ARTICULO DE INVESTIGACIÓN

ESTRATEGIA METODOLÓGICA PARA MINIMIZAR RIESGOS DE FUGA DE INFORMACIÓN EMPRESARIAL EN TELETRABAJO

ELABORADO POR:

LORENA ISABEL VIANCHA ACERO
NIXON FERNEY SARMIENTO GAMEZ

PRESENTADO AL:

DOCTOR JAVIER FERNADO KLAUS

UNIVERSIDAD SANTO TOMAS

FACULTAD DE CIENCIAS ADMINISTRATIVAS

ESPECIALIZACIÓN EN AUDITORÍA Y ASEGURAMIENTO DE LA INFORMACIÓN

TUNJA,2021

Estrategia metodológica para minimizar riesgos de fuga de información empresarial en teletrabajo

Autor (es):

Resumen:

El presente trabajo de investigación es un estudio de campo, tipo cualitativo documental, que aplicando como técnica el estudio de caso, genera una propuesta de una “Estrategia metodológica para minimizar los riesgos de fuga de información empresarial en teletrabajo”. Dicha propuesta siguió los procesos de identificación y análisis de los temas de riesgos cibernéticos, fuga de información en una empresa, dominio de redes y aplicaciones tecnológicas; de tal manera que cualquier empresa que requiera una capacitación sobre esos temas, tome en cuenta la estrategia y la importancia del desarrollo de la misma en la empresa, para así prevenir o atacar alguna problemática que se pueda presentar al respecto, sobre todo porque hoy día, debido a la situación mundial que ha generado la pandemia Covid 19, las empresas se valen mucho de las herramientas, recursos, aplicaciones y programas tecnológicos para que el trabajo no pare y el desempeño laboral resulte eficiente.

Palabras claves: riesgos cibernéticos, fuga de información y teletrabajo.

Abstract:

The present research work is a field study, qualitative documentary type, which, applying the case study as a technique, generates a proposal for a "Methodological strategy to minimize the risks of business information leakage in teleworking". Said proposal followed the processes of identification and analysis of cyber risk issues, information leakage in a company, domain of networks and technological applications; in such a way that any company that requires training on these issues,

takes into account the strategy and the importance of its development in the company, in order to prevent or attack any problem that may arise in this regard, especially since today Due to the global situation that has generated the Covid 19 pandemic, companies make great use of the tools, resources, applications and technological programs for non-stop work and efficient work performance.

Keywords: cyber risks, information leakage and teleworking.

Introducción:

En una era de múltiples complejidades las organizaciones han iniciado la migración de sus operaciones a un proceso alterno basado en la colaboración remota y de espacios virtuales. De allí que, la fuga de información se ha convertido en una causa importante de fraude en las empresas, por lo que garantizar la protección de la información por ciberataques ha sido una necesidad en los últimos tiempos, más ahora que se vive en un contexto particular, donde se debe dar respuesta de manera activa tanto a los riesgos de ciberataques como a los de salud, implícitos por la pandemia relacionada al COVID-19 (Valero-Pacheco & Riaño-Casallas, 2020).

Planteamiento del Problema:

El Instituto Nacional de Ciberseguridad de España, en su guía de aproximación para el empresario titulada “Ciberseguridad en el teletrabajo” emitida en el 2020, define el teletrabajo como *“una actividad laboral que se desarrolla desde otros lugares que no sean las propias instalaciones de la institución, por medio de un sistema de telecomunicación” (pág. 4)*, es decir, que es el trabajo que realizan los empleados desde otros sitios alejados de la empresa, pero utilizando las herramientas tecnológicas que tengan disponibles, como computadoras, Tablet, teléfonos inteligentes, entre otros.

Para algunas organizaciones, el teletrabajo era una herramienta desconocida o poco usada, por el temor de que la información saliera de su entorno. No obstante, el constante avance de la tecnología ha hecho que estas organizaciones minimicen su resistencia a este cambio. En la actualidad, el problema de confinamiento, debido al Covid-19, ha convertido el teletrabajo en una herramienta esencial y de suma importancia para la continuidad de las actividades bajo un mundo virtual.

En la misma guía mencionada anteriormente, se señala que:

> El teletrabajo se ha desarrollado de forma vertiginosa en los últimos meses como consecuencia del COVID-19. Para muchas empresas se ha convertido en una modalidad esencial para la continuidad de su negocio. Su uso debe hacerse respetando una serie de medidas de seguridad si no se quiere ser víctima de un incidente de seguridad que ponga en riesgo la continuidad de la empresa. (2020:)

La disposición del teletrabajo, ha generado el surgimiento de ciberataques, aprovechándose del contexto donde se labora, situación que produce inseguridades cibernéticas, que ponen en duda las capacidades de protección de información.

Tal situación, ha hecho que países como España pongan a disposición de las empresas españolas su plataforma de evaluación e identificación de riesgos cibernéticos (CYQu o Cyber Quotient Evaluation), con el fin de hacer frente a los numerosos ciberataques surgidos en esta época de pandemia (NOA, 2020). Colombia no escapa de ello, el Cuarto Estudio de Penetración del Teletrabajo en Empresas Colombianas, (2018), reseña un crecimiento constante “pasando de 31.553 en el 2012 a 122.278 este año. Además, triplicamos el número de empresas que implementan esta modalidad, al pasar de 4.292 a 12.912 en el mismo periodo” (Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC, 2018, p. 15).

Este crecimiento acelerado, ha traído dificultades para las organizaciones, relacionadas con la dificultad de supervisar los riesgos en el entorno del teletrabajador, los medios para el diagnóstico de condiciones de salud, la

implementación de controles, los procesos de reintegro laboral y el seguimiento a los resultados (Valero-Pacheco & Riaño-Casallas, 2020).

Mucho más allá de esta problemática, en el último año han aumentado los problemas relacionados con riesgos cibernéticos y fuga de información tanto para la empresa como para el usuario particular, lo que conlleva a consecuencias como la inseguridad en la filtración de datos de información que supone debe estar protegida (Abril Martínez, 2019). Lo que trae como consecuencia la necesidad de implementar estrategias, normas y capacitaciones tendientes a proteger esta problemática.

Por su parte, García F. (2020) en el informe de SAFE, titulado “Incidencia del Covid-19 en las tendencias del cibercrimen 2020” plantea que:

> En Colombia la dinámica del cibercrimen durante el 2020 utilizó como vector de infección la preocupación e incertidumbre derivada de la cuarentena y el aislamiento, así como la necesidad de las empresas para generar nuevos entornos de trabajo desde la virtualidad (p. 16).

Todo eso, para que las empresas, aún cuando asumieran el confinamiento obligatorio, no dejaran de laborar, puesto que las empresas igual debían producir y optimizar el trabajo, bien sea con la ayuda de la tecnología requerida y con el esfuerzo de sus empleados.

Sin embargo, muchas empresas no garantizaron la seguridad de la información de la información y la labor y por lo tanto, se produjo una oleada importantísima de ciberataques.

Al respecto, García F. (2020) plantea que

> Las cifras de denuncias por ciberataques exitosos durante el denominado periodo COVID, es decir entre marzo y diciembre, registró un incremento superior al 101% con más de 37 mil reportes de noticias criminales instauradas ante la Fiscalía General de la Nación. El

> consolidado final de Ciberdelitos desde enero a diciembre 2020 ascendió a más de 45.104 casos, lo que supone un incremento neto del 89%, siendo el año de mayor crecimiento en cifras e impacto de ciberdelincuencia en Colombia, desde la existencia de la ley de delito informático (p. 16).

Eso quiere decir que, en los últimos tiempos de pandemia, la mayoría de las empresas colombianas fueron víctimas de ciberataques, como suplantación de sitios web para robar información personal de las empresas corporativas, exposición de datos importantes de las empresas en el internet y hasta estafas bancarias importantes por medios informáticos; convirtiéndose la ausencia de estrategias de capacitación en uno de los facilitadores del actuar de ciberatacantes.

Objetivo General:

Diseñar una propuesta de estrategia metodológica de capacitación en ciberseguridad, usando los espacios virtuales (intranet) en teletrabajo y definiendo un Plan de Capacitación organizacional para la prevención de los Ciber riesgos derivados del Teletrabajo.

Objetivos específicos

- Identificar los riesgos cibernéticos a los que están expuestas las organizaciones en teletrabajo.
- Analizar los riesgos de fuga de información empresarial en teletrabajo.
- Elaborar la estrategia metodológica de capacitación.

Justificación de la investigación:

Ante la creciente vulnerabilidad de la gestión de riesgos dentro de las organizaciones, asociados a la seguridad de la información y salud en el teletrabajo, y dada la actual normatividad vigente es primordial que las empresas asuman estrategias de capacitación en ciberseguridad, usando los espacios virtuales (intranet) de la misma empresa, con el fin de minimizar los riesgos de fuga de información empresarial en teletrabajo.

El presente trabajo de investigación responde a la necesidad de identificar los factores que afectan la Ciberseguridad y la importancia del estudio del teletrabajo, el cual ha sido definido por la Organización Internacional de Trabajo -OIT- como:

Una forma de trabajo en la cual:

a) el mismo se realiza en una ubicación alejada de una oficina central o instalaciones de producción, separando así al trabajador del contacto personal con colegas de trabajo que estén en esa oficina.

b) la nueva tecnología hace posible esta separación facilitando la comunicación (OIT, 2011). Apegados a este lineamiento rector, en Colombia, el teletrabajo se encuentra establecido en la Ley 1221, de fecha junio de 2008, la cual expone: Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo". (Artículo 2, 2008).

Visto lo anterior el presente trabajo se justifica porque no existe actualmente un estudio comprehensivo respecto a los riesgos identificados durante la pandemia COVID 19 y que están directamente asociados al Teletrabajo y menos un trabajo

investigativo, que, a partir de ese estudio, genere un plan de capacitación basado en la sensibilización de los usuarios (internos) y terceras partes involucradas en la interacción de la empresa.

Finalmente, la proliferación avanzada que ha tenido el cibercrimen en Colombia, motiva las empresas a mejorar su modalidad de trabajo y también sus modelos de ciberseguridad, por lo que la presente investigación propone un modelo de capacitación para que los teletrabajadores cumplan con su labor eficientemente y sin riesgos.

Aspectos teóricos:

Descripción histórica de los riesgos cibernéticos:

Las amenazas cibernéticas y los ataques continúan creciendo en número y complejidad - todo mientras el mundo de los negocios crece cada vez más conectado y digital. En medio de este nuevo paisaje, la gestión de las amenazas cibernéticas se convierte en un imperativo empresarial y estratégico, con estándares más altos que nunca. Hoy en día, el delito cibernético involucra más que el fraude y el robo.

Con la presencia de extensas redes criminales, los hackers extranjeros patrocinados por gobiernos y los terroristas cibernéticos, el crimen cibernético se extiende a través del espectro de riesgo que involucra; la interrupción de los servicios, la corrupción o la destrucción de datos, e incluso actividades que buscan extorsionar solicitando dinero, acceso o secretos corporativos de las víctimas.

El riesgo cibernético es un imperativo para todos dentro de la empresa, pero la responsabilidad misma de supervisar el riesgo recae en los principales líderes. La gestión eficaz del riesgo cibernético empieza con la conciencia de la junta y la alta gerencia. Perfeccionar su capacidad de comprender el riesgo, gestionar el rendimiento y acercar su organización a la madurez cibernética a menudo inicia con la respuesta a preguntas importantes - y como resultado su negocio debe convertirse en más seguro, vigilante y resiliente.

Todas las anteriores cuestiones son críticamente importantes hoy - aunque tradicionalmente la gestión cibernética se ha centrado en “ser seguro” mientras se presta menos atención en “ser vigilante” (monitoreando exhaustivamente el extenso panorama de amenazas) y “ser resiliente” (respondiendo y recuperándose de los ataques).

En los últimos 30 años, los gobiernos, las empresas y los ciudadanos se han vuelto críticamente dependientes del Internet y de las tecnologías de la información y las comunicaciones (TIC), no obstante, existen países y empresas que a pesar de los cambios tecnológicos y la digitalización comercial en la cual están inmersos, aún presenta debilidades, tales como:

- Escaso nivel de concienciación por parte de directivos-empleados.
- Débil implementación de políticas de ciberseguridad.
- Priorización de otros riesgos por encima del cibernético.
- Obsolescencia tecnológica en las plataformas.
- Descoordinación entre las áreas de seguridad física y tecnológica.
- Exposición de información sensible empresarial en internet.
- Desconocimiento del actual nivel de riesgo de la compañía.
- Inexistencia de un estudio del estado actual de la ciberseguridad de la empresa.
- Estructuras organizativas desactualizadas o inexistencia de áreas, cargos y responsabilidades frente a la ciberseguridad (Bautista García, p. 62).

Se tiene la creencia que siempre funcionarán los servicios esenciales para el ciudadano, como la energía y las telecomunicaciones, y que los bienes, servicios, datos y capital cruzan fronteras sin inconvenientes. La realidad, sin embargo, es que muchos sistemas e infraestructuras en red son vulnerables y están siendo explotados. Por su parte, Hathaway M. (2018), en su artículo *Gestión del Riesgo Cibernético Nacional,* editado por la Organización de Estados Americanos (OEA):

> Organizaciones de todo tipo están sufriendo mayores violaciones a sus datos, actividad criminal, interrupción del servicio y destrucción de su propiedad.

> Colectivamente, nuestra inseguridad está creciendo. Más de 100 países y un número cada vez mayor de actores y personas no estatales pueden causar daños a las infraestructuras en red de gobiernos y de la industria.
>
> Los objetivos varían según el actor, desde: el activismo político; fraude y delito informático; robo de propiedad intelectual (PI); espionaje; interrupción del servicio; y destrucción de bienes y activos.
>
> Los países y las empresas están viviendo en un mundo de inseguridad cibernética: todos los gobiernos, empresas y personas están enfrentando riesgos cibernéticos. Y todos comparten un nivel de responsabilidad en su gestión. Como lo evidencian eventos recientes, los países y las empresas deben primero comprender que en el centro de su estrategia y agenda digital debe estar un enfoque disciplinado de gestión de riesgos. El riesgo de inacción es demasiado grande (p. 5).

Por lo tanto, existe una necesidad urgente de organizaciones internacionales e instituciones académicas en crear procesos efectivos para maximizar la gestión de riesgos cibernéticos y puedan abordar en los diversos los riesgos digitales, todo ello, bajo el marco de las tecnologías de información comercial, que hoy día están dadas a aportar una mayor productividad, altos niveles de eficiencia, minimizan los costos de capital, almacenamiento y procesamiento de datos, y como consecuencia generan un alto crecimiento en los resultados.

Con base a lo anterior, es importante destacar lo planteado por Bautista García (2019):

> Los cibercriminales se han convertido en una de las principales amenazas a la seguridad empresarial en el mundo, y las pérdidas derivadas de los ciberataques ya superan las generadas por los riesgos tradicionales, como fraudes internos o incluso eventos inesperados, como son los desastres naturales. La tendencia y el comportamiento de estas estructuras delictivas demuestran el alto nivel de sofisticación y, por ende, la tasa de éxito con la que consiguen vulnerar la seguridad de las empresas crece anualmente (p. 60).

Razón a ello, se puede observar que ningún país o empresa está exento del riesgo cibernético, por lo que se debe tener en cuenta un enfoque de gestión de riesgos, bajo principios de responsabilidad, justicia y disciplina, los cuales permitirán reducir la problemática de inseguridad en ciberentornos empresariales.

Colombia, uno de los países con mayor grado de riesgo cibernético, se ha propuesto, a partir de políticas gubernamentales, evaluar su preparación cibernética y promover la confianza de la sociedad en el uso del entorno digital, frente a esto, se da inicio a una Política Nacional de Seguridad Digital (estrategia nacional de seguridad digital), aprobada en abril de 2016 por el Consejo Nacional de Política Económica y Social (CONPES), mediante la emisión del Documento CONPES 3854 de 2016.

En este sentido, Colombia adoptó la guía de gestión de riesgos de la OCDE, adaptando las recomendaciones de la OEA, la UIT y la Organización del Tratado del Atlántico Norte (OTAN) con el fin de identificar la afectación de los incidentes cibernéticos en las empresa colombianas, incluyendo sector privado como el público, hecho este que hace que el Estado colombiano asuma como una prioridad la actividad cibernética, elemento importante de desarrollo socioeconómico, la digitalización del sector y la transformación digital, lo que permite elevar de la seguridad cibernética a la par de una política de seguridad nacional de un país.

Reducción del riesgo empresarial a través de una planificación cuidadosa

Para corregir las deficiencias y apoyar las futuras prioridades económicas y de seguridad empresarial, con el firme objetivo de cerrar la brecha entre la seguridad cibernética y las capacidades cibernéticas empresariales, es preciso realizar un trabajo en conjunto dentro de la empresa, por tanto, es necesario:

- Elaborar y revisar el plan de capacitación, para incrementar el nivel de seguridad de todo el personal.
- Mantener un registro de asistencia , si es necesario, la

aprobación de cursos y conferencias de concienciación sobre seguridad cibernética, estableciendo una periodicidad que certifique la actualización de empleados de riesgo de TI.

- Verificar la asimilación de los conocimientos adquiridos, mediante la Realización de auditorías internas para todos los empleados.

Estas líneas, direccionan el diseño, implementación, ejecución y retroalimentación de la c

ultura de ciberseguridad, fácilmente aplicada a toda la cadena productiva de la empresa, incluyendo a clientes y los proveedores, por lo que estos se hacen partícipes del cambio.

Por lo que, continuando con Hathaway M. (2018), en su artículo Gestión del Riesgo Cibernético Nacional, editado por la Organización de Estados Americanos (OEA), se toma como base algunas estrategias comunes para mitigar eficazmente el riesgo cibernético:

- Construcción de una sólida cultura de seguridad cibernética. Crear una cultura de seguridad cibernética implica involucrar a todo aquel que hace parte de la empresa y de su seguridad, esto para que cada persona comprenda que sus actividades diarias están en riesgo. Por lo tanto, el gobierno debería iniciar una campaña nacional de pública, promover la educación, la capacitación y el desarrollo de habilidades para una concientización del riesgo que puede tener la información que se maneja y así sean ellos quienes formen parte de la solución.
- Todas la empresas deben apegarse a marcos legales y regulatorios apropiados diseñados por los gobiernos, con el fin de proteger su empresa y al Estado del delito cibernético, la interrupción del servicio y la destrucción de la propiedad.
- Usar las herramientas TIC para aumentar la confianza y la seguridad y minimizar las deficiencias en los procesos y productos.

- Hacer prospectivas tecnológicas con el fin de evaluar nuevas vulnerabilidades y riesgos y visualizar cómo podrían convertirse en oportunidades para brindar seguridad, fiabilidad y resiliencia a sus infraestructuras y activos.

Es necesario para todas las organizaciones, independientemente de su tamaño, valor o recursos, adopten políticas de seguridad que mejoren los procesos internos y ayuden a mitigar el impacto de las fallas de ciberseguridad.

Estas políticas se pueden implementar con la adopción de planes que involucren a los gerentes, al equipo técnico y, en general, a todos los empleados de la organización, incluidos los contratistas y otros sujetos involucrados en la cadena productiva de cada empresa, así como la relación con clientes y proveedores, entre otros.

Definición de términos:

- **El riesgo:** se define en términos de tiempo, cuando algo o alguien está expuesto a un peligro, daño o pérdida.
- **El riesgo cibernético:** Según el Instituto de Gestión de Riesgos (Institute of Risk Management), organismo líder a nivel mundial en todo lo que compete a la gestión de losf riesgos que enfrentan las empresas, el riesgo cibernético se define como cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información. El FSB (2017a) clasifica al cibernético como un riesgo microfinanciero de carácter operativo, debido a que puede surgir de fallas en los sistemas de información, error humano o influencias externas.
- **La seguridad en el trabajo:** es una disciplina técnica que engloba el conjunto de técnicas y procedimientos que tienen por objeto eliminar o disminuir el riesgo de que se produzcan los accidentes de trabajo. Por ello, en este apartado se recogen todos aquellos factores de riesgo relacionados con la seguridad en el trabajo que pueden ocasionar daños a los trabajadores en forma de accidentes de trabajo.

Metodología:

Diseñar una estrategia para un trabajo de investigación, constituye una acción que exige un procedimiento organizado que amerita conocer y determinar lo que se quiere lograr y lo que se tiene que hacer para lograrlo. Es por ello, para el presente estudio, se consideró diseñar una estrategia metodológica que permita la capacitación en ciberseguridad, utilizando los espacios virtuales en teletrabajo.

Dicha estrategia es definida por Chaparro J. y otros (2016) como:

> Camino que hemos de seguir en la investigación, para responder a las preguntas de investigación derivadas de los objetivos específicos y en coherencia con el objetivo general. Todo ello en los marcos del problema de investigación y el contexto mismo de realización del estudio (p. 46).

Por tanto, el diseño de la estrategia metodológica para este trabajo, pretende cumplir con los objetivos planteados, de forma sistemática, tomando en cuenta el contexto y la situación real actualizada. Es decir, para diseñar la estrategia metodológica de capacitación en ciberseguridad, se tuvo que conocer los riesgos cibernéticos y luego analizarlos.

Con base a que la estrategia de capacitación será una propuesta que estará dirigida a una población específica, y que, además, se tomará en cuenta los posibles resultados que se generen de la misma, se consideró que el tipo de investigación que más se adecuaba era el cualitativo, ya que según "Investigación cualitativa". En: *Significados.com*. (2019):

> Es un método de estudio que se propone evaluar, ponderar e interpretar información obtenida a través de recursos como entrevistas, conversaciones, registros, memorias, entre otros, con el propósito de indagar en su significado profundo (p. 4).

El presente estudio evaluó e interpretó información para poder elaborar la estrategia metodológica, aplicando además el método de estudio de casos

porque se estudió la situación tomando en cuenta sus aspectos más importantes según lo que realmente interesaba, que era conocer y buscar la manera de atacar los riesgos cibernéticos en el teletrabajo. ***"Un estudio de casos*** *pretende analizar un problema para identificar sus características y tomar decisiones a partir de allí".* "Investigación cualitativa". (*Significados.com*. 2019)

Asimismo, la técnica utilizada en este trabajo es la de producción y revisión de documentos, los cuales se definen *"como una técnica de Investigación Documental que se centran en todos aquellos procedimientos que conllevan el uso práctico y racional de los recursos documentales disponibles en las fuentes de información".* Rizo J. (2015, p. 3). La propuesta de esta investigación se realizó en base a toda la información recabada de documentos relacionados con el tema.

Informaciones importantes tomadas de García F. (2020) en el informe de SAFE, titulado "Incidencia del Covid-19 en las tendencias del cibercrimen 2020", donde información cifrada de los delitos cibernéticos acaecidos al comienzo de la pandemia, delitos como:

> La suplantación de sitios Web para capturar datos personales con un crecimiento del 303% respecto al 2019 es el delito de mayor incidencia durante el presente año. Este tipo penal tiene una relación directa con modalidades conocidas tales como los ataques de Phishing1, Spoofing2 y Pharming3 que sufrieron las empresas y que utilizaron los cibercriminales para capturar datos personales o dispersar malware en las redes corporativas con 5440 casos denunciados. (Pág. 16)

Otro delito descrito fue:

> la violación de datos personales con un 174% como consecuencia de la filtración y robo de datos con más de 9487 casos registrados, lo que generó un doble impacto que compromete aspectos operativos, así como legales y de cumplimiento por la pérdida de información sensible. (Pág. 16)

Y por último García F. (2020) también describe otro delito cibernético importante como:

> El hurto por medios informáticos con un 37% de crecimiento registró más de 16.654 casos denunciados, pese a tener la mayor frecuencia estadística, la modalidad más común sigue siendo el apoderamiento de credenciales para el acceso a servicios de banca online, con los cuales los cibercriminales, consiguen suplantar al titular del producto bancario y apoderarse del dinero generalmente dispuesto en cuentas bancarias. (Pág. 17)

Tomando en cuenta todas esas cifras, de cibercrimen detectados en Colombia, resulta obligatorio que las empresas fortalezcan sus modelos informáticos adoptados, aplicando las más óptimas estrategias de trabajo que brindan una completa seguridad en el trabajo cibernético que empleen.

A continuación se presenta una propuesta de la estrategia a implementar.

Estrategia Metodológica propuesta:

Título:

"Estrategia metodológica de capacitación en ciberseguridad, usando los espacios virtuales (intranet) en teletrabajo".

Objetivo General:

Diseñar propuesta de estrategia metodológica de capacitación en ciberseguridad, usando los espacios virtuales (intranet) en teletrabajo.

Objetivos específicos

- Identificar los riesgos cibernéticos a los que están expuestas las organizaciones en teletrabajo.
- Analizar los riesgos de fuga de información empresarial en teletrabajo.
- Estudiar los crímenes cibernéticos más comunes acaecidos últimamente en tiempos de pandemia en las empresas de Colombia.

Contenido	Actividad	Recursos	Evaluación	Indicadores	Dimensión
Los riesgos cibernéticos: Historia, definición de cibernética, riesgos, teletrabajo, información, fuga, fuga empresarial. Crímenes cibernéticos. Crímenes cibernéticos más comunes en Colombia últimamente influenciados por la pandemia Covid-19.	Reconocimiento, identificación, análisis y caracterización de todos los elementos que implican los riesgos cibernéticos, organizando y ejecutando un taller informativo, foro, y mesas de trabajo que permitan estudiar y analizar el tema. Identificación y reconocimiento de los Crímenes cibernéticos más comunes en Colombia últimamente influenciados por la pandemia Covid-19.	Salón de sesiones. Video beam. Computador. Material bibliográfico. Personal especializa-do. Informe de SAFE, titulado “Incidencia del Covid-19 en las tendencias del cibercrimen 2020”.	Taller informativo: Trabajo grupal. Foro: Participación. Mesa de trabajo: Producción oral y escrita. Creación y propuesta de nuevos modelos tecnológicos que apliquen la ciberseguridad en el teletrabajo.	Reconocimiento de los riesgos cibernéticos. Identifica y caracteriza todos los elementos de los riesgos cibernéticos en el teletrabajo. Participa activamente en las actividades. Presentación adecuada de las producciones.	Empresarial. Tecnológica y didáctica.

Resultados:

El estudio realizado representa un propuesta para capacitar a personas empresarias o empleados de una empresa que utiliza como herramientas las nuevas tecnologías aplicándolas en el teletrabajo, por lo que la estrategia debe implicar una serie de contenidos y acciones que realmente permitan al participante conocer y dominar los riesgos cibernéticos de fuga de información en el teletrabajo, de tal manera que se generen ideas que más se adecuen a atacar dicha problemática para mejorar el desempeño de la empresa u organización donde labora.

En tal sentido, el presente trabajo ofrece una idea alternativa con acciones pertinentes que se debe desarrollar, para que cualquier empresa tome en cuenta si requiere que sus empleados dominen la temática y no generen problemas de fuga de información empresarial, sino que más bien los aborden o resuelvan.

Conclusiones

Finalmente, respondiendo a los objetivos planteados en esta investigación, es necesario que la propuesta proyectada sea coherente y relevante para que cada participante pueda dominar el tema de riesgos informáticos y fuga de información corporativa en el teletrabajo, teniendo en cuenta la identificación y estudio completo del tema y sus elementos e implicaciones, que luego te permitirán analizar la información y comprenderla para prevenir o solucionar el problema.

Esto nos permite considerar que es imperativo que todos los empleados de las empresas que utilizan las nuevas redes y aplicaciones tecnológicas como sus principales herramientas, estén formados en el tema con el fin de prevenir cualquier tipo de problema laboral que posteriormente pueda tener un impacto económico en las empresas y sus empleados.

Referencias:

Abril Martínez, L.P.; Abril Martínez, M. C.; Abril Martínez, S. C. (2019). Modelo de gestión de seguridad y salud en el trabajo para Teletrabajo autónomo en Colombia. Universidad Santo Tomás e Icontec. Maestría En C alidad Y Gestión Integral. Colombia.

Bautista García, F. (2019). Guía práctica para la ciberseguridad en las empresas colombianas. En *Herramienta de Seguridad para los actores de la Cadena de Suministro. Pautas para la prevención criminal.* Ministerio de Defensa Nacional Policía Nacional de Colombia. Dirección de investigación Criminal e INTERPOL, pp 60-72. Disponible en: https://www.policia.gov.co/sites/default/files/descargables/herramienta_de_seguridad_digital1.pdf

Chaparro J. y otros. (2016). “Análisis y diseño de sistemas de información”. Centro de investigación de ingeniería de sistemas. Venezuela.

García F. (2020). Informe de SAFE, titulado “Incidencia del Covid-19 en las tendencias del cibercrimen 2020”. Recuperado de: https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-entornos-cotidianos-vfene-1.pdf

Hathaway M. 2018. Gestión del riesgo cibernético Nacional. 2ª Edición Whiter papers series. EE. UU.

El Instituto Nacional de Ciberseguridad. “Guía de aproximación para el empresario titulada “Ciberseguridad en el teletrabajo” emitida en España en el 2020. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

"Investigación cualitativa". En: *Significados.com*. Disponible en: https://www.significados.com/investigacion-cualitativa/ Consultado: 6 de junio de 2021.

Financial Stability Board (FSB, 2017b). “Summary Report on Financial Sector Cybersecurity Regulations, Guidan-ce and Supervisory Practices”.

Ley 1221 (2008). Congreso de Colombia. Normas para promover y regular el Teletrabajo. Recuperado de: http://www.desarrolloeconomico.gov.co/sites/default/files/marco-legal/Ley-1221-2008.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones - MINTI (2018). Teletrabajo. Recuperado de: https://teletrabajo.gov.co/622/w3-article-75998.html

NOA. Creating Future Thinking. Recuperado de: https://noa.aon.es/ciberseguridad-teletrabajo-diagnostico-cyber/

OIT. (2011). Manual de buenas prácticas en teletrabajo. 1ra. ed. Buenos Aires, Oficina Internacional del Trabajo, Ministerio de Trabajo, Empleo y Seguridad Social, Unión Industrial Argentina. Recuperado de: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-buenos_aires/documents/publication/wcms_bai_pub_143.pdf

Rizo J. (2015). “Técnicas de investigación documental”. Programa educativo de la Universidad Nacional Autónoma de Nicaragua.

Valero-Pacheco, I. C., & Riaño-Casallas, M. I. (2020). Teletrabajo: Gestión de la Seguridad y Salud en el Trabajo en Colombia. Archivos De Prevención De Riesgos Laborales, 23(1), 22-33. https://doi.org/10.12961/aprl.2020.23.01.03