atividades. Isso torna necessário praticar políticas de segurança cibernética adequadas para qualquer pessoa que envie ou receba informações pela Internet. Este artigo apresenta uma proposta de políticas de segurança cibernética voltadas para pessoas que fazem teletrabalho. Para avaliar a referida

proposta, foi realizado um estudo de caso com pessoas que fazem teletrabalho e que pertencem ao Reitor da Escola Superior Politécnica de Chimborazo (ESPOCH). Os resultados do estudo de caso sugerem que a implementação de políticas de cibersegurança para teletrabalho permite o uso adequado das informações da Reitoria da ESPOCH.

Palavras-chave: Cibersegurança; teletrabalho; políticas.

Introducción

La crisis sanitaria que comienza a afectar al mundo entero debido a la propagación del virus denominado SARS-CoV-2, declarada pandemia por la Organización Mundial de la Salud (OMS) el 11 de marzo de 2020 (*COVID-19: cronología de la actuación de la OMS*, 2020, 28 abril), hace que la comunicación y demás actividades cotidianas se las maneje de forma masiva por Internet exponiéndonos a todos los peligros que este conlleva. Martín, F. A. (2020) menciona que tenemos memoria corta en temas de ciberseguridad, aduciendo que existen actores que generan inseguridad en el ciberespacio, y que estos aprovechan cualquier oportunidad para hacer daño y lucrar de esta además que aprovechando la confusión creada por el teletrabajo masivo y las dificultades para parchear los terminales conectados remotamente, los ciberataques pasaron de algunos centenares de miles por día a casi un millón en algunos países como España y Estados Unidos

Los avances tecnológicos y el mundo en el que nos desenvolvemos han modificado las relaciones sociales tradicionales, haciendo que con teletrabajo se garantice y obtenga los resultados deseados por parte de las personas que laboran en las instituciones, sin la presencia ni el cumplimiento de horarios rígidos; es así como, esta modalidad, que si bien es cierto no es nuevo como oferta laboral, hace que la persona se relacione de otra manera con la institución. (Cifuentes-Leiton & Londoño-Cardozo, 2020)

En la actualidad el distanciamiento social, por la crisis del Covid-19 se ha convertido en una norma de convivencia (Ballestero, 2020), el teletrabajo se transforma en la opción prioritaria a nivel público como privado para dar continuidad a sus actividades.

En Ecuador, el Comité de Operaciones de Emergencia Nacional (COE) del Ecuador, con fecha 28 de abril prioriza el teletrabajo como forma de desenvolvimiento laboral en todas las instituciones públicas y privadas del país, (Resoluciones COE Nacional 28 de abril 2020 – Servicio Nacional de

Gestión de Riesgos y Emergencias, 2020), hace que estas adopten esta modalidad para dar continuidad a sus actividades.

En la Escuela Superior Politécnica de Chimborazo (ESPOCH) el trabajo es presencial tanto en las labores administrativas como académicas, y a partir de la declaración de Pandemia a causa de la COVID-19, en un giro inesperado se comienza a teletrabajar.

En la ESPOCH, la mayoría de los procesos administrativos se los realiza por medio del Internet y gran parte de la documentación ya se encuentra en forma digital, haciendo que, la información salga de la "seguridad" del rectorado de la Institución y comience a ser manejada desde los hogares de los funcionarios; donde no existe una infraestructura de red administrada y, tampoco personal técnico que pueda brindar soporte apropiado en el uso de esta.

En este contexto, muchas veces la falta de experiencia en temas de ciberseguridad por parte de los funcionarios en sus hogares, hacen que se cometan ciertos errores que pueden afectar sea a la Confidencialidad, Integridad o Disponibilidad de la información manejada.

Por tal razón, la motivación del presente trabajo es proponer una serie de políticas de Ciberseguridad en el ámbito de Teletrabajo y evaluar la propuesta en el estudio de caso de los funcionarios del Rectorado de la ESPOCH.

Trabajos relacionados

La globalización del mundo hace que nuevas tendencias aparezcan en todos los ámbitos, es así como, el auge de las Tecnologías de la información y Comunicación (TIC) ha inspirado a que el teletrabajo se convierta en una alternativa bastante atractiva para el desenvolvimiento profesional, haciendo que la continuidad de las actividades de una entidad mantenga el empleo que se puso en riesgo a causa del confinamiento por el Covid-19 (Diego Rodríguez, 2020), y que el conocimiento sobre temas de ciberseguridad sean necesario para evitar que la triada de la información sean vulneradas.

Según Kaspersky, K. (2021) "La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil".

Para el Banco Internacional de Desarrollo (BID) y la Organización de los estados Americanos (OEA) en su publicación de ciberseguridad 2020, BID - OEA, B.-O. (2020), el Ecuador, como estado, aun

no cuenta con una estrategia sólida de Ciberseguridad, se ha logrado avances significativos en contra de amenazas en la red, pero aún no son suficientes, uno de estos avances es el EcuCERT, denominado el equipo de respuesta ante incidentes cibernéticos, mismo que se encuentra a cargo de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

En la actualidad, menciona Arroyo (2020), los delitos cometidos por los ciberdelincuentes van desde ataques a la propiedad intelectual hasta ciberacoso entre otros, bajo este apartado en un ataque buscan apoderarse de credenciales que les permitan tener acceso a información privilegiada de distinta índole de las entidades, sea para beneficio propio o poder obtener algún beneficio con terceros.

Bajo estas afirmaciones se hace necesarias la creación o implementación de políticas de ciberseguridad en el ámbito de teletrabajo para que los funcionarios del Rectorado de la ESPOCH efectúen un correcto manejo de la información teletrabajando.

A continuación, se describe brevemente trabajos relacionados y que han sido desarrollados por investigadores que de una u otra forma han utilizado ciberseguridad para la protección de la información.

Carrillo, J. J. M., Zambrano, N. A., Zambrano, T. J. L., & Bravo, M. Z. 2020, propone la implementación de ciberseguridad basado en 3 ámbitos: Auditoría interna en los procesos de las áreas de Redes, Desarrollo de Software y Documentación; Análisis de Vulnerabilidades e Identificación de Riesgos, mismos que van encaminados a la protección de infraestructura y software, sin mencionar el ámbito de teletrabajo.

Gayo, M. R. 2021, habla sobre definiciones de Teletrabajo y Ciberseguridad, donde se indica que la empresa debe estar atenta a los posibles riesgos que esta modalidad de trabajo conlleva, también da a conocer los riesgos a los cuales se está expuesto y entrega alternativas para teletrabajar de manera segura mediante el uso de una VPN.

Adeva, A., & Ortiz, J. M. V. 2020, menciona que con la pandemia del COVID 19 el teletrabajo creció considerablemente, y con este el porcentaje de ciberataques. Al utilizar software para interconectarse también se buscó como hacer seguras estas interconexiones haciendo de las VPNs una alternativa de protección.

La ciberseguridad, según Ballestero, F. 2020, debe minimizar los riesgos de pérdida de la información y muestra 3 etapas para lograr este cometido, prevención, detección y control y recuperación, mostrando un ecosistema de ciberseguridad basados en una interacción continua entre la

administración pública, empresas proveedoras de productos y servicios, empresas, instituciones y ciudadanos demandantes, universidades, medios de comunicación e instituciones diversas.

Lema, L. L, 2020, menciona que los delitos cibernéticos podrían duplicarse durante el período del brote de coronavirus y no solo por las estafas de phishing , sino también por los ataques de ransomware , debido al acceso remoto inseguro a las redes corporativas, por la falta de formación de los teletrabajadores que exponen sus credenciales de inicio de sesión de los equipos de núcleo familia, así como, por la utilización de los equipos informáticos por todos ellos comprometiendo los archivos e información de la institución a la que presta sus servicios, para lo cual propone una metodología de análisis de vulnerabilidades en 6 etapas bajo un proceso del Instituto Nacional de Ciberseguridad de España.

Y cerrando esta sección un estudio realizado por CEDIA informa que tan sólo el 8% tiene una implementación completa de políticas de seguridad en las universidades del país, el 60% lo tenía de manera parcial y un 32% no contaba con dichas políticas, mostrando el bajo interés sobre los temas de ciberseguridad de las instituciones, (Padilla, R., Cadena, S., Enríquez, R., Córdova, J., & Llorens, F. 2017).

Si bien se han encontrado trabajos que cuentan sus experiencias en la utilización de metodologías, guías o procedimientos de ciberseguridad, en este contexto no se han encontrado trabajos que aborden políticas de ciberseguridad en el ámbito del teletrabajo.

Políticas de ciberseguridad para el teletrabajo

Para la ISO-27001, una afirmación de política define un compromiso general, y debe incorporar objetivos de seguridad de la información o facilitar su desarrollo, además, la intención de la seguridad de la información es proteger la confidencialidad, integridad y disponibilidad de la información.

Es muy importante definir políticas de seguridad interna de una institución sea esta pública o privada con la finalidad de estandarizar las condiciones en las que las personas van a llevar a cabo sus labores cotidianas con la modalidad de teletrabajo.

Las políticas definidas deben resguardar al menos lo siguiente:

- Los perfiles de usuarios para el teletrabajo definiendo los permisos de acceso.
- La posible utilización de equipos personales (BYOD) para el teletrabajo y las debidas medidas de seguridad.
- Política para el almacenamiento de la información de la institución.

- Procedimiento para proteger físicamente los accesos a los equipos de cómputo de la institución.

Bajo la norma NTC-ISO/IEC ISO27001 la aplicación de los controles debe garantizar usos aceptables del manejo adecuado de la información en condiciones de teletrabajo. (Andrés, 2015.)

A continuación, se listan una serie de políticas que pueden ayudar al uso adecuado de la información en condiciones de teletrabajo para los funcionarios del Rectorado de la ESPOCH.

Equipos de cómputo y sistemas operativos

Los equipos proporcionados por la institución o equipos de uso personal deben cumplir con parámetros mínimos de seguridad, y al no cumplirlos serán catalogados como equipos no confiables, en la actualidad no se puede decir que un equipo 100% seguro pero si se puede establecer una línea base para determinar la confiabilidad del equipo de cómputo (Andrés, 2015.)

Los requerimientos mínimos para asegurar un equipo de cómputo son:

Equipos de confianza

- Proteger el acceso de la maquina mediante una contraseña en BIOS
- Sistema operativo y aplicaciones actualizadas.
- Software antivirus, antimalware, antispyware.
- Perfiles de usuario para sin privilegios para instalación de software y modificación de configuraciones.
- Configuraciones seguras para los navegadores de internet
- Bloqueo automático por inactividad.
- Control de acceso sólido.
- Cifrado de disco duro.
- Verificación periódica de las reglas de seguridad de los equipos

Equipos no confiables

En caso de tener múltiples perfiles de usuario en el sistema operativo, debe existir un perfil protegido con contraseña robusta y la información que contiene este perfil no debe ser accedida por otros perfiles en la misma máquina.

En lo posible emplear arranque dual el cual permite dos sistemas operativos en la misma maquina uno destinado para actividades de teletrabajo y el segundo para fines personales**.** (Andrés, 2015.)

BYOD (Bring Your Own Device)

Es una modalidad donde las instituciones optan por reducir costos y la administración de los equipos de cómputo permitiendo al empleado mezclar su vida laboral y personal con el objetivo de aumentar la productividad. Este modelo lleva a importantes problemas de seguridad ya que no existe administración o control por el departamento TI, para lo cual se debe considerar lo siguiente:

- Políticas de seguridad indicando el uso adecuado de los equipos y de la información.
- Cláusula de responsabilidades en el manejo de la información de la institución.

Comunicaciones

La infraestructura en las comunicaciones brinda grandes beneficios en la disponibilidad de aplicativos y de la información de las compañías, pero este denota riesgos en la seguridad ya que los métodos de acceso en las redes sugieren miles de conexiones que pueden ser vectores de ataque.

La seguridad en las comunicaciones debe estar dirigida en combatir o contrarrestar una o varias amenazas ya sea inmediato, latente o potencial que pretendan atentar con los principios de confidencialidad, disponibilidad e integridad de la información.

La creación de un modelo de seguridad para las comunicaciones debe identificar los componentes o características de las redes de comunicación, existen tres tipos de redes. (Andrés, 2015.)

Redes no controladas

Este tipo de red es aquella que no puede ser gestionada o controlada por el departamento de TI Institucional.

Red controlada

Este tipo de red es toda aquella que se encuentra bajo el control del departamento TI institucional.

Red en ámbito protegido

Este tipo de red se encuentra bajo la conceptualización de la red controlada, pero adiciona componentes criptográficos.

Estos componentes de criptografía punto a punto se consiguen mediante la configuración de VPNs.

VPN (Virtual Private Network)

Esta configuración brinda beneficios para los administradores de TI ya que permite una administración centralizada evitando abrir accesos a cada una de las aplicaciones con sus consiguientes riesgos de ataque y sus controles de seguridad.

Otra de las bondades de las redes VPN radica en su robustez y seguridad, para que utilicen autenticación fuerte de doble factor el cual consiste en combinar certificados de seguridad con una autenticación mediante contraseña. (Andrés, 2015.)

Seguridad de la Información

La seguridad de la información es el conjunto de medidas técnicas, organizativas y legales que permiten a las instituciones asegurar la confidencialidad, integridad y disponibilidad de su sistema de información la definición brindada por el estándar para la seguridad de la información ISO/IEC 27001, aprobado y publicado en octubre de 2005 por la ISO (International Organization for Standardization) y por la comisión IEC (International Electrotechnical Commission).

Al establecer los controles de la familia de la norma NTC-ISO/IEC ISO27000 permite asegurar el activo más importante de una organización como lo es la información. (Andrés, 2015.)

Copias de seguridad

En el entorno de teletrabajo no se aplican mejores prácticas en respaldar la información.

El método de backup, varía de acuerdo con la forma de teletrabajo:

- Escritorios remotos
- Perfil móvil, o sincronización automática, mediante software
- Sincronización manual.
- Copias de seguridad offline

Sistemas de almacenamiento en línea

Andrés, (2015.) hace mención que los múltiples proveedores de almacenamiento en línea; entregan beneficios en la portabilidad, disponibilidad de la información en diferentes dispositivos, control de versiones, acceso controlado a otros usuarios, suprimiendo el uso de medios extraíbles, el software de sincronización viene incluido en la mayoría de los sistemas operativos. A pesar de todos los beneficios, se deben considerar los peligros de este tipo de almacenamiento.

- Valorar el tipo de información que será guardada en los almacenamientos en línea ya que si la plataforma es vulnerable a un ataque podría ser posible acceder a la información por terceros.
- La información puede ser accedida por los funcionarios de la institución o gobierno donde se encuentre alojada la plataforma.

- El cifrado de la información es delegada a la plataforma de almacenamiento lo cual no permite tener control sobre esto.
- La información almacenada en sistemas en línea puede incurrir en incumplimientos de normativas o leyes de protecciones de datos.
- No descuidar los contratos de prestación de servicio que ofrecen estas plataformas ya que no siempre se comprometen a garantizar la disponibilidad de la información, pudiendo tener fallos técnicos que les dejen sin conectividad durante días, o pudiendo llegar al extremo de cerrar por temas legales con el país donde se aloja la plataforma

Seguridad del Talento Humano

Andrés, (2015.) en su investigación indica que el talento humano quizá es el eslabón más crítico al momento de garantizar las tres características de la seguridad de la información: integridad, confidencialidad y disponibilidad, por lo tanto, deben adoptarse controles y prácticas de gestión que ayuden a mitigar el impacto de los riesgos que por este factor se pudieran materializar. Uno de los pilares básicos de la norma ISO 27001 es la seguridad sujetada a los recursos humanos, que debe enfocarse desde la definición de las funciones y los recursos hasta la finalización de la relación laboral, y en el desarrollo normal de sus funciones.

Con la definición de sus funciones a desempeñar se asegura que todo el recurso humano en el modo de teletrabajo de la institución entienda sus responsabilidades y estén en las condiciones para desarrollarlos; de esta forma se pueden reducir riesgos de fraude y uso inadecuado de los activos de información de la institución.

Es necesario establecer los procedimientos para garantizar que el retiro de la institución por parte del recurso humano sea controlado para garantizar la devolución de todo el equipamiento y la eliminación de las credenciales de acceso a los sistemas.

Lo más recomendable es remover, en primer lugar, el acceso a los sistemas institucionales, incluyendo las cuentas de correo electrónico para garantizar que no se extraiga información confidencial, respetando las consideraciones de privacidad que apliquen.

Todo lo relacionado con la finalización de contrato debería estar formalizado para incluir el retorno previo del software, documentos institucionales, equipos, dispositivos móviles, tarjetas de acceso e información guardada en medios electrónicos.

Ingeniería social

En la actualidad la ingeniería social es uno de los métodos más utilizados para tratar de vulnerar la seguridad de las personas, se logra por medio de manipulación psicológica y habilidades sociales con el objetivo de obtener algún tipo de información sensible o útil de la institución o empleado.

La ingeniería social tiene diversas formas de actuar:

- Técnicas Pasivas: Basadas en observar y analizar a los empleados, permitiendo crear un perfil psicológico que permite abordar al empleado.
- Técnica no presencial: Se emplea medios de comunicación como teléfono, correo electrónico.
- Técnica presencial no agresiva: Mediante el seguimiento, vigilancia de domicilios, búsqueda en la basura del empleado con el fin de recolectar la mayor cantidad de información.
- Técnicas activas: Mediante la suplantación de identidad, personalizaciones de otros empleados y presión psicológica

Como menciona, Andrés, (2015.) Para implementar defensas ante amenazas de ingeniera social se debe tener en cuenta los siguientes parámetros:

- Diseñar y efectuar políticas de seguridad las cuales deben darse a conocer a los funcionarios donde ellos adquieran el conocimiento y compromisos por parte de ellos.
- Las campañas de concienciación son muy importantes mediante aprendizaje estructurado, reuniones menos formales, campañas con pósteres u otros eventos para anunciar las directivas de seguridad. Cuanto más refuerce los mensajes de sus directivas, más exitosa será su implementación.
- Deben existir protocolos reactivos en los procedimientos relacionados con la directiva de seguridad, registrando los posibles ataques de ingeniería social para prevenir posibles ataques.

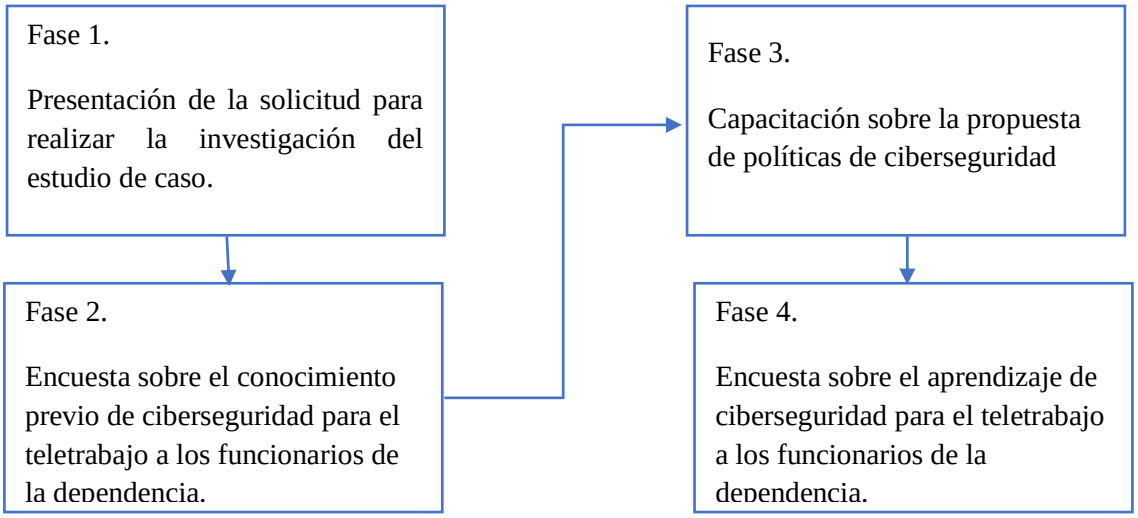
Si las propuestas de seguridad afectan negativamente a la agilidad laboral de la institución, es probable se deba evaluar el riesgo. Se debe lograr un equilibrio entre la seguridad y la operatividad.

Estudio de caso

Este artículo se basa en la investigación de estudio de caso que, según Mertens (2010); un grupo de personas es visto y analizado como una entidad, así como sostiene Yin (1994), el estudio de caso es una indagación profunda sobre un fenómeno contextualizado en el mundo real, en este contexto el grupo de estudio fue el personal administrativo que labora en la oficina del Rectorado de la ESPOCH (6 personas), donde se efectuó a cada uno de ellos una encuesta de 18 preguntas.

Para el desarrollo del trabajo de investigación se destacan 4 fases que a continuación se resumen en el siguiente gráfico.

Figura. 1: Fases de la Investigación.



El Dr. Rector de la ESPOCH con la propuesta de investigación, dando su aprobación para realizar la misma.

Fase 2. Para la toma de muestras iniciales se realizó la encuesta de 18 preguntas enfocadas en 4 aspectos que son: Equipos de Cómputo y Sistemas Operativos, Comunicaciones, Seguridad de la Información y el Talento Humano todo en torno a la temática de ciberseguridad y teletrabajo a los 15 días del mes de marzo del 2021.

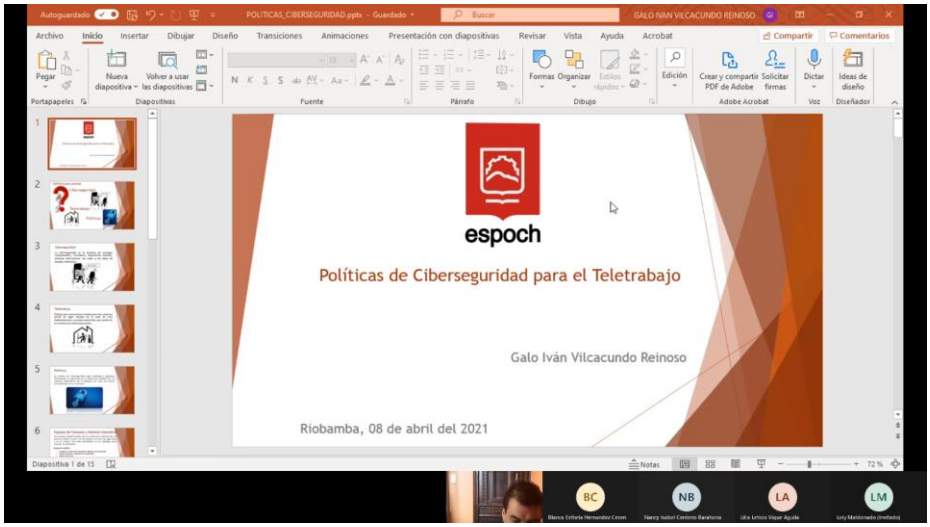
Fase 3. Se promocionó el evento de capacitación por medio del portal web *CiberSeguridad*. (2021, abril), donde se mostró definiciones sobre ciberseguridad, teletrabajo y la temática de capacitación, y en la misma web los funcionarios de esta dependencia se inscribieron para recibir la preparación, página que se encuentra activa desde el 01 de abril de 2021. En la Figura 2 se muestra parte de la web en mención.

Figura. 2: Portal web

Fuente: (*CiberSeguridad.*. 2021, abril)

La capacitación se llevó a cabo en 2 días, 8 y 9 de abril de 2021, que, por causas de la pandemia, se lo realizó por la plataforma virtual Microsoft Teams donde se desarrollaron los temas propuestos en la Fase 2, contando con la aceptación de los funcionarios del rectorado de la ESPOCH, como se observa en la Figura 3.

Figura. 3: Capacitación vía Microsoft Teams Políticas de Ciberseguridad.



Fuente: Autores

Fase 4. Se utiliza la misma encuesta de la fase 2 para recolectar las muestras finales y poder realizar el análisis, esta encuesta se la realiza el viernes 25 de abril de 2021.

El enfoque aplicado en la investigación es cuantitativo, y se utilizó la escala de Likert para dar una valoración a las respuestas obtenidas en las encuestas previa y post capacitación, como se muestra en la tabla 1.

Tabla 1: Escala de Likert para valoración del Test

ITEM	PUNTAJE
TOTALMENTE DE ACUERDO	5
DE ACUERDO	4
INDECISO	3
EN DESACUERDO	2
TOTALMENTE EN DESACUERDO	1

Fuente: Autores

En la Tabla 1 se puede apreciar que el puntaje máximo asignado es de 5 y el puntaje mínimo es de 1, estos valores se aplicaran a cada pregunta según como respondan los participantes de la encuesta.

Resultados

Partimos de la pregunta ¿La Selección y/o creación de políticas adecuadas de ciberseguridad para el teletrabajo, permite el uso adecuado de la información del Rectorado de la ESPOCH?, misma que para el efecto de análisis la plantearemos como la hipótesis alternativa.

Mientras que la Hipótesis nula ¿La Selección y/o creación de políticas adecuadas de ciberseguridad para el teletrabajo, NO permite el uso adecuado de la información del Rectorado de la ESPOCH?

Para determinar si esta hipótesis alternativa es viable se realizó una encuesta preliminar (Pre-Test) y la misma encuesta después de socialización de Políticas de Ciberseguridad para el Teletrabajo (Post-Test) a los 6 funcionarios del Rectorado de la ESPOCH, los resultados arrojados en esta son los que se detallan continuación.

Tabla 2: Resultados del Pre-Test.

PRE-TEST																				
CASO	**P 1**	**P 2**	**P 3**	**P 4**	**P 5**	**P 6**	**P 7**	**P 8**	**P 9**	**P 10**	**P 11**	**P 12**	**P 13**	**P 14**	**P 15**	**P 16**	**P 17**	**P 18**	**T P**	**P M**	**%**
1	3	4	3	5	3	3	5	3	3	3	4	3	5	3	3	3	3	5	64	90	0,71
2	3	4	5	4	3	4	3	4	3	4	4	4	4	4	3	3	4	4	67	90	0,74
3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	1	4	5	85	90	0,74
4	5	3	5	5	5	5	5	3	5	3	5	5	4	4	4	3	5	5	79	90	0,88
5	3	4	4	5	3	5	4	3	3	4	5	5	5	5	5	4	5	5	77	90	0,86
6	2	3	3	3	2	3	3	3	3	3	3	4	3	3	3	3	3	3	53	90	0,59

Fuente: Autores

En la Tabla 2 se puede observar los puntajes obtenidos de cada una de las preguntas de la encuesta (P1 hasta P18) antes de realizar la capacitación, donde TP es el puntaje total obtenido de la suma de los valores de cada una de las preguntas, PM es el valor máximo que se puede obtener de la suma de los valores de las preguntas (caso ideal), asumiendo que, en todas estas se escogió la opción "Totalmente de acuerdo" (5P), el porcentaje (%) aparece de la división entre TP y PM.

Tabla 3: Resultados del Post-Test

POST-TEST																				
CASO	**P 1**	**P 2**	**P 3**	**P 4**	**P 5**	**P 6**	**P 7**	**P 8**	**P 9**	**P 10**	**P 11**	**P 12**	**P 13**	**P 14**	**P 15**	**P 16**	**P 17**	**P 18**	**T P**	**P M**	**%**
1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90	90	1
2	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	88	90	0,98
3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90	90	1
4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90	90	1
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90	90	1
6	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	90	90	1

Fuente: Autores

En la Tabla 3 se puede observar los puntajes obtenidos de cada una de las preguntas de la encuesta (P1 hasta P18) después de realizar la capacitación, donde TP es el puntaje total obtenido de la suma de los valores de cada una de las preguntas, PM es el valor máximo que se puede obtener de la suma de los valores de las preguntas (caso ideal), asumiendo que, en todas estas se escogió la opción "Totalmente de acuerdo" (5P), el porcentaje (%) aparece de la división entre TP y PM.

Tabla 4: Análisis descriptivo

ANALISIS DESCRIPTIVO							
GRUPO	**CASOS**	**PROM**	**MED**	**DESVIACIÓN ESTANDAR**	**VARIANZA**	**MIN**	**MAX**
PRETEST	6	79%	74%	11%	1%	59%	94%
POST-TEST	6	99,6%	100%	0,8%	0,006%	97,8%	100%

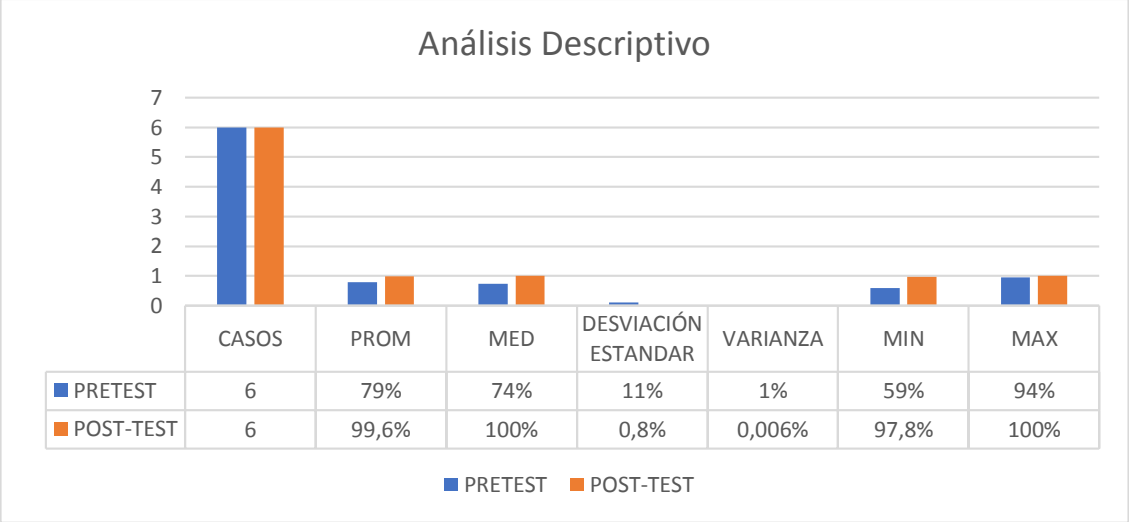
Fuente: Autores

En la Tabla 4 se puede observar el Análisis Descriptivo del Pre-Test y Post-Test en donde podemos resaltar los valores obtenidos de la desviación Estándar en el Pre-Test es del 11% indicando que existe

mayor dispersión en las mediciones, y que, en cambio en el Post-Test es mucho menor con tendencia a 0 con un 0,8% de dispersión.

Al observar los valores mínimos y máximos, en el Pre-Test se encuentra entre el 59% y el 94% notando de mejor manera esta dispersión en las muestras, mientras que en el Post-Test estos valores se encuentran entre el 97,8% y el 100% mostrando una mayor precisión de la muestra y con menos dispersión de estas.

Figura. 3: Histograma del Análisis descriptivo.



Fuente: Autores

Para el análisis estadístico se utilizó el análisis inferencial, ya que, provee elementos que permiten la evaluación sistemática y eficiente de una muestra de población del estudio. La prueba de rangos con signo de Wilcoxon fue el utilizado para dicho análisis, ya que se comparó los resultados obtenidos de las encuestas del Pre-Test y Post-Test y no cumple con el supuesto de normalidad, siendo la alternativa no paramétrica del método t de Student para muestras relacionadas y además que la muestra de población es pequeña, 6 casos, indicando que no es una distribución normal de las muestras obtenidas. En la siguiente tabla se muestra los valores calculados.

Tabla 5: Prueba de rangos con signo de Wilcoxon

DIFERCIA PRE-TEST Y POS-TEST	VALOR ABSOLUTO	RANGOS
-26	26	5
-21	21	4

-5	5	1
-11	11	2
-13	13	3
-37	37	6

Fuente: Autores

Primero se calculó la diferencia de los valores obtenidos entre el PT de los datos obtenidos del Pre y Post Test, también se muestran los valores absolutos de las diferencias encontradas, y el rango al que pertenece cada valor.

Tabla 6: cálculos de valores preliminares

CALCULO DE VALORES PRELIMINARES	
CASOS (n)	6
SUMA DE RANGOS POSITIVOS	0
SUMA DE RANGOS NEGATIVOS	21

Fuente: Autores

La finalidad de encontrar los rangos fue para obtener la suma de estos con respecto al signo que se obtiene de las diferencias y continuar con los cálculos posteriores.

Observemos los valores de la siguiente tabla.

Tabla 7: Resultados de la prueba de rangos con signo de Wilcoxon

Estadístico (W)	0
Z(cal)=	-2,201398157
NIVEL DE SIGNIFICANCIA	0,05

Fuente: Autores

En la tabla 7 se muestran los valores del estadístico W, del valor Z calculado y el nivel de significancia con el que se trabajó en este análisis.

De donde se obtuvo un valor crítico y un P valor mostrados en la siguiente tabla

Tabla 8: Valor crítico y P Valor de la prueba de rangos con signo de Wilcoxon

RESULTADOS	
VALOR CRITICO	1,96
P VALOR	0,0139

Fuente: Autores

Al arrojar en los cálculos un valor crítico de 1,96 y un P valor de 0.0139 se puede decir que la hipótesis nula es rechazada, dando paso a que la hipótesis alternativa es viable.

Las diferencias estadísticamente son significativas, tomando en cuenta que el personal encuestado tiene cierto conocimiento previo en seguridad de la información no de una forma técnica, pero si en nociones básicas del tema.

Discusión y conclusiones

En el análisis realizado se demuestra una diferencia significativa del antes y después en reflejado en el P Valor, donde, este es menor al valor de significancia demostrando la propuesta de políticas de ciberseguridad para el teletrabajo permite el uso adecuado de la información del Rectorado de la ESPOCH.

Luego de haber aplicado la propuesta de políticas de ciberseguridad para el teletrabajo en el Rectorado de la ESPOCH, se puede afirmar que los funcionarios de esta dependencia se vuelven menos vulnerables a posibles ataques cibernéticos.

En el análisis de resultados se observa que los valores obtenidos en el pretest son altos, al observar la valoración dada para los ítems se nota que el valor asignado para “indeciso” es de 3 y este, al ser el más escogido en la encuesta previa en las preguntas planteadas, hace que los valores obtenidos sean altos, a más de un conocimiento previo referente a seguridad de la información, no evita que la propuesta sea viable.

Las prácticas de políticas orientadas a ciberseguridad para el teletrabajo han hecho que los funcionarios del Rectorado de la ESPOCH conozcan de los riegos que conlleva el teletrabajo y las formas que se pueden evitar posibles ataques y la pérdida de la información de esta dependencia.

Si bien las políticas de ciberseguridad para el teletrabajo están bajo la norma ISO/IEC 27001, estás no están complementadas con las buenas prácticas o controles establecidos en la norma ISO/IEC 27002 siendo una limitante en este estudio.

Referencias

1. Adeva, A., & Ortiz, J. M. V. (2020). Teletrabajo seguro, el catalizador digital de la transformación socioeconómica. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 29(140), 62-63.
2. Andrés, B. G. C. (s. f.). SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN EMPRESAS PRIVADAS EN COLOMBIA. 5.
3. Arroyo, S. C. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente(*). 43.
4. Ballestero, F. (2020). La ciberseguridad en tiempos difíciles. Boletín Económico de ICE, 3122. https://doi.org/10.32796/bice.2020.3122.6993
5. BID - OEA, B.-O. (2020). CIBERSEGURIDAD. Reporte de ciberseguridad 2020. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
6. Carrillo, J. J. M., Zambrano, N. A., Zambrano, T. J. L., & Bravo, M. Z. (2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. Revista Ibérica de Sistemas e Tecnologias de Informação, (E29), 41-50.
7. CiberSeguridad. (2021, abril). Ciberseguridad y Teletrabajo. https://ciberseguridad.siscomelectric.com
8. Cifuentes-Leiton, D. M., & Londoño-Cardozo, J. (2020). Teletrabajo: El problema de la institucionalización. Telecommuting: The problem of institutionalization. 9.
9. COVID-19: cronología de la actuación de la OMS. (2020, 28 abril). OMS. https://www.who.int/es/news/item/27-04-2020-who-timeline---covid-19
10. Gayo, M. R. (2021). Ciberseguridad en el Trabajo en Movilidad ya Distancia (Teletrabajo). Revista Derecho social y empresa, (14), 6.
11. International Labour Office, ILO Office in Argentina, Argentina, Ministerio de Trabajo, E. y S. S., & Unión Industrial Argentina. (2011). Manual de buenas prácticas en teletrabajo. OIT.
12. Kaspersky, K. (2021). Lider en seguridad. Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
13. Lema, L. L. (2020). La gestión de la información durante etapas de teletrabajo en la época de la COVID-19. P erspectivas, (3).

14. Martín, F. A. (2020). Ciberseguridad en tiempos de pandemia: repaso a la COVID-19. Análisis del Real Instituto Elcano (ARI), (67), 1.
15. Mertens, D.M. (2010). Research and evaluation in education and psychology: integrating diversity with quantitative, qualitative, and mixed methods. (3rd ed.). Thousand Oaks, CA: Sage Publications.
16. Padilla, R., Cadena, S., Enríquez, R., Córdova, J., & Llorens, F. (2017). Uetic, 1–93. Retrieved from https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/ UETIC_2017.pdf
17. Rodríguez, D. R., & de, M. (s. f.). Teletrabajo, acceso a Internet y apoyo a la digitalización en el contexto del Covid-19. 19.
18. Wilcoxon, Frank (Dec 1945). "Individual comparisons by ranking methods". Biometrics Bulletin. 1 (6): 80–83
19. Yin, Robert K. (1994). Case Study Research: Design and Methods. Sage Publications, Thousand Oaks, CA.