UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación del dominio “Seguridad de la Información Ligada a los Recursos Humanos” según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTOR:

Carrasco Ramirez, David Agusto (orcid.org/0000-0002-8620-3014)

ASESOR:

Dr. Necochea Chamorro, Jorge Isaac (orcid.org/0000-0002-3290-8975)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento.

LIMA – PERÚ

2022

Dedicatoria

A mis padres, por su amor, valores, sacrificio y esfuerzo para convertirnos en la persona que soy ahora y confiar en mí, y este es el resultado de todo lo que han sembrado.

Agradecimiento

En primer lugar, a Dios, por darme la vida y permitirme cumplir mis objetivos. Al docente, que con sus enseñanzas, consejos, paciencia y tiempo fueron un ejemplo para seguir nuestro desarrollo.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La presente investigación tuvo como objetivo general determinar que la aplicación de la propuesta de estrategias de seguridad de la información según la ISO 27001:2013 mejorará el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A. Fue una investigación aplicada de diseño experimental. La muestra seleccionada fue de 60 colaboradores con cargo de gerente. Los instrumentos para la recolección de datos fueron dos cuestionarios uno para seguridad de la información y otro para recursos humanos, ambos instrumentos fueron validados por expertos y se determinó su confiabilidad a través del Alfa de Cronbach de valor de 0.807 y 0.799 respectivamente. Los resultados indicaron que el 61.7% de los empleados percibieron la concientización de recursos humanos en un nivel medio, y el 83% percibió en nivel alto la seguridad de la información. La comparación de los resultados del pre test y post test del nivel de concientización de los recursos humanos después de haber aplicado la propuesta mostró mejoras en la disminución del nivel bajo de 36.7% a 0% y el aumento del nivel alto de 1.7% a 76.7% lo que indica que las estrategias aplicadas fueron efectivas.

Palabras clave: Seguridad de la información, concientización de recursos humanos, ISO 27001:2013

Abstract

The general objective of this investigation was to determine that the application of the information security strategy proposal according to ISO 27001:2013 will improve the level of awareness of human resources in the company Komatsu - Mitsui Maquinarias Perú S.A. It was an applied research of experimental design. The selected sample was made up of 60 employees with a managerial position. The instruments for data collection were two questionnaires, one for information security and the other for human resources, both instruments were validated by experts and their reliability was determined through Cronbach's Alpha of 0.807 and 0.799 respectively. The results indicated that 61.7% of employees perceived human resources awareness at a medium level, and 83% perceived information security at a high level. The comparison of the results of the pre-test and post-test of the level of awareness of human resources after having applied the proposal showed improvements in the decrease of the low level from 36.7% to 0% and the increase of the high level from 1.7% to 76.7 % which indicates that the strategies applied were effective.

Keywords: Information security, human resources awareness, ISO 27001:2013

I. INTRODUCCIÓN

En 1989 un trabajador de una empresa de seguros situada en Bélgica, recibió un paquete por correo postal, en el cual se encontraba un disquete que prometía contener un informe de la más actual investigación de la OMS sobre el SIDA (Síndrome de Inmunodeficiencia Adquirida), aquel ejecutivo llamado Eddy Willems insertó el disquete en su computadora personal y se llevó una gran sorpresa cuando dio en cuenta que toda su información alojada en el disco C o principal de su computador había sido "secuestrada" por un software malicioso que solicitaba un rescate de 189 dólares para "devolver" su información. Esta persona sin darse cuenta había sido víctima del primer caso de Ransomware del mundo, tal como se ha indicado líneas atrás un Ransomware es un software malicioso que encripta o "secuestra" la información y pide algo a cambio como rescate de esta.

En esa ocasión, tal como el disquete que le llegó a Willems hubieron 20.000 adicionales circulando por todo el mundo, y a pesar de que ahora se puede decir que era "fácil" revertir su efecto en ese momento causó tantos estragos que las fuerzas del orden no tardaron en buscar al o los responsables de este caso. Finalmente se llegó a un investigador, biólogo de Harvard llamado Joshep Popp, que en ese momento era miembro de los investigadores del SIDA de la OMS, aquel personaje se excusó ante las autoridades diciendo que creo el ransomware con la intención de donar el dinero para la investigación contra el SIDA.

Actualmente los ataques por ransomware son infinitamente peores, los atacantes los envían por internet de manera masiva y en muchos de los casos solicitan el "rescate" por medio de cripto-monedas, las cuales complica el rastreo de las transacciones y por ende la identificación de los responsables, que ahora son organizados y verdaderos expertos en seguridad informática, no biólogos que atacan en solitario.

Esto se puede ver reflejado en el WEF 2022 (Informe Global de Riesgos) de Marsh, un bróker de seguros y gestión de riesgos catalogado dentro de los mejores del mundo indicó que a partir del 2020 al 2022 se ha incrementado un 435% los casos de ransomware, indicando también que todos los eventos de ciberseguridad en empresas se derivan en un 95% de errores humanos. Esto nos indica que una de las vulnerabilidades más explotadas por los atacantes de compañías, lejos de

ser algún software desactualizado o hardware mal implementado, son los recursos humanos.

Con esta información, nos podemos preguntar ¿Qué se está haciendo para protegernos de estos ataques? Pues, bien, los esfuerzos de los profesionales de seguridad de la información y ciberseguridad no son en vano. En este proyecto de investigación se explicará el proceso de implementación de controles incluidos en el dominio 7 “Seguridad de la Información ligada a los recursos humanos”, de uno de los marcos de trabajo sobre seguridad de la información más popular y solido entre las empresas del mundo, la ISO/IEC 27001:2013 en este documento de referencia internacional podemos encontrar los requerimientos para establecer, mantener y optimizar continuamente un SGSI, por sus siglas Sistema de Gestión de Seguridad de la Información; este sistema permite preservar la disponibilidad, integridad y confidencialidad de la información gracias a que aplica un proceso de gestión de riesgos y genera confianza a todos los interesados del negocio sobre la buena gestión de estos.

La ejecución de este proyecto se realizó en la organización industrial/comercial Komatsu – Mitsui Maquinarias Perú S.A. proveedora de soluciones en los sectores de construcción y minería, la mayor parte de sus ingresos están en la venta, mantenimiento y servicio post-venta de maquinaria amarilla, motores y equipos de generación energética.

La presente investigación se justifica metodológicamente con el efecto de fomentación a una cultura de identificación y prevención de riesgos y brechas de seguridad de la información ligados a los recursos humanos en empresas de menor o mayor tamaño a la cual está dirigida la aplicación de este proyecto, se dará a conocer cuál es el resultado de aplicar controles de seguridad que mitiguen el error del factor humano con respecto a los criterios de seguridad informática.

Este estudio también cuenta con una justificación técnica, ya que utiliza marcos de trabajo e implementaciones similares nacionales e internacionales con respecto a la implementación de controles de seguridad de la información, como la norma ISO 27001 e ISO 27002 las cuales favorece a cualquier área de TI de una organización indicando las buenas prácticas de implementación y trabajo con respecto a la seguridad de la información.

Adicionalmente este trabajo se justifica operativamente, debido a que diversos estudios de empresas e instituciones dedicadas a la seguridad de la información y ciberseguridad afirman que los eventos de ciberseguridad han evolucionado y aumentado, teniendo como foco la búsqueda del error humano, intentando así facilitar la intrusión a los sistemas o red de una compañía, mediante técnicas de ingeniería social.

En concordancia de los párrafos anteriores, este estudio presenta una justificación teórica, ya que forma parte de un pequeño porcentaje de trabajos con línea de investigación “Seguridad de la información” que se han relacionado con los Recursos Humanos de una compañía, este proyecto podrá tomarse como referencia de otros trabajos similares que busquen esta novedosa relación de variables, tal como en la recientemente actualizada norma ISO 27001:2022 que toma como uno de sus cuatro pilares a los recursos humanos.

Finalmente; este trabajo también cuenta con una justificación económica, ya que al prevenir riesgos cibernéticos evita incidentes que comprometan la operatividad de la compañía lo que causaría perdidas según el tiempo, además de conllevar un ahorro en el pago del ciberseguro de la empresa.

El problema general descrito en ese proyecto es: ¿De qué manera la aplicación de la propuesta de estrategias de seguridad de la información según la ISO 27001:2013 mejorará el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A.? Desglosado en cinco problemas específicos: ¿Cuál es el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.?; ¿Cuál es el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.?; ¿De qué manera se puede mejorar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.?; ¿Cuál es el nivel de concientización de los recursos humanos en seguridad de la información después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.? y ¿Se evidencian mejoras al Comparar el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la

seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.?

Adicionalmente se cuenta con el objetivo general: Determinar que la aplicación de la propuesta de estrategias de seguridad de la información según la ISO 27001:2013 mejorará el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A. Y los objetivos específicos: Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.; identificar el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.; Diseñar e implementar la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 para mejorar el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A.; Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. y Comparar las mejoras en el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.

Finalmente, se tiene como hipótesis general: Las estrategias de la seguridad de la información según la ISO 27001:2013 mejoran el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.

II. MARCO TEÓRICO

En este proyecto de implementación se respalda con distintas tesis de investigación que serán catalogadas como antecedentes, las cuales se procede a describir: Benites (2019) tuvo por objetivo en su tesis de titulación la ejecución de un proyecto de implementación de un SGSI en una planta de fabricación de Radiadores, en la cual usa como metodología un proyecto experimental, documental – correlacional, y concluye que gracias a la implementación del SGSI en la organización aumentó el nivel de madurez de Gestión de Riesgos de un 3.65 a un 5.22 llegando a un estado de Definido/Administrado.

Torres y Chicaiza (2020) en su tesis grado de titulación, tuvo por objetivo la implementación de un Plan de Seguridad Informática según los lineamientos de la ISO 27001:2013 para la correcta gestión y protección de activos de información para la empresa MEGAPROFER S.A. en la cual usa las modalidades Aplicada y Bibliográfica o documentada como metodología de investigación, para poder determinar el problema de la compañía de manera objetiva tomando en cuenta marcos de trabajo internacionales. Finalmente, concluye que gracias a la implementación de un plan de seguridad informática se incrementó favorablemente la preservación de la disponibilidad, confidencialidad e integridad de los activos de información de la compañía.

Vásquez (2018) En su trabajo de tesis, tiene como objetivo la implementación de un Sistema de Gestión de Seguridad de la Información, adicionalmente plantea una metodología de investigación experimental con una población de 56 colaboradores, los cuales tomará en cuenta en su totalidad para la ejecución de aquel proyecto, entre sus técnicas de recolección de datos existen las auditorías que indica ayudarán a la revisión del debido cumplimiento de los controles implementados en la empresa según la ISO 27001:2013. Finalmente concluye que el personal de la compañía es un activo muy importante para la seguridad de la información, por lo tanto, es prioritario que aquellos estén en constante capacitación y concientización sobre los riesgos y brechas de seguridad que podrían causar.

Adicionalmente se tomó como referencias algunos artículos científicos y experimentos que nos guiarán en la ejecución y comparación de resultados de este proyecto de investigación: El sector empresarial privado es uno de los focos

en implementación de proyectos ligados a la tecnología e informática por lo que Kobis Pawel, Karvy Oleh y Chmielarz Grzegorz (2021) ejecutaron un proyecto de investigación con la finalidad de estudiar las amenazas de seguridad de la información que los recursos humanos impulsan, bajo el punto de vista de los Responsables de la gestión de recursos, ellos incluyeron en una de las conclusiones de su trabajo que el añadir medidas de protección, como controles de seguridad, destinados a reducir o eliminar el error humanos en la gestión de seguridad de la información es necesario.

También en este mismo sector Wipawayangkool, Kamphol y Lilly, Juliana (2021) ejecutaron un proyecto para una compañía con la finalidad de Atraer talento para mitigar los riesgos de Seguridad de la Información, definiendo en una de las conclusiones de su trabajo que debido a que las organizaciones están bajo constantes amenazas cibernéticas. La relación entre técnicas de activos humanos y seguridad informática brindan una ventaja competitiva a la compañía que lo emplea

Adicionalmente Natalia Bahashova, Hanna Puriy e Inta Kotane (2018) en su investigación titulada Seguridad de la información de la movilidad de los recursos humanos en condiciones de integración, concluyen que, actualmente, en el mundo existe inestabilidad con respecto a la seguridad de la información, por lo que, para las empresas es necesario pasar por un proceso de cambio cultural a todos sus integrantes con respecto a ciberseguridad, seguridad de la información y gestión de riesgos. Si a esta la relacionamos a los recursos humanos se convierte en una importante estrategia considerando los riesgos que estos pueden generar si no están debidamente capacitados.

Siguiendo con el mismo enfoque Zeng, Zhen y Zhang, Jiajia (2021) con su trabajo de investigación buscaban el papel que tiene la seguridad de internet de las cosas en la gestión de la fuga de información de Recursos Humanos de la empresa. Sintetizando que, el rápido desarrollo de la tecnología atraerá inevitablemente más brechas de seguridad de la información, por esto es necesario una gestión de cambios en transformación digital y tecnología para que las personas de una compañía se adapten a la rápida evolución de la tecnología. Por eso es necesario también adoptar las leyes de Protección de datos personales y los lineamientos de la ISO 27701.

Luego, Phudphad, et al. (2017) clasifica los factores de seguridad del sistema de información de recursos humanos (HRIS) que influyen en el clima de trabajo abierto: uso del proceso de jerarquía analítica (AHP) concluyendo que, en las compañías según este estudio se da una mayor prioridad a los pilares de un SGSI definido en la ISO 27001 según orden: confidencialidad, no repudio o trazabilidad, integridad y disponibilidad de la información; seguido por la tecnología y la cultura organizacional, esto puede reflejar la gran cantidad de brechas en seguridad de la información ligada a los recursos humanos ya que la cultura en seguridad de la información es última prioridad en las organizaciones.

Así mismo, Kobis P. y Karyy O. (2021) estudiaron el Impacto del factor humano en la seguridad de los recursos de información de las empresas durante la pandemia del COVID-19, En este estudio se realizó una comparación entre informes de "Global Security Insights Report 2021: Extended enterprise under threat" el publicado en el 2020, presentando los activos objetivos más sensibles para generación de intrusiones o ciberataques hacía la infraestructura de los sistemas de las organizaciones a nivel mundial, se puede verificar que existe una gran tendencia de atacar a los recursos humanos por vectores como phishing e ingeniería social y se es posible atribuirlo a la introducción al trabajo remoto por la pandemia Covid – 19.

Finalmente, en este sector Bahrami, et al. (2021) estudió el Efecto de la Motivación, Oportunidad y Habilidad en la Información de Recursos Humanos y Gestión de la seguridad teniendo en cuenta los roles de los factores de actitud, comportamiento y factores organizacionales. En este artículo se revisa la óptima aplicación de dominio de Seguridad de a información ligada a los recursos humanos según la ISO 27001:2013 y sus controles de concientización, educación y comunicación; además de los procesos disciplinarios. Se indica la motivación y efectividad de los dominios aplicados según las capacitaciones que apliquen las compañías, según los medios de refuerzo. Además de explorar la efectividad de los procesos disciplinarios al colaborador que no evidencia efectividad al recibir los controles.

Explorando ahora estudios y proyectos aplicados en el sector público, gobierno y universidades, Mo'ath Y, et al. (2020) estudió el papel de los procesos de gestión de recursos humanos para lograr la seguridad de la información: un

estudio aplicado en las universidades del gobierno saudí; concluyendo que, el compromiso de la alta gerencia y de los colaboradores de la compañía es importante cuando se aprueban e implementan políticas de seguridad de la información.

De igual manera, Anang, A., Gandhi A. y Sucahyo, Y. (2021) aplicaron el diseño de la gestión de riesgos de seguridad de la información: un estudio de caso del sistema de información de recursos humanos en la Universidad XYZ. En este artículo se explora la gestión de riesgos e incidentes de seguridad de la información en un sistema de información de recursos humanos, se usó técnicas de gestión según la ISO 27001 y según el análisis se pudo encontrar 40 riesgos, de los cuales la mayoría estaban ligados a los recursos humanos.

En concordancia con los antecedentes y artículos consultados, la implementación de controles de seguridad en una compañía debe ser guiada por buenas prácticas que se pueden encontrar en ese caso en el estándar ISO 27001 y ISO 27002.

En primera instancia definiremos qué es la información, según la Organización Internacional de Normalización (ISO 2013) un activo de información son datos o conocimiento que tienen valor para la compañía u organización, y los sistemas de información como el conjunto de servicios, aplicativos, tecnologías de información u otros que procesen o manejen a la misma.

Ahora vamos a explorar la definición de Seguridad de la Información, como una característica de esta misma que se logra a partir de la aplicación de procesos, metodologías y buenas prácticas que funcionen como protectores de los activos de información y sistemas de información, para el debido cumplimiento de la disponibilidad integridad y confidencialidad de la información. (Vega 2021) Esta definición básicamente nos indica que debemos proteger nuestra información de todo aquel que intente hacer mal uso de aquella.

También indicaremos qué es la ciberseguridad, según ISACA (2019) (Information Systems Audit and Control Association), se toma como ciberseguridad la protección de activos de información, mediante la mitigación de riesgos la información que puede ser almacenada, procesada y transportada por los sistemas de información.

Primero se define qué es un Sistema de Gestión de Seguridad de la Información (SGSI), “[…]es un marco de trabajo que permite conocer las pautas de creación, implementación, monitoreo y mejora continua de la protección de activos de información, relacionados con el cumplimiento de los objetivos del negocio.” (CEUPE 2018)

Un SGSI incluye la estructura organizativa de la compañía, las políticas internas, la planificación y programación de actividades y responsabilidades; las prácticas, los procedimientos y los recursos de una organización; Adicionalmente este modelo cuanta con tres pilares o dimensiones importantes; las cuales son, Disponibilidad, confidencialidad e integridad de la información, cabe recalcar que en cada organización se puede evaluar la necesidad de agregar más dimensiones según la necesidad, como por ejemplo, la trazabilidad y la autenticidad o el no repudio. Todo lo anterior indicado está dimensionado y detallado en la norma internacional ISO/IEC 27001: 2013.

La triada de seguridad de la información son los criterios que evalúan la maduración en el tema a una organización, por los cuál en este proyecto es importante definir estas características necesarias.

Confiabilidad, es la capacidad de protección de acceso a la información de una organización, a entes no autorizados. Esta característica es un elemento necesario para brindar privacidad. (Vega 2021)

Integridad, es la característica que refiere a la fidelidad, completitud y veracidad de la información o recursos. También tiene que ver con la prevención de cambios o modificaciones no autorizadas de la información. (Ordoñez 2021). Disponibilidad, hace referencia a la accesibilidad de la información cuándo es consultada o necesitada. (INCIBE 2020). Cabe recalcar que este modelo internacional además de indicar los requisitos, responsabilidades y pilares de un SGSI también detalla en su Anexo A 14 Dominios, 35 Objetivos de control y 114 Controles de aplicación, en el dominio 7 se puede encontrar Seguridad Ligada a los Recursos Humanos, la cual tiene tres Objetivos de Control:

Antes de la contratación: El objetivo es el de reducir el riesgo de fraude, robo, mal uso de las instalaciones o infraestructura de la compañía a partir de no asegurar las responsabilidades y aptitudes de los colaboradores, usuarios,

contratistas, etc. Este Objetivo de Control cuenta con dos Controles: Investigación de Antecedentes y Términos y condiciones de contratación.

Durante la contratación: El objetivo de este conjunto de controles es de asegurarse de que todos los colaboradores están alineados con sus responsabilidades y riesgos de seguridad de la información. Este Objetivo de Control cuenta con tres Controles: Responsabilidades de gestión, Concientización, educación y capacitación en SI y Proceso disciplinario.

Cese o cambio de puesto de trabajo: Este Objetivo de Control protege los intereses de la compañía en el proceso de finalización o cambio de empleo de colaboradores o contratistas. Cese o cambio de puesto de trabajo.

También se toma en cuenta las buenas prácticas que se pueden tomar al implementar un SGSI, indicadas en la norma "[…]ISO/IEC 27002 el cual define las buenas prácticas que se deberían llevar al implementar un SGSI". (CEUPE, 2018)

Adicionalmente también se dio importancia como parte de estas normativas internacionales y leyes, la ISO/IEC 27701 la cual proporciona los lineamientos para implementar un Sistema de Gestión de Privacidad de Información (SGPI) esta norma es una variante de la ISO/IEC 27001 (se mencionó en el párrafo anterior), estas normativas son muy similares ya que tienen objetivos en común, sin embargo, en esta variante de la normativa principal se ha hecho una integración de la Ley de protección de datos personales la cual fue gestada en Europa y ha ido migrando a los distintos continentes del mundo. En Perú esta ley fue adoptada en el 2011 la cuál tomó el nombre de la Ley N° 29733 (2011) la cual fue aprobada por el Decreto Supremo N° 003-2013-JUS (2007), esta norma nacional tiene el objetivo de garantizar el derecho fundamental de la Ley de protección de datos personales previsto en el numeral 2 artículo 6 de la Constitución Política del Perú (1993). El objetivo de que las empresas adopten esta norma y ley es que tengan un buen proceso de gestión de datos personales de sus empleados, clientes, proveedores, etc. Para evitar riesgos y faltas en su reputación como organización.

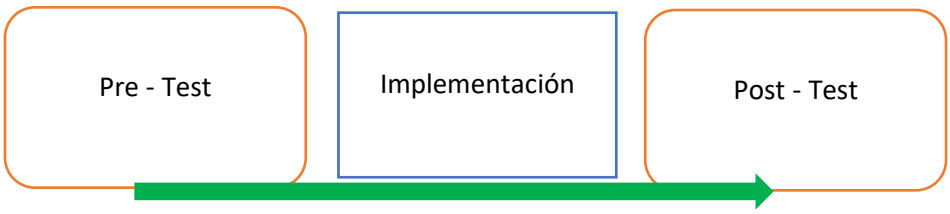
III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Este estudio presenta un diseño experimental para la subsección de pre-experimental, con énfasis en el enfoque de pre-prueba y post-prueba, en el que se diagnostica la situación actual mediante la comparación de pruebas antes y después. Los resultados de la prueba son generados por la nueva implementación, el propósito de este diseño es comprobar la hipótesis y los objetivos. El método de investigación es cuantitativo, el cual se define como un estudio estadístico que se aplica para medir las relaciones numéricas entre variables y que tiene como objetivo medir causa y efecto.

La investigación tiene un nivel explicativo, la cual Cornelissen et al. (2019) la define como una investigación profunda y social. Adicionalmente se tiene como enfoque cualitativo para este proyecto, definida por Taxer et al. (2015), como una investigación con el objetivo de comprobar un proceso de causa y efecto en base a estadísticas.

El objetivo es, manipular de deliberadamente las variables, para posteriormente analizar los efectos de la acción. (Rodríguez 2012). Su esquema fue:



3.2. Variables y operacionalización

Variable 1. Seguridad de la información

Para Perez (2015) indica que la seguridad de la información es la protección de la disponibilidad, integridad y confidencialidad de la información según el nivel requerido para el cumplimiento de los objetivos de negocio.

Variable 2. Recursos Humanos

Garcés (1999), Los recursos humanos son la parte más valiosa y sensible en la organización, su gente, que es el capital humano.

La variable independiente contiene tres dimensiones, “confidencialidad”, “integridad”, “disponibilidad”; la variable dependiente contiene una dimensión, “concienciación” sobre seguridad de la información.

3.3. Población, muestra y muestreo

La población es la agrupación de personas u objetos con el objetivo de extraer datos e información significativa para una investigación (Boody 2016). Para este estudio la población fue de 70 colaboradores con cargo de gerente dentro de la empresa Komatsu – Mitsui Maquinarias Perú S.A.

Con respecto a la muestra, se calculó una muestra con muestreo probabilístico en la cual dio como resultado una muestra de 60 colaboradores con cargo de gerente.

$$n_0 = \frac{NZ^2pq}{(N-1)E^2 + pqZ^2}$$

Donde:

N= tamaño de población = 70

Z= Nivel de confianza = 1.95

p= Probabilidad a favor = 0.5

q= Probabilidad en contra = 0.5

e= Error muestral = 0.05

n= Tamaño de la muetra = 60

3.4. Técnicas e instrumentos de recolección de datos

Para Hernández (2014) un instrumento es el que permite a un investigador medir y registrar datos e información de las variables que planteó en su estudio. (p. 199). Como técnica de recolección de datos se utilizó la encuesta, y como instrumento el cuestionario, este método de recolección de datos e información registra sistemática, valida y confiablemente los eventos o conductas que los examinados o participantes del estudio puedan tener, esto se clasifica si es necesario en grupos de categorías y subcategorías. (Hernández 2014)

Por otro lado, los instrumentos de recolección de datos pasaron por un proceso de validez de dos expertos los cuales emitieron opinión muy favorable sobre la validez de los cuestionarios elaborados. Por otro lado, se determinó la confiabilidad de los cuestionarios a través de una prueba piloto a 10 gerentes de otra compañía del mismo sector de la de estudio, para dicho fin se usó el alfa de Crombach obteniéndose para el cuestionario de seguridad de la información un valor de 0.807 y para el cuestionario de recursos humanos un valor de 0.799, ambos valores son de muy alta confiabilidad.

3.5. Procedimientos

En este proyecto de investigación se propone una solución para una de las problemáticas más comunes de seguridad de la información y ciberseguridad de cualquier compañía, y Komatsu – Mitsui Maquinarias Perú S.A. no es ajena a este problema, que es la concientización de los recursos humanos en seguridad de la información es por eso por lo que, se ha planteado como la variable dependiente de esta investigación.

Posteriormente a la determinación del enfoque se investigó las situaciones y soluciones similares en otras empresas, instituciones u organizaciones del Perú y del mundo, adicionalmente se consultaron marcos de trabajo y normativas internaciones que guían este tipo de proyectos con buenas prácticas y modelos de implementación, en base a toda la información y datos la unidad de negocio de Tecnología de la Información de la compañía tomó la decisión de implementar un Sistema de Gestión de Seguridad de la Información, en cuál es la variable independiente del proyecto, dentro del cual se encuentra el objetivo de control que es implementado en este proyecto, para lo cual se aplican tres actividades, una principal que nos ayudará a medir la efectividad del proyecto y dos de apoyo con el objetivo de reducir los índices de vulnerabilidad calculados en la ejecución de la primera actividad, estás actividades o controles son parte de la implementación del proyecto como tal.

Este proyecto propone una investigación detallada de la relación de las variables planteadas consultando diferentes fuentes como libros, tesis, artículos y revistas científicas, etc. Con el fin de respaldar científicamente el desarrollo de esta

investigación, con los datos recopilados y procesados se propone que la investigación sea aplicada pre-experimental.

Con respecto al instrumento de recolección de datos será revisado por expertos en la materia evaluando su validez con el “Coeficiente de validez de contenido” (Hernandez - Nieto, 2002) y también se midió su confiabilidad con el coeficiente de alfa de Cronbach. De la misma forma se definirá el método de procesamiento de datos haciendo uso del software SPSS que ayudará a realizar los análisis descriptivos e inferenciales que se realizarán a los datos obtenidos. Finalmente se definen los aspectos éticos y administrativos del proyecto, detallando los costos de la aplicación del mismo y el financiamiento total de la Compañía al cuál va dirigido.

3.6. Método de análisis de datos

La presente investigación se realizó mediante el análisis descriptivo e inferencial de la variable dependiente Recursos Humanos en relación con la variable independiente Seguridad de la Información mediante los indicadores “Confidencialidad”, “Integridad” y “Disponibilidad”. Para tal fin se recopiló información mediante los instrumentes en dos ocasiones, una antes de la aplicación de la propuesta de solución (pre-test) y otra después de la ejecución (post-test).

3.7. Aspectos éticos

Este estudio está completamente comprometido con la ética del investigador, siguiendo los lineamientos de las normativas y leyes que rigen mundialmente. De esta forma se respeta toda propiedad intelectual, añadiendo las referencias pertinentes de cada estudio, investigación consultada y agregada al presente estudio.

Gonzales (2002), Las conductas éticas en la investigación científica son indispensables para el investigador y el maestro; las conductas no éticas no tiene lugar en la ciencia.

Siguiendo también, el modelo presentado por el investigador citado se añadió a este estudio los siguientes aspectos éticos:

Privacidad en el empleo de datos, la identidad de los participantes del cuestionario será completamente confidencial y la información obtenida de aquellos

solo será utilizada para la realización de esta investigación; validez científica, el método científico y las teorías de investigación están presentes en todo el estudio, además de que los instrumentos fueron validados por expertos y evaluados en su confiabilidad; Consentimiento informado de la institución, la institución ha brindado la autorización para la realización de la investigación.

IV. RESULTADOS

Objetivo específico 1

Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa objetivo.

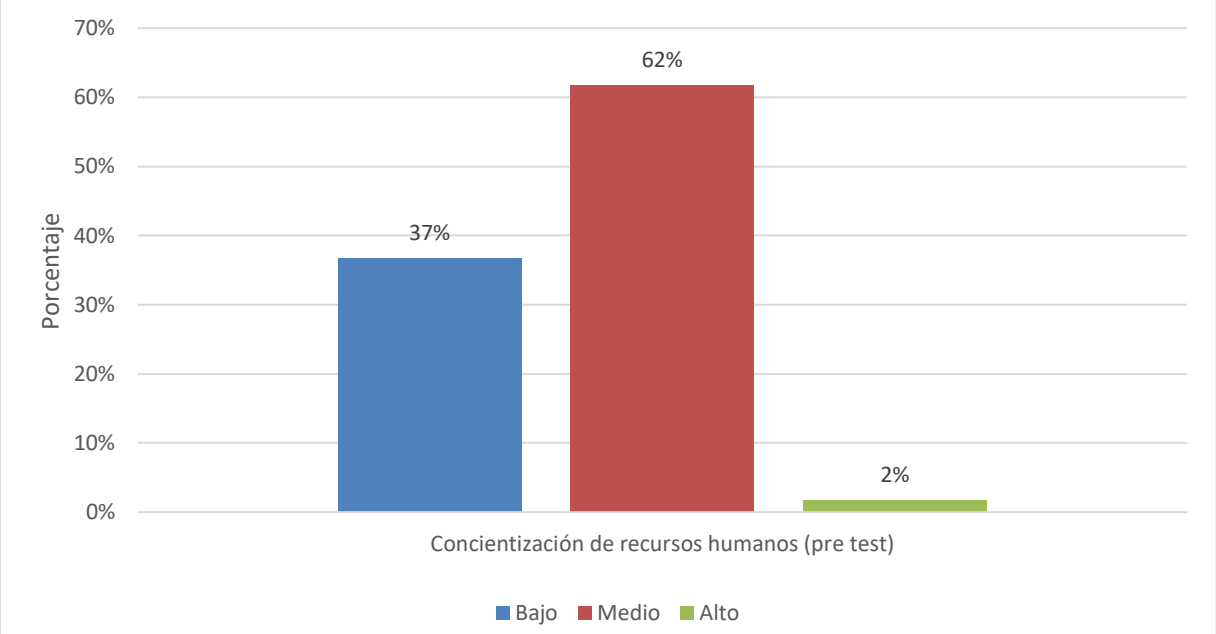
Tabla 1

Concientización de recursos humanos (pre test)

Nivel	f	%
Bajo	22	36,7
Medio	37	61,7
Alto	1	1,7
Total	60	100,0

Figura 1

Concientización de recursos humanos (pre test)



De los resultados obtenidos en el pretest de la concientización de recursos humanos en seguridad de la información en la empresa objetivo. se obtuvo que la percepción de los colaboradores encuestados un 36.7% indicó tener un nivel bajo, el 61.7% indicó un nivel medio y sólo el 1.7% percibió tener un nivel alto. Este se ve reflejado en la parte descriptiva de las preguntas realizadas, en las cuales para

todas las preguntas los valores promedio oscilaron entre 2.43 y 2.90 que su ubican en el nivel de respuestas 2: muy pocas veces y 3: algunas veces (ver Anexo 7).

Objetivo específico 2

Identificar el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa objetivo.

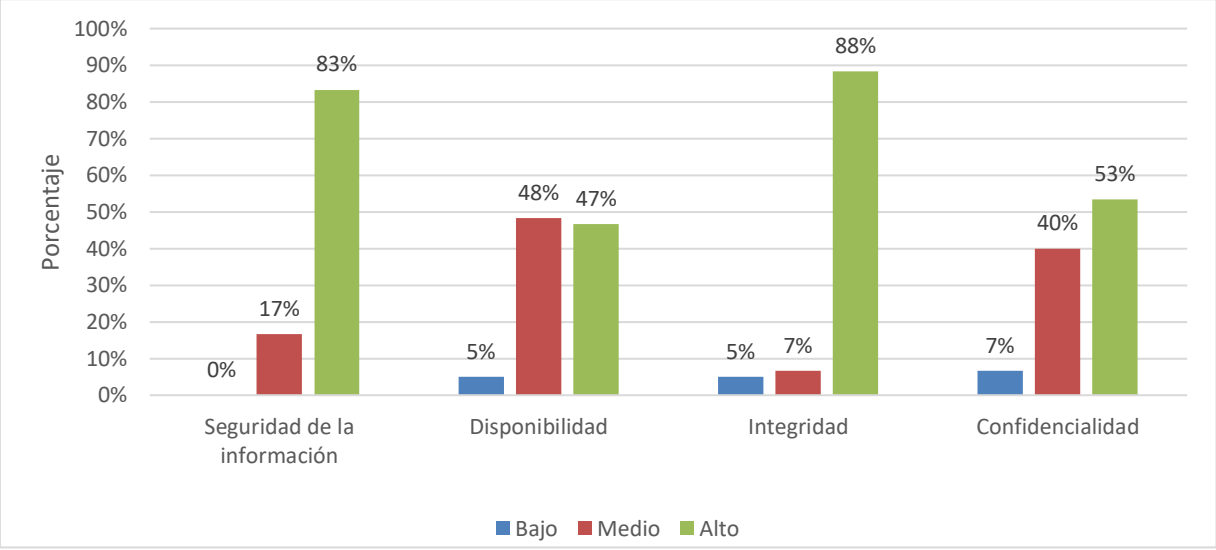
Tabla 2

Criterios determinantes de la seguridad de la información

Nivel	Seguridad de la información		Disponibilidad		Integridad		Confidencialidad	
	f	%	f	%	f	%	f	%
Bajo	0	0%	3	5%	3	5%	4	7%
Medio	10	17%	29	48%	4	7%	24	40%
Alto	50	83%	28	47%	53	88%	32	53%
Total	60	100%	60	100%	60	100%	60	100%

Figura 2

Criterios determinantes de la seguridad de la información



De los resultados obtenidos en cuanto al nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa objetivo. se obtuvo que la percepción de los colaboradores encuestados, un 83% indicó percibir un nivel alto y el 17% un nivel medio. Esto se ve reflejado en el análisis de las dimensiones disponibilidad; se obtuvo para esta dimensión un

47% indicó percibir un nivel alto, el 48% un nivel medio y sólo un 5% un nivel bajo; integridad, se obtuvo para esta dimensión un 88% indicó percibir un nivel alto, el 7% un nivel medio y sólo un 5% un nivel bajo y confidencialidad donde se obtuvo un 53% indicó percibir un nivel alto, el 40% un nivel medio y sólo un 7% un nivel bajo.

Objetivo específico 3

Diseñar e implementar la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 para mejorar el nivel de concientización de los recursos humanos en la empresa objetivo.

La propuesta de estrategias basadas en la seguridad de la información según la ISO 27001:2013 en la empresa objetivo, se desarrolló posterior a la recolección y el procesamiento de los datos obtenidos de los cuestionarios aplicados a los empleados de dicha compañía, donde se logró identificar los principales criterios determinantes de la seguridad de la información según la ISO 27001:2013 y así diseñar actividades estratégicas que permitan mejorar la concientización del recurso humano en este aspecto. Entre las principales estrategias diseñadas se aplicó: Estrategia 1: Plan de difusión comunicados de Seguridad de la Información; Estrategia 2: Campañas de simulación de ataques de ingeniería social con concientización instantánea; Estrategia 3: Publicación de contenido audiovisual de Seguridad de la Información; Estrategia 4: Inducciones Corporativas y estrategia 5: Monitoreo de efectividad de controles de SI ligados a los recursos humanos. (ver Anexo 11).

Tabla 3

Plan de acción de la propuesta

Estrategia	Objetivo	Actividad	Responsable
Estrategia 1: Plan de difusión comunicados de Seguridad de la Información.	Utilizar los medios de comunicación corporativa para capacitar y comunicar aspectos importantes y recomendaciones de Seguridad de la información.	• Redactar comunicados de seguridad de la información, ciberseguridad y trabajo seguro con dispositivos finales. • Crear una programación de difusión de comunicados. • Coordinar con el área de comunicaciones corporativas la correcta redacción de los comunicados y la programación de difusión. • Presentar a la Gerencia de TI, la programación y solicitar el visto bueno para su ejecución.	Carrasco Ramirez, David Agusto.
Estrategia 2: Campañas de simulación de ataques de ingeniería social con concientización instantánea.	Concientizar en base a ejemplos de ataques cibernéticos de ingeniería social a los colaboradores de la compañía.	• Ejecutar las campañas de simulación mensualmente. • Cada colaborador víctima recibirá un mensaje de concientización instantánea. • Los colaboradores víctimas recibirán un correo de parte de la Sub – Gerencia de Seguridad de la Información o la Gerencia de TI, indicando que ha sido víctima de una simulación de ataque y dándole recomendaciones para una futura ocasión. • Los colaboradores reincidentes en 3 oportunidades de manera consecutiva recibirán una amonestación formal de parte de la Sub – Gerencia de Seguridad de la Información o la Gerencia de TI, indicando que ha atentado contra los lineamientos de la Normativa Interna de Seguridad de la Información.	Carrasco Ramirez, David Agusto.

		• Los colaboradores reincidentes recibirán una llamada de parte del personal del área de Seguridad de información para capacitarlo de manera particular.	
Estrategia 3: Publicación de contenido audiovisual de Seguridad de la Información.	Informar, concientizar y capacitar en seguridad de la información y ciberseguridad mediante vídeos cortos difundidos por los medios de comunicación corporativa.	• Redactar el guion. • En coordinación con Comunicaciones corporativas realizar la grabación de los vídeos. • Solicitar el visto bueno para difusión del contenido. • Difundir los contenidos mediante los medios de comunicación corporativa.	Carrasco Ramirez, David Agusto.
Estrategia 4: Inducciones Corporativas	Capacitar y concientizar a todos los nuevos ingresos de la compañía.	• Diseñar y redactar una presentación que esté alineada a los lineamientos de la Normativa interna de Seguridad de la Información. • Coordinar con el área Recursos Humanos las sesiones de inducción cuando se integren más miembros a la compañía. • Evaluar dentro del tiempo de la sesión el entendimiento de los nuevos colaboradores sobre la capacitación realizada.	Carrasco Ramirez, David Agusto.
Estrategia 5 Monitoreo de efectividad de controles de SI ligados a los recursos humanos.	Evaluar la efectividad de los controles de seguridad de la información que protegen a los activos de información y al factor humano.	• En coordinación con el área de Control Interno, diseñar las evidencias y criterios de evaluación con los que se evaluará la efectividad de controles, según la matriz de riesgos - compañía. • Crear un cronograma y solicitar visto bueno de la Gerencia TI. • Realizar la evaluación de los controles y subsanar las brechas o vulnerabilidades encontradas.	Carrasco Ramirez, David Agusto.

Fuente: Elaboración propia

Objetivo específico 4

Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa objetivo.

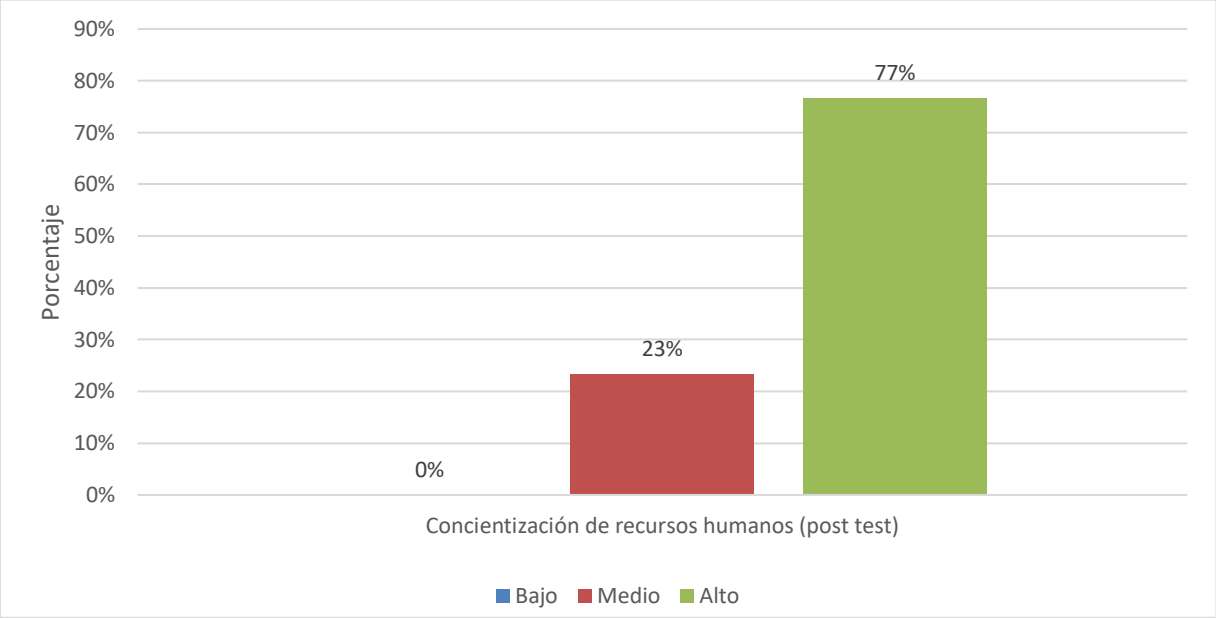
Tabla 4

Concientización de recursos humanos (post test)

Nivel	f	%
Bajo	0	0
Medio	14	23.3
Alto	46	76.7
Total	60	100,0

Figura 3

Concientización de recursos humanos (post test)



De los resultados obtenidos en el post test de la concientización de recursos humanos en seguridad de la información en la empresa objetivo, se obtuvo que la percepción de los colaboradores encuestados un 76.7% indicó tener un nivel alto y solo el 23.3% indicó un nivel medio.

Objetivo específico 5

Comparar las mejoras en el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa objetivo.

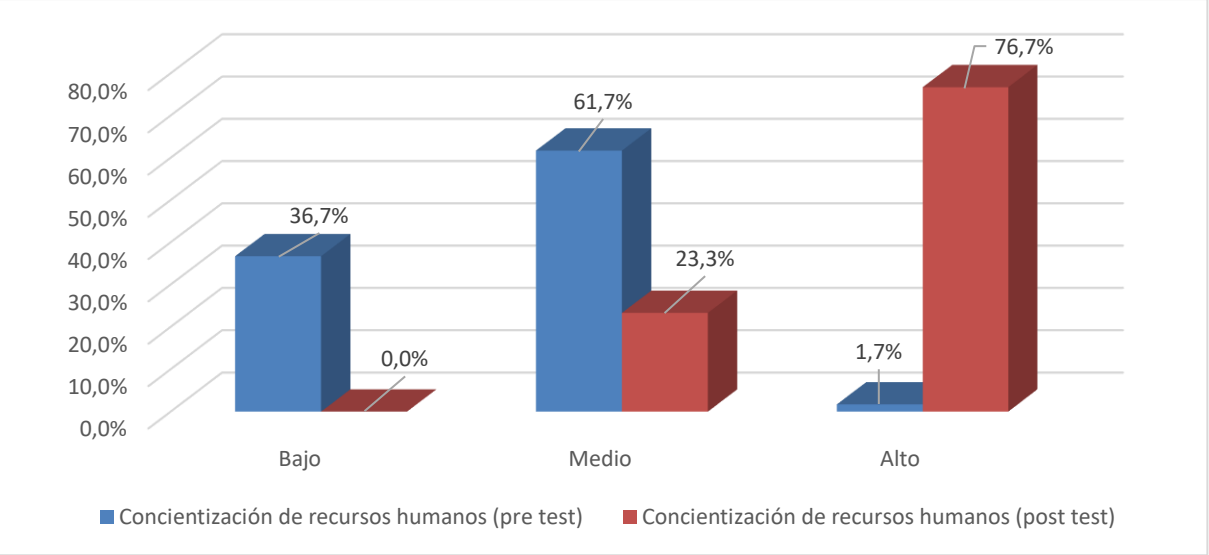
Tabla 5

Comparación resultados pre test y post test

Nivel	Concientización de recursos humanos (pre test)		Concientización de recursos humanos (post test)	
	f	%	f	%
Bajo	22	36.7	0	0.0
Medio	37	61.7	14	23.3
Alto	1	1.7	46	76.7
Total	60	100.0	60	100.0

Figura 4

Comparación resultados pre test y post test



La comparación de los resultados del pre test y post test del nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa objetivo muestras mejoras en la disminución del nivel bajo de 36.7% a 0% y el aumento del nivel alto de 1.7% a 76.7% lo que indica que las estrategias aplicadas fueron efectivas.

Estadística inferencial

Tabla 6

Prueba de normalidad

	Kolmogorov-Smirnov[a]			Condición Sig. > 0.05 hay normalidad
	Estadístico	gl	Sig.	
Concientización de recursos humanos (pre test)	0.250	60	0.000	No hay normalidad
Concientización de recursos humanos (post test)	0.154	60	0.001	No hay normalidad

a. Corrección de significación de Lilliefors

Como los datos de significancia calculados son menores a 0.05 quiere decir que dichos datos tanto del pre test como del post test de concientización de recursos humanos no poseen distribución normal, por lo que la hipótesis general se probó con la prueba no paramétrica de U Mann-Whitney.

Hipótesis general

H_0: La aplicación de estrategias de la seguridad de la información según la ISO 27001:2013 no mejoran el nivel de concientización de los recursos humanos en seguridad de la información en la empresa objetivo.

H_1: La aplicación de estrategias de la seguridad de la información según la ISO 27001:2013 mejoran el nivel de concientización de los recursos humanos en seguridad de la información en la empresa objetivo.

Tabla 7

Prueba de U de Mann-Whitney

	Concientización de los recursos humanos
U de Mann-Whitney	50,000
W de Wilcoxon	1880,000
Z	-9,200
Sig. asintótica (bilateral)	0.000

El valor de la significancia calculado fue de 0.000 y al ser menor que el valor de 0.05 se procedió a rechazar la H0 y aceptar la H1, que indica que la aplicación de estrategias de la seguridad de la información según la ISO 27001:2013 mejoran

el nivel de concientización de los recursos humanos en seguridad de la información en la empresa objetivo.

V. DISCUSIÓN

En primer lugar, tomaremos el resultado del objetivo específico 1: Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A. Se pudo visualizar que, De los resultados obtenidos en el pre test de la concientización de recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A. se obtuvo que la percepción de los colaboradores encuestados un 36.7% indicó tener un nivel bajo, el 61.7% indicó un nivel medio y sólo el 1.7% percibió tener un nivel alto.

El resultado obtenido en el primer objetivo concuerda con los resultados obtenidos por Kowis Pawel y Karvy Oleh (2021) quien revisó el efecto del conocimiento (concientización) en seguridad de la información y el funcionamiento de sistemas de los recursos humanos en el nivel de eventos de ciberseguridad. Encontrando que el factor humano es el responsable del 95% de eventos de ciberseguridad, por lo que un humano es responsable de 19 de 20 ataques cibernéticos hacía las instituciones a las que pertenecen, extrapolando así que, el 46.7% de colaboradores de las compañías que fueron parte de este estudio tienen un nivel de concientización bajo.

En concordancia con lo anterior Kobis, et al. (2021) en otro de sus trabajos versó las amenazas a la seguridad de la información impulsadas por el factor humano, incluyendo en una de sus conclusiones que 33,3% de colaboradores participantes de su estudio tienen un nivel bajo y 66.7% un nivel medio de concientización ya que nunca o rara vez tienen presente la ciberseguridad en su operativa diaria, esto desemboca en que el 88% de los incidentes y posibles incidentes que comprometen a la seguridad de la información resultan por errores del factor humano.

Estos resultados se argumentan o justifican con el concepto de los recursos humanos, ya que estos son la parte más valiosa pero también sensible en la compañía, y los ciberdelincuentes tienen muy claro cuál es el objetivo más vulnerable. Por lo que podemos decir que la concientización del factor humano en seguridad de la información debe ser trabajada para brindar resultados positivos en la compañía.

Con respecto al resultado del *objetivo específico 2:* Identificar el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. Se pudo observar que, de los resultados obtenidos en cuanto al nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. se obtuvo que la percepción de los colaboradores encuestados, un 83% indicó percibir un nivel alto y el 17% un nivel medio. Esto se ve reflejado en el análisis de las dimensiones: Disponibilidad; se obtuvo para esta dimensión un 47% indicó percibir un nivel alto, el 48% un nivel medio y sólo un 5% un nivel bajo; integridad, se obtuvo para esta dimensión un 88% indicó percibir un nivel alto, el 7% un nivel medio y sólo un 5% un nivel bajo y confidencialidad donde se obtuvo un 53% indicó percibir un nivel alto, el 40% un nivel medio y sólo un 7% un nivel bajo.

Estos resultados están de acuerdo con los obtenidos por Torres Christian y Chizaica Dennis (2019) al evaluar el nivel de la triada de seguridad de la información, indicando que en disponibilidad obtuvo un 77,80% en nivel alto, un 16,60% un nivel medio y un 5,60% un nivel bajo; en integridad obtuvo un 75% en nivel alto, un 16,70% un nivel medio y un 8,30% un nivel bajo; finalmente en confidencialidad obtuvo un 75% en nivel alto, un 17,86% un nivel medio y un 7,14% un nivel bajo.

Los resultados presentados se argumentan mediante el marco teórico de la seguridad de la información y sus variables, disponibilidad, integridad y confidencialidad. Las cuales van ligadas al valor que le da la compañía institución, etc. a los datos que maneja, cuando un dato que puede ser procesado, almacenado y distribuido tiene valor para una compañía, este se transforma en un activo de información, el cual desde el momento de su obtención de valor será resguardado por los controles de seguridad de la información, considerando los criterios de que debe estar accesible a los colaboradores que la consulten (disponibilidad), debe estar completa y valida (integridad) y solo debe entregarse a las personas que están autorizadas (confidencialidad).

Con respecto al resultado del objetivo específico 3: Diseñar e implementar la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. Se desarrolló posterior a la recolección y el procesamiento de los datos obtenidos de los cuestionarios aplicados a los empleados de dicha compañía, donde se logró identificar los principales criterios determinantes de la seguridad de la información según la ISO 27001:2013 y así diseñar actividades estratégicas que permitan mejorar la concientización del recurso humano en este aspecto. Entre las principales estrategias diseñadas se aplicó: Estrategia 1: Plan de difusión comunicados de Seguridad de la Información; Estrategia 2: Campañas de simulación de ataques de ingeniería social con concientización instantánea; Estrategia 3: Publicación de contenido audiovisual de Seguridad de la Información; Estrategia 4: Inducciones Corporativas y estrategia 5: Monitoreo de efectividad de controles de SI ligados a los recursos humanos.

El resultado presentado tiene relación con lo indicado por Torres Christian y Chizaica Dennis (2019), los cuales elaboraron un proyecto de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) donde dentro de su propuesta agregó 4 directrices relacionadas con la seguridad de la información ligada a los recursos humanos.

Los resultados obtenidos de las propuestas planteadas se argumentan bajo el uso de las buenas prácticas de la ISO:27001:2013, la cual presenta su dominio “seguridad de la información ligada a los recursos humanos”, se puede verificar que en la propuesta de solución implementada, cumple con los controles de los objetivos de control de la norma mencionada.

Ahora con respecto a los resultados obtenidos del objetivo específico 4: Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. Se obtuvo como resultados en el post test de la concientización de recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A., se obtuvo que la percepción de los colaboradores encuestados un 76.7% indicó tener un nivel alto y solo el 23.3% indicó un nivel medio.

Los resultados obtenidos en el objetivo específico 4 tienen relación con los resultados obtenidos por Kobis, et al. (2021) donde indicó que evaluó los resultados de la concientización de recursos humanos con una escala de 5 puntos (escala de Likert), obteniendo como resultados de los encuestados que, el nivel de concientización en seguridad de la información posterior a la aplicación de su solución fue de 68.49% en nivel alto, 31.51% en nivel medio y un 0% en nivel bajo.

Finalmente, con el objetivo específico 5: Comparar las mejoras en el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. La comparación de los resultados del pre test y post test del nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. muestras mejoras en la disminución del nivel bajo de 36.7% a 0% y el aumento del nivel alto de 1.7% a 76.7% lo que indica que las estrategias aplicadas fueron efectivas.

VI. CONCLUSIONES

1. Como solución del objetivo general del proyecto: Determinar la influencia de la aplicación de estrategias de la seguridad de la información según la ISO 27001:2013 en la concientización de los recursos humanos de la empresa Komatsu-Mitsui Maquinarias Perú -2022., se determina que, con la aplicación de las 4 estrategias de la propuesta dirigidas a todos los colaboradores de la compañía, se mejoró significativamente la concientización de los recursos humanos respecto a la seguridad de la información.
2. Los resultados que se obtuvieron al diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A. antes de la implementación de la propuesta, permiten concluir que se tenían varias debilidades, debido a que obtuvo un 99.3% entre los niveles bajo y medio.
3. Los resultados que se obtuvieron al identificar el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A., permiten concluir que se tenían controles solidos con respecto a la seguridad de la información y sus tres dimensiones: Disponibilidad, confidencialidad e integridad, debido a que en general la variable independiente obtuvo un 83% de nivel alto.
4. En la propuesta de estrategias basadas en la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A., se diseñaron e implementaron actividades estratégicas que permitan mejorar la concientización del recurso humano en este aspecto. Entre las principales estrategias diseñadas se aplicó: Estrategia 1: Plan de difusión comunicados de Seguridad de la Información; Estrategia 2: Campañas de simulación de ataques de ingeniería social con concientización instantánea; Estrategia 3: Publicación de contenido audiovisual de Seguridad de la Información; Estrategia 4: Inducciones Corporativas y estrategia 5: Monitoreo de efectividad de controles de SI ligados a los recursos humanos.

5. Los resultados que se obtuvieron al diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A. después de la implementación de la propuesta, permiten concluir que, en gran parte, los encuestados adquirieron una concientización sólida. debido a que obtuvo un 76.7% en el nivel alto.
6. Por último, al comparar las mejoras en el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A., concluimos que se mejoró de manera significativa la concientización de los recursos humanos debido a la aplicación de las estrategias propuestas, teniendo en cuenta que el nivel bajo disminuyó hasta el 0% y el nivel alto aumentó hasta el 76,7%.

VII. RECOMENDACIONES

1. Después de la ejecución del proyecto, podemos recomendar que los controles aplicados tengan constante monitoreo de efectividad para identificar nuevas brechas que surjan al pasar el tiempo.

2. Es necesario recalcar que la estrategia 2 de la propuesta implementada debe realizarse de manera mensual para mantener los niveles de vulnerabilidad bajo.

3. Se recomienda a la compañía actualizar la ejecución a los nuevos lineamientos de la ISO 27001:2022.

4. Como recomendación a los futuros investigadores, continúen con el estudio de la relación de las variables propuestas, debido a que, las normas, marcos de trabajo y las instituciones se están adaptando a los riesgos cibernéticos más explotados por los ciberdelincuentes en la actualidad.

REFERENCIAS

Al-Thunaibat, M. Y., Al-shawabkeh, A. A. ., & Al-baqor, K. K. . (2020). The Role of Human Resource Management Processes in Achieving Information Security: An applied Study on Saudi Government Universities. Management & Economics Research Journal, 2(3), 1-23. https://doi.org/10.48100/merj.v2i3.107

ANANG, Agus, GANDHI, Arfive y SUCAHYO, Yudho Giri, 2021. The design of information security risk management: A case study human resources information system at XYZ university. In: 2021 4th International Conference of Computer and Informatics Engineering (IC2IE). IEEE. 2021.

BAHASHOVA, Natalia, PURIY, Hanna y KOTANE, Inta, 2018. *Seguridad de la Información de la movilidad de los recursos humanos en condiciones de integración.* Polonia: Scientific Journal of Polonia University. DOI 26. 34-42. 10.23856/2603.

BAHRAMI, Et al. Effect of motivation, opportunity and ability on human resources information security management considering the roles of Attitudinal, behavioral and organizational factors, 2021. International journal of engineering. Online. Vol. 34, no. 12. DOI 10.5829/ije.2021.34.12c.07.

BENITES, César, 2019. Implementación de un sistema de gestión de seguridad de la información - Norma ISO 27001 para la fábrica Radiadores Fortaleza. Repositorio Universidad Tecnología del Perú, Lima- Perú. Disponible en: https://hdl.handle.net/20.500.12867/1933

CENTRO EUROPEO DE POSTGRADO (CEUPE), Centro Europeo, 2020. Modulo: ISO/IEC 27001.

Constitución Política del Perú [Const]. Art. 6. 29 de diciembre de 1993 (Perú).

Decreto Supremo N° 003-2013-JUS, 2013. Gob.pe. Online. [Accessed 29 mayo 2022]. Available from: https://www.gob.pe/institucion/minjus/normas-legales/1941246-003-2013-jus

Franco García, D., & Quintanilla Perea, A. (2020). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. Derecho PUCP, 84, 271–299. https://doi.org/10.18800/derechopucp.202001.009

FRANCO GARCÍA, Devora y QUINTANILLA PEREA, Alejandro, 2020. La protección de datos personales y el derecho al olvido en el Perú. A propósito de

los estándares internacionales del Sistema Interamericano de los Derechos Humanos. Derecho PUCP. Online. 2020. No. 84, p. 271–299. [Accessed 28 mayo 2022]. DOI 10.18800/derechopucp.202001.009.

GARCÉS, César Montalván, 1999. *Los recursos humanos para la pequeña y mediana empresa*. Universidad Iberoamericana.

GIRALDEZ, Alfonso, 2021. ISO 27701 en español. Implementación de la norma. UBT Compliance. Online. 3 diciembre 2021. [Accessed 28 mayo 2022]. Available from: https://ubtcompliance.com/iso-27701-en-espanol-implementacion-de-la-norma/

GONZÁLEZ, M. 2002. Aspectos éticos de la investigación cualitativa. Madrid: Redalyc. ISBN 1681-5653.

GREEN, Samuel y SALKIND, Neil. Using SPSS for Windows and Macintosh, Books a la Carte. Pearson: ACM. 8th Edition. ISBN: 978-0-13-431988-9. 2016. Disponible en: https://url2.cl/c7ZF7

HERNÁNDEZ Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6a. ed. --.). México D.F.: McGraw-Hill. ISBN: 978-1-4562-2396-0

Hernández-Nieto, R. A. (2002), Contribuciones al Análisis Estadístico. Mérida, Venezuela: Universidad de Los Andes.

INCIBE, 2020. *Protección de la Información.* España: INCIBE-Protege tu empresa.

ISACA., 2019. Obtener los fundamentos de la ciberseguridad correcta. En: ISACA Journal [en línea]. Disponible en: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/getting-the-basics-of-cybersecurity-right.

ISO, 2013. Sistema de Gestión de Seguridad de la Información.

Julio César Miguel Pérez. Protección de Datos y Seguridad de La Información. Vol. 4a edición actualizada. Paracuellos de Jarama, Madrid: RA-MA Editorial, 2015.

https://search.ebscohost.com/login.aspx?direct=true&db=e086tww&AN=2498239&lang=es&site=ehost-live.

KOBIS ET.AL, 2021. Threats to Information Security Driven by Human Factor in the Perception of Persons in Charge of Intangible Resources Management, vol.25, ISSN: 0137-7221. DOI: https://doi.org/10.33141/po.2021.5.03

KOBIS, Paweł y KARYY, Oleh, 2021. Impact of the human factor on the security of information resources of enterprises during the covid-19 pandemic. Polish Journal of Management Studies. Online. 2021. Vol. 24, no. 2, p. 210–227. DOI 10.17512/pjms.2021.24.2.13.

Ley de Protección de Datos Personales, Ley N° 29733 (e de Julio 2011). En: Normas Legales. Diario Oficial “El Peruano”. Lima: Congreso de la República.

MARSH MCLENNAN, 2022. Informe Global de Riesgos WEF.

ORDOÑEZ, Carlos Junior, 2021. *Triada de la seguridad de la información*. Ecuador: Universidad Nacional de Loja.

PHUDPHAD, Kanyarat, WATANAPA, Bunthit, KRATHU, Worarat y FUNILKUL, Suree, 2017. Rankings of the security factors of human resources information system (HRIS) influencing the open climate of work: using analytic hierarchy process (AHP). Procedia computer science. Online. 2017. Vol. 111, p. 287–293. DOI 10.1016/j.procs.2017.06.065.

PORRAS, Miguel. 2019. Sistema de gestión de seguridad de la información para la gestión de riesgos en activos de información. Repositorio Universidad Peruana de los Andes. Disponible en: https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2604/T037_45702501_T.pdf?sequence=1&isAllowed=y

Rodríguez, Metodología De Investigación Científica Aplicado A La Ingeniería. Informe. (2012).

Sánchez, C. (2017, mayo 27). Así fue el primer ‘ransomware’ del mundo: disquetes con sida que secuestraban tu PC. El Confidencial. https://www.elconfidencial.com/tecnologia/2017-05-27/primer-ransomware-diskete-panama_1389351/

TORRES, Christian y CHICAIZA, Dennis, 2019. Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A. Repositorio Universidad Tecnologíca de Ambato, Ecuador. Disponible en: https://repositorio.uta.edu.ec/jspui/handle/123456789/30690

VÁSQUEZ, Jaime. 2018. Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Industrial, Escuela Profesional de Ingeniería Industrial]. Repositorio institucional Cybertesis UNMSM.

VEGA, Edgar, 2021. *Seguridad de la Información.* España: 3Ciencias. 978-84-122093-6-5

WIPAWAYANGKOOL, K. and LILLY, J., 2021. Enlisting Human Resources to Mitigate Information Security Risks. Strategic HR Review, vol. 20, no. 1, pp. 27-29 ProQuest Central. ISSN 14754398. DOI https://doi.org/10.1108/SHR-09-2020-0080.

ZENG, Z. and ZHANG, J., 2021. Based on the Role of Internet of Things Security in the Management of Enterprise Human Resource Information Leakage. Wireless Communications & Mobile Computing (Online), vol. 2021 ProQuest Central. ISSN 1530-8669. DOI https://doi.org/10.1155/2021/5936390.

ANEXOS

Anexo 1: Matriz de consistencia

<table>
<tr><td colspan="5">Título: Implementación del dominio “Seguridad de la Información Ligada a los Recursos Humanos” según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú – 2022</td></tr>
<tr><td>Problema</td><td>Objetivos</td><td>Hipótesis</td><td>Variable Independiente: Seguridad de la Información</td><td>Indicadores</td></tr>
<tr><td rowspan="4">Problema General:

PG: ¿De qué manera la aplicación de la propuesta de estrategias de seguridad de la información según la ISO 27001:2013 mejorará el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A.?

Problemas Específicos:
PE1: ¿Cuál es el nivel de concientización de los recursos humanos en seguridad de la información en la empresa</td><td rowspan="4">Objetivo General:
OG: Determinar que la aplicación de la propuesta de estrategias de seguridad de la información según la ISO 27001:2013 mejorará el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A.

Objetivos Específicos:
OE1: Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.</td><td rowspan="4">Hipótesis General:
HG: Las estrategias de la seguridad de la información según la ISO 27001:2013 mejoran el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.</td><td>Disponibilidad</td><td>Nivel de disponibilidad de la información</td></tr>
<tr><td>Confidencialidad</td><td>Nivel de Confidencialidad de la información</td></tr>
<tr><td>Integridad</td><td>Nivel de integridad de la información</td></tr>
<tr><td>Variable Dependiente: Recursos Humanos</td><td>Indicadores</td></tr>
</table>

Komatsu – Mitsui Maquinarias Perú S.A.? PE2: ¿Cuál es el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.? PE3: ¿De qué manera se puede mejorar el nivel de concientización de los recursos humanos en seguridad de la información en la empresa Komatsu – Mitsui Maquinarias Perú S.A.? PE4: ¿Cuál es el nivel de concientización de los recursos humanos en seguridad de la información después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.? PE5: ¿Se evidencian mejoras al Comparar el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.?	OE2: Identificar el nivel de desarrollo de los criterios determinantes de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. OE3: Diseñar e implementar la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 para mejorar el nivel de concientización de los recursos humanos en la empresa Komatsu – Mitsui Maquinarias Perú S.A. OE4: Diagnosticar el nivel de concientización de los recursos humanos en seguridad de la información después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A. OE5: Comparar las mejoras en el nivel de concientización de los recursos humanos después de haber aplicado la propuesta de estrategias de la seguridad de la información según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.		Concientización	Nivel de concientización de los colaboradores

Fuente: Elaboración propia.

Anexo 2: Matriz de operacionalización de variables

Variables	Definición conceptual	Definición Operacional	Dimensiones	Indicadores	Instrumento	Escala
Independiente: Seguridad de la Información	Perez (2015) indica que la seguridad de la información es la protección de la disponibilidad, integridad y confidencialidad de la información según el nivel requerido para el cumplimiento de los objetivos de negocio.	El cuestionario medirá las dimensiones: disponibilidad, integridad y confidencialidad. Estas dimensiones son la clave para generar estrategias que puedan impactar en la concientización de los colaboradores en la institución en estudio.	Disponibilidad Integridad Confidencialidad	Relación de conocimiento, presentación de problemas y tiempo de respuesta.	Cuestionario	Escala Ordinal 1. Nunca. 2. Casi nunca. 3. A veces. 4. Casi siempre. 5. Siempre
Dependiente: Recursos Humanos	Garcés (1999), Los recursos humanos son la parte más valiosa y sensible en la organización, su gente, que es el capital humano.	El cuestionario medirá la dimensión: Concientización. Esta dimensión se evaluará en dos ocasiones; primero, antes de la implementación de la propuesta y segundo, después de la implementación.	Concientización	Nivel de concientización de colaboradores.	Cuestionario	Escala Ordinal 1. Nunca. 2. Casi nunca. 3. A veces. 4. Casi siempre. 5. Siempre

Fuente: Elaboración propia.

Anexo 3: Certificado de Validez de los indicadores Disponibilidad, Integridad y Confidencialidad.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE: Seguridad de la Información.

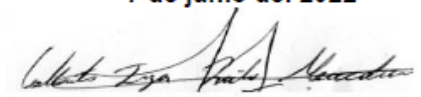
Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿El tiempo de respuesta frente a la caída del sistema son los apropiados?	X		X		X		
2	¿Siente usted que la información está disponible y a su disposición todo el tiempo o las veces que usted la consulta o solicita?	X		X		X		
3	¿Alguna vez ha percibido o experimentado un problema con la disponibilidad de la información?	X		X		X		
	DIMENSIÓN 2 Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿La validación con base en los riesgos a la información cumplen con los estándares de calidad?	X		X		X		
5	¿Conoce usted qué es la integridad de la información?	X		X		X		
6	¿Siente usted que la información que consulta llega de manera íntegra (completa y verdadera)?	X		X		X		
7	¿Alguna vez ha percibido o experimentado un problema con la Integridad de la información?	X		X		X		
	DIMENSIÓN 3 Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	¿Aplica políticas de seguridad interna para preservar la confidencialidad de los datos de los usuarios?	X		X		X		
9	¿Siente usted que la información solamente es entregada a las personas que están debidamente autorizadas?	X		X		X		
10	¿Alguna vez ha percibido o experimentado un problema con la Confidencialidad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia):_EL CUESTIONARIO SI ES SUFICIENTE _____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Ing. Zoila Collantes Inga DNI: 40335157
Especialidad del validador: ... Ingeniería de Sistemas y Computo
.....

7 de junio del 2022



ZOILA MERCEDES
COLLANTES INGA
Ingeniera de Sistemas y Cómputo
CIP N° 279212

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Anexo 4: Certificado de Validez de los indicadores Disponibilidad, Integridad y Confidencialidad – Segundo experto.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE: Seguridad de la Información.

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 Disponibilidad	Si	No	Si	No	Si	No	
1	¿El tiempo de respuesta frente a la caída del sistema son los apropiados?	X		X		X		
2	¿Siente usted que la información está disponible y a su disposición todo el tiempo o las veces que usted la consulta o solicita?	X		X		X		
3	¿Alguna vez ha percibido o experimentado un problema con la disponibilidad de la información?	X		X		X		
	DIMENSIÓN 2 Integridad	Si	No	Si	No	Si	No	
4	¿La validación con base en los riesgos a la información cumplen con los estándares de calidad?	X		X		X		
5	¿Conoce usted qué es la integridad de la información?	X		X		X		
6	¿Siente usted que la información que consulta llega de manera íntegra (completa y verdadera)?	X		X		X		
7	¿Alguna vez ha percibido o experimentado un problema con la Integridad de la información?	X		X		X		
	DIMENSION 3 Confidencialidad	Si	No	Si	No	Si	No	
8	¿Aplica políticas de seguridad interna para preservar la confidencialidad de los datos de los usuarios?	X		X		X		
9	¿Siente usted que la información solamente es entregada a las personas que están debidamente autorizadas?	X		X		X		
10	¿Alguna vez ha percibido o experimentado un problema con la Confidencialidad de la información?	X		X		X		

Observaciones (precisar si hay suficiencia): EL CUESTIONARIO SI ES SUFICIENTE

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr. Jose Gerardo Saavedra Carrasco DNI:
Especialidad del validador: Ingeniería Industrial

7 de junio del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

Anexo 5: Certificado de Validez del cuestionario de recursos humanos

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE: Recursos Humanos.

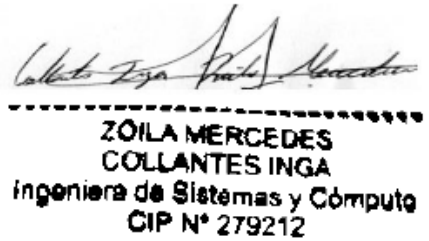
N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 Concientización	Si	No	Si	No	Si	No	
1	¿Es consciente de las amenazas a las cuales está expuesto al usar dispositivos inteligentes e internet?	X		X		X		
2	¿Alguna vez ha recibido un correo sospechoso?	X		X		X		
3	¿Alguna vez ha reportado un correo al área de Seguridad de la información (seguridad.ti@kmmp.com.pe)?	X		X		X		
4	¿Conoce usted los lineamientos del reglamento interno de seguridad de la información?	X		X		X		
5	¿Mantienen presentes los lineamientos del reglamento interno de seguridad de la información al utilizar los servicios de TI de la compañía?	X		X		X		
6	¿Alguna vez ha sido víctima de alguna simulación de ataques cibernéticos organizados por el equipo de seguridad de la información?	X		X		X		
7	¿Alguna vez ha sido víctima de un fraude por internet?	X		X		X		
8	¿Alguna vez ha visto o leído las recomendaciones publicadas en KMMP Noticias del área de Tecnología de la Información?	X		X		X		
9	¿Siente usted que está preparado para reconocer un correo malicioso?	X		X		X		
10	¿Se siente conforme con la inducción de Seguridad de la Información recibida al ingresar a la compañía?	X		X		X		

Observaciones (precisar si hay suficiencia): _EL CUESTIONARIO SI ES SUFICIENTE _____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Ing. Zoila Collantes Inga..... DNI: 40335157
Especialidad del validador:.....Ingeniería de Sistemas y Computo.....

8 de noviembre del 2022



ZOILA MERCEDES
COLLANTES INGA
Ingeniera de Sistemas y Cómputo
CIP N° 279212

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Anexo 6: Certificado de Validez del cuestionario de recursos humanos – Segundo experto.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE: Recursos Humanos.

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 Concientización	Si	No	Si	No	Si	No	
1	¿Es consciente de las amenazas a las cuales está expuesto al usar dispositivos inteligentes e internet?	X		X		X		
2	¿Alguna vez ha recibido un correo sospechoso?	X		X		X		
3	¿Alguna vez ha reportado un correo al área de Seguridad de la información (seguridad.ti@kmmp.com.pe)?	X		X		X		
4	¿Conoce usted los lineamientos del reglamento interno de seguridad de la información?	X		X		X		
5	¿Mantienen presentes los lineamientos del reglamento interno de seguridad de la información al utilizar los servicios de TI de la compañía?	X		X		X		
6	¿Alguna vez ha sido víctima de alguna simulación de ataques cibernéticos organizados por el equipo de seguridad de la información?	X		X		X		
7	¿Alguna vez ha sido víctima de un fraude por internet?	X		X		X		
8	¿Alguna vez ha visto o leído las recomendaciones publicadas en KMMP Noticias del área de Tecnología de la Información?	X		X		X		
9	¿Siente usted que está preparado para reconocer un correo malicioso?	X		X		X		
10	¿Se siente conforme con la inducción de Seguridad de la Información recibida al ingresar a la compañía?	X		X		X		

Observaciones (precisar si hay suficiencia): EL CUESTIONARIO SI ES SUFICIENTE

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Dr. Jose Gerardo Saavedra Carrasco DNI:
Especialidad del validador: Ingeniería Industrial

7 de junio del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

Anexo 7: Estadística descriptiva de la concientización de los recursos humanos (pre test).

			Estadístico	Desv. Error
Pregunta11	Media		2,90	,111
	95% de intervalo de confianza para la media	Límite inferior	2,68	
		Límite superior	3,12	
	Media recortada al 5%		2,83	
	Mediana		3,00	
	Varianza		,736	
	Desv. Desviación		,858	
	Mínimo		2	
	Máximo		5	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		1,031	,309
	Curtosis		,872	,608
Pregunta12	Media		2,73	,106
	95% de intervalo de confianza para la media	Límite inferior	2,52	
		Límite superior	2,95	
	Media recortada al 5%		2,67	
	Mediana		3,00	
	Varianza		,673	
	Desv. Desviación		,821	
	Mínimo		1	
	Máximo		5	
	Rango		4	
	Rango intercuartil		1	
	Asimetría		,918	,309
	Curtosis		1,210	,608
Pregunta13	Media		2,47	,110
	95% de intervalo de confianza para la media	Límite inferior	2,25	
		Límite superior	2,69	
	Media recortada al 5%		2,43	
	Mediana		2,50	
	Varianza		,728	
	Desv. Desviación		,853	
	Mínimo		1	
	Máximo		5	
	Rango		4	
	Rango intercuartil		1	

	Asimetría		,446	,309
	Curtosis		1,220	,608
Pregunta14	Media		2,57	,093
	95% de intervalo de confianza para la media	Límite inferior	2,38	
		Límite superior	2,75	
	Media recortada al 5%		2,50	
	Mediana		2,00	
	Varianza		,521	
	Desv. Desviación		,722	
	Mínimo		2	
	Máximo		5	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		1,158	,309
	Curtosis		1,012	,608
Pregunta15	Media		2,60	,076
	95% de intervalo de confianza para la media	Límite inferior	2,45	
		Límite superior	2,75	
	Media recortada al 5%		2,59	
	Mediana		3,00	
	Varianza		,346	
	Desv. Desviación		,588	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		-,145	,309
	Curtosis		-,304	,608
Pregunta16	Media		2,52	,087
	95% de intervalo de confianza para la media	Límite inferior	2,34	
		Límite superior	2,69	
	Media recortada al 5%		2,54	
	Mediana		3,00	
	Varianza		,457	
	Desv. Desviación		,676	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		-,402	,309
	Curtosis		-,093	,608

Pregunta17	Media		2,58	,087
	95% de intervalo de confianza para la media	Límite inferior	2,41	
		Límite superior	2,76	
	Media recortada al 5%		2,57	
	Mediana		3,00	
	Varianza		,451	
	Desv. Desviación		,671	
	Mínimo		1	
	Máximo		5	
	Rango		4	
	Rango intercuartil		1	
	Asimetría		,381	,309
	Curtosis		1,874	,608
Pregunta18	Media		2,43	,096
	95% de intervalo de confianza para la media	Límite inferior	2,24	
		Límite superior	2,63	
	Media recortada al 5%		2,41	
	Mediana		2,00	
	Varianza		,555	
	Desv. Desviación		,745	
	Mínimo		1	
	Máximo		5	
	Rango		4	
	Rango intercuartil		1	
	Asimetría		,618	,309
	Curtosis		1,460	,608
Pregunta19	Media		2,68	,087
	95% de intervalo de confianza para la media	Límite inferior	2,51	
		Límite superior	2,86	
	Media recortada al 5%		2,67	
	Mediana		3,00	
	Varianza		,457	
	Desv. Desviación		,676	
	Mínimo		1	
	Máximo		4	
	Rango		3	
	Rango intercuartil		1	
	Asimetría		,144	,309
	Curtosis		-,344	,608
Pregunta20	Media		2,65	,111
		Límite inferior	2,43	

	95% de intervalo de confianza para la media	Límite superior	2,87	
	Media recortada al 5%		2,59	
	Mediana		3,00	
	Varianza		,740	
	Desv. Desviación		,860	
	Mínimo		1	
	Máximo		5	
	Rango		4	
	Rango intercuartil		1	
	Asimetría		,920	,309
	Curtosis		1,119	,608

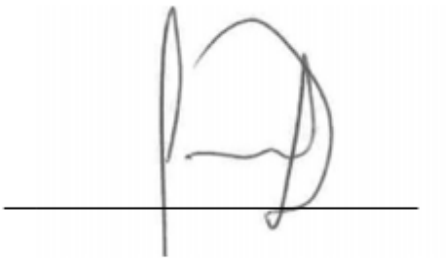
Anexo 8: Autorización para la realización y difusión de resultados de la investigación

AUTORIZACIÓN PARA LA REALIZACIÓN Y DIFUSIÓN DE RESULTADOS DE LA INVESTIGACIÓN

Por medio del presente documento, Yo Marcos Uriel Pinto Mamani identificado con DNI N° 41220736 y representante legal de Komatsu Mitsui Maquinarias Perú S.A. autorizo a David Agusto Carrasco Ramirez identificado con DNI N° 76589920 a realizar la investigación titulada: "Implementación del dominio "Seguridad de la Información Ligada a los Recursos Humanos" según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A." y a difundir los resultados de la investigación utilizando el nombre de Komatsu Mitsui Maquinaras Perú S.A.

Lima, 14 de Noviembre de 2022.

FIRMA



Marcos Uriel Pinto Mamani

DNI N° 41220736

Gerente de TI.

Komatsu Mitsui Maquinarias Perú S.A.

Anexo 9: Consentimiento informado

CONSENTIMIENTO INFORMADO

Yo Marcos Uriel Pinto Mamani identificado(a) con DNI N.º 41220736 he sido informado(a) sobre el procedimiento de la investigación titulada "Implementación del dominio "Seguridad de la Información Ligada a los Recursos Humanos" según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.", cuyos autore es David Agusto Carrasco Ramirez con DNI 76589920 se me ha entregado una copia de este consentimiento informado, fechado y firmado.

Además, se me ha explicado las características y el objetivo del estudio, así como los posibles beneficios de este. He contado con el tiempo y la oportunidad para realizar preguntas y plantear las dudas que poseía. Todas las preguntas fueron respondidas a mi entera satisfacción.

Se me ha asegurado que se mantendrá la confidencialidad de mis datos. Mi consentimiento lo otorgo de manera voluntaria y sé que soy libre de retirarme del estudio en cualquier momento, por cualquier razón de fuerza mayor. Por lo tanto, en forma consciente y voluntaria doy mi consentimiento para ser parte de esta investigación.

Lima, 14 Noviembre 2022

Marcos Uriel Pinto Mamani		
Apellidos y nombres	Firma	
41220736	41	M
DNI	Edad	Sexo (F:Femenino / M:Masculino)

Anexo 10: Porcentaje de similitud

Anexo 11: Propuesta

Implementación de controles de seguridad de la Información ligada a los recursos humanos en Komatsu – Mitsui Maquinarias Perú S.A.

I. Presentación

Los activos de información son cualquier dato o registro que tiene valor para una empresa, organización, etc. La seguridad de la información es, en este caso, la característica que protege a esta misma de todo aquel que tenga la intención de usar ese valor para otros fines, atentando a los objetivos de la empresa.

Sabemos que, en la actualidad, cualquier compañía que desea ser competitiva en el mercado utiliza la tecnología como herramienta; sin embargo, esta herramienta también es usada por algunos ilícitamente para el beneficio de sus propios intereses. Por lo que según el pasar del tiempo se ha dado casos de ataques cibernéticos a empresas y estados afectando o anulando la operativa de estas instituciones.

En el presente la mayoría de eventos de ciberseguridad están dirigidos no a un sistema de información o a la red perimetral de una compañía, sino que buscan al factor humano, se ha evidenciado que en los últimos 2 años el 95% de eventos de ciberseguridad han sido dirigidos a los recursos humanos, mediante técnicas de ingeniería social, las cuales buscan engañar al empleado o colaborador de la empresa para que este; infecte, entregue accesos, entregue credenciales de usuario, de noticias falsas, etc. Estos ataques son enviados en gran parte mediante el correo electrónico, también se utilizan los mensajes de texto (SMS), redes sociales, llamadas, etc.

Por esta razón múltiples instituciones han dado la importancia de generar cultura en sus recursos humanos, concientizándolos sobre a qué riesgos están expuestos y aplicando controles de seguridad que estén ligados a ellos mismos para tratar los riesgos cibernéticos.

II. Generalidades de la empresa

2.1 Breve reseña histórica

Komatsu Ltd. es uno de los líderes mundiales en la fabricación de equipos para Minería y Construcción. Fue fundado el 13 de mayo de 1921 y es accionista de Komatsu-Mitsui Maquinarias Perú S.A.

Sus principales negocios son la fabricación y venta de equipos de construcción y minería, servicios, maquinaria forestal y maquinaria industrial. El grupo Komatsu Ltd. está conformado por 178 empresas. Cuenta con 146 subsidiarias consolidadas y un total de 46, 730 trabajadores.

La piedra angular de la administración de Komatsu Ltd. es el compromiso a la "Calidad y Confiabilidad". Este principio no sólo aplica a los esfuerzos de entregar productos y servicios seguros y novedosos desde el punto de vista de nuestros clientes, también se extiende a mejorar la “Calidad y Confiabilidad” de todas las organizaciones, negocios, empleados y la administración del grupo Komatsu Ltd.

En nuestro país la marca Komatsu es distribuido por la compañía Komatsu-Mitsui Maquinarias Perú (KMMP).

Actualmente KMMP distribuye la marca para los mercados de minería y construcción. Dentro de su portafolio de clientes tiene a las principales Mineras del Perú y a las más importantes empresas del rubro de Construcción.

2.2 Descripción

Komatsu-Mitsui Maquinarias Perú (KMMP) es una empresa socialmente responsable, proveedora de soluciones integrales y servicio post venta para los sectores de minería y construcción (venta y servicio de maquinaria amarilla, equipos de generación y motores).

Los accionistas de KMMP son:

- Mitsui& Co. Una de las empresas comerciales, de inversión y de servicios más diversificadas del mundo.
- Komatsu Ltd. Empresa líder mundial en fabricación para equipos de Minería y Construcción.
- Cummins Inc. Líder global en la industria energética y el fabricante más importante del mundo de motores diesel de más de 50 HP.

Actualmente KMMP atiende el mercado peruano a través de una red de 15 Sucursales y Tiendas. Ofrecemos soporte con personal destacado en 12 Faenas Mineras. Contamos con más de 2,200 colaboradores.

2.3 Misión

Entregar soluciones de excelencia e innovadoras que contribuyen al crecimiento y desarrollo sostenible de nuestros grupos de interés.

2.4 Visión

Ser reconocidos por contribuir al éxito de nuestros clientes generando valor de largo plazo.

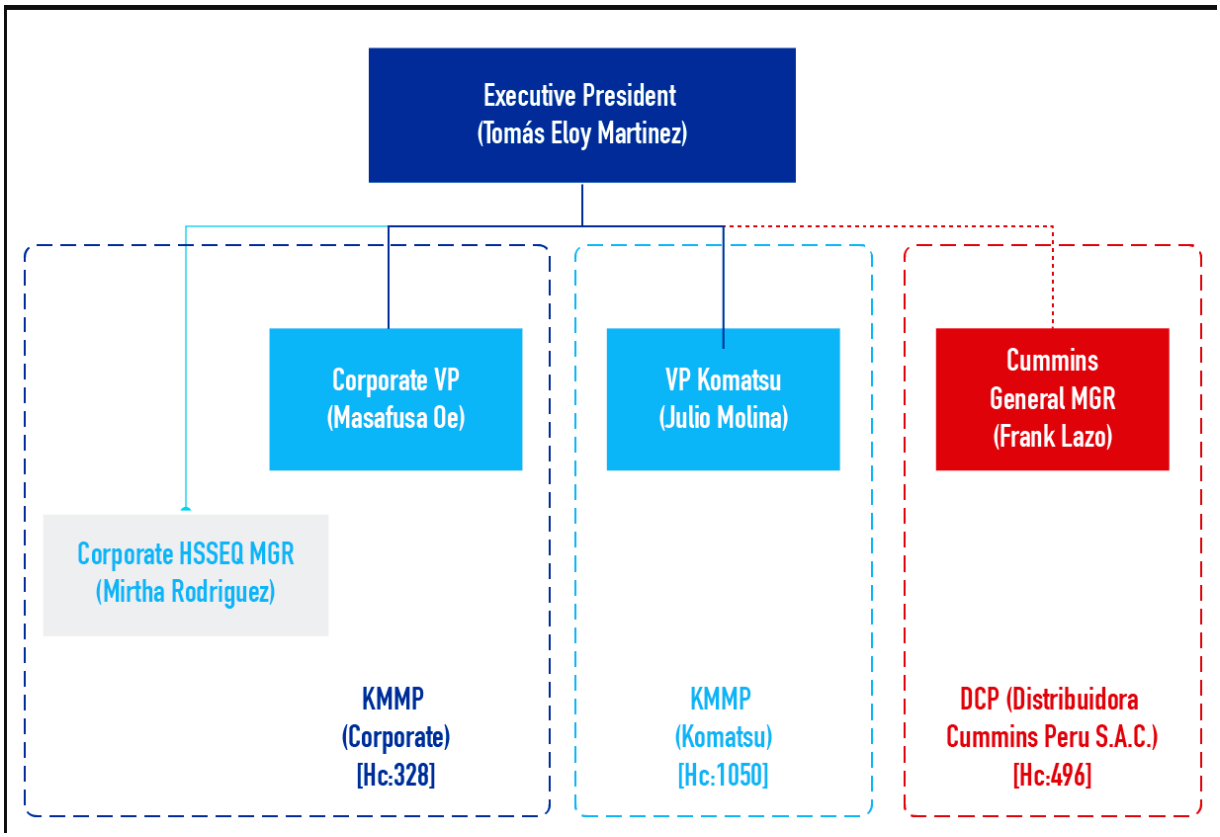
2.5 Valores

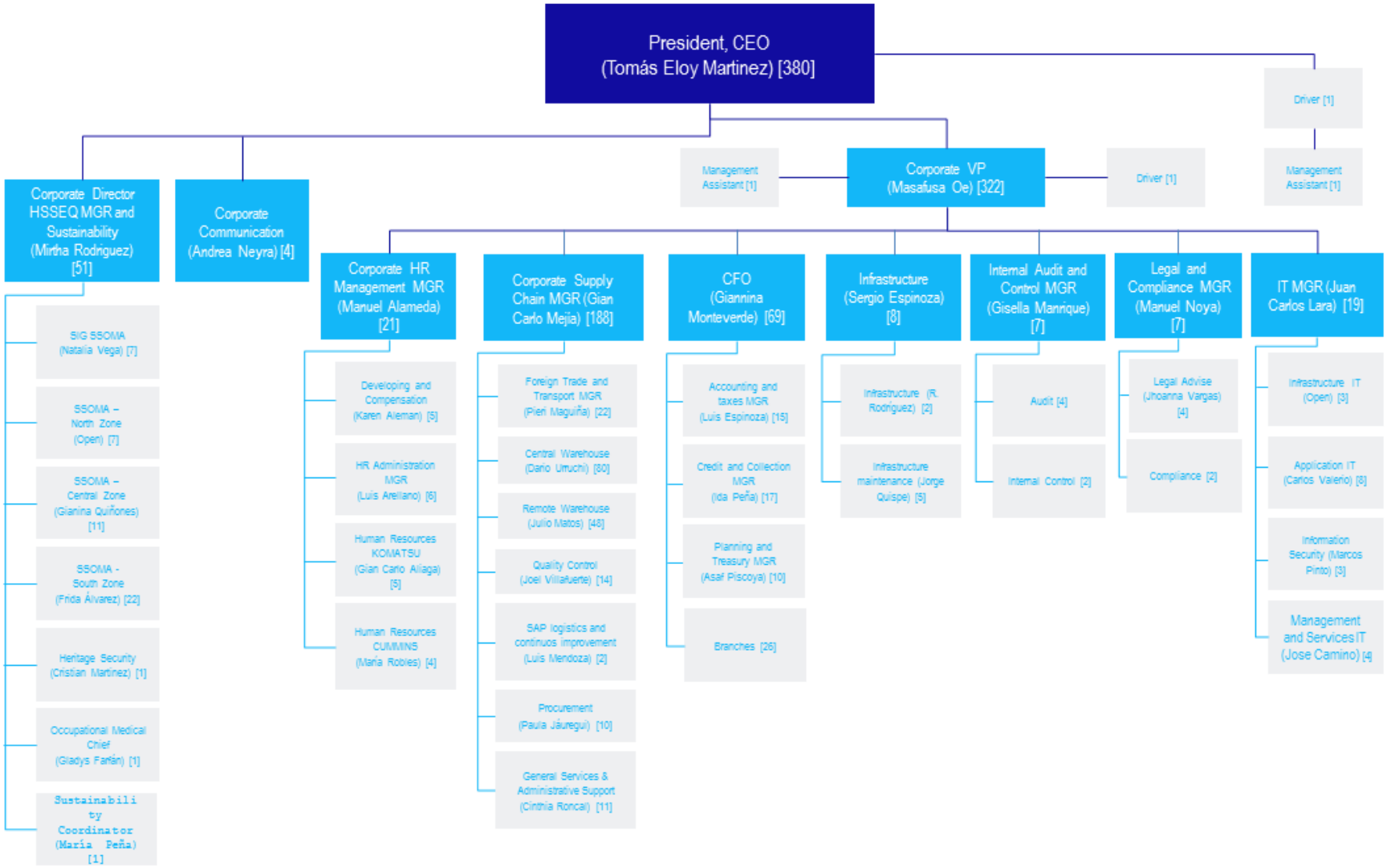
A. Salud y Seguridad: Cuídate y cuida a quienes te rodean. La salud y la seguridad no son negociables.
B. Integridad: Haz lo correcto y sé transparente siempre.
C. Diversidad & Inclusión: Promueve, respeta y valora las diferencias entre las personas creado un entorno donde nos sintamos parte.
D. Orientación al cliente: Entiende las necesidades de tus clientes internos y externos para superar constantemente sus expectativas.
E. Excelencia: Hazte cargo. Sé ágil buscando siempre nuevas formas de hacer las cosas mejores.
F. Trabajando en equipo: Contribuye al éxito del equipo colaborando y participando activamente.

2.6 Organigrama

Komatsu – Mitsui Maquinarias Perú S.A. se forma de una sociedad de 3 organizaciones, Komatsu como grupo dedicado a la maquinaria pesada, Mitsui

como grupo inversionista en proyectos mineros y Cummins como grupo especialista en el ensamblaje de motores de alto rendimiento




President, CEO
(Tomás Eloy Martinez) [380]
Driver [1]
Management Assistant [1]
Corporate VP
(Masafusa Oe) [322]
Driver [1]
Management Assistant [1]
Corporate Director HSSEQ MGR and Sustainability (Mirtha Rodriguez) [51]
Corporate Communication (Andrea Neyra) [4]
Corporate HR Management MGR (Manuel Alameda) [21]
Corporate Supply Chain MGR (Gian Carlo Mejia) [188]
CFO (Giannina Monteverde) [69]
Infrastructure (Sergio Espinoza) [8]
Internal Audit and Control MGR (Gisella Manrique) [7]
Legal and Compliance MGR (Manuel Noya) [7]
IT MGR (Juan Carlos Lara) [19]
SIG SSOMA (Natalia Vega) [7]
SSOMA – North Zone (Open) [7]
SSOMA – Central Zone (Gianina Quiñones) [11]
SSOMA - South Zone (Frida Álvarez) [22]
Heritage Security (Cristian Martinez) [1]
Occupational Medical Chief (Gladys Farfán) [1]
Sustainability Coordinator (María Peña) [1]
Developing and Compensation (Karen Aleman) [5]
HR Administration MGR (Luis Arellano) [6]
Human Resources KOMATSU (Gian Carlo Aliaga) [5]
Human Resources CUMMINS (Maria Robles) [4]
Foreign Trade and Transport MGR (Pieri Maguiña) [22]
Central Warehouse (Dario Urruchi) [80]
Remote Warehouse (Julio Matos) [48]
Quality Control (Joel Villafuerte) [14]
SAP logistics and continuos improvement (Luis Mendoza) [2]
Procurement (Paula Jáuregui) [10]
General Services & Administrative Support (Cinthia Roncal) [11]
Accounting and taxes MGR (Luis Espinoza) [15]
Credit and Collection MGR (Ida Peña) [17]
Planning and Treasury MGR (Asaf Piscoya) [10]
Branches [26]
Infrastructure (R. Rodriguez) [2]
Infrastructure maintenance (Jorge Quispe) [5]
Audit [4]
Internal Control [2]
Legal Advise (Jhoanna Vargas) [4]
Compliance [2]
Infrastructure IT (Open) [3]
Application IT (Carlos Valerio) [8]
Information Security (Marcos Pinto) [3]
Management and Services IT (Jose Camino) [4]

III. Justificación

La propuesta planteada se justifica debido a que se espera ejecutar varias estrategias que están alineadas con los objetivos y valores de la compañía, además los resultados de la aplicación permitirán mejorar la conciencia de los recursos humanos frente a las amenazas cibernéticas, cómo identificarlas y qué hacer cuando estén frente a ellas.

IV. Objetivos

4.1 Objetivo general

Concientizar al colaborador sobre las amenazas cibernéticas a las que está expuesto, enseñarles a identificarlas e indicarles qué hacer cuando estén frente a ellas.

4.2 Objetivos específicos

- Diseñar las estrategias de concientización y capacitación para mejorar la cultura informática de los colaboradores.
- Establecer las actividades a desarrollar por cada estrategia propuesta, asignar responsables, recursos, fechas y presupuesto.

V. Meta

El resultado que se espera obtener en la ejecución de esta propuesta es mejorar significativamente la conciencia de los colaboradores de la compañía sobre las amenazas cibernéticas a las que están expuestos, conllevando así, el tratamiento de riesgos de la matriz de riesgos de la compañía, evitando perdidas y gastos por ataques, además de un ahorro en el pago del ciberseguro de la empresa.

VI. Acciones a desarrollar

Plan de Acción de la Propuesta

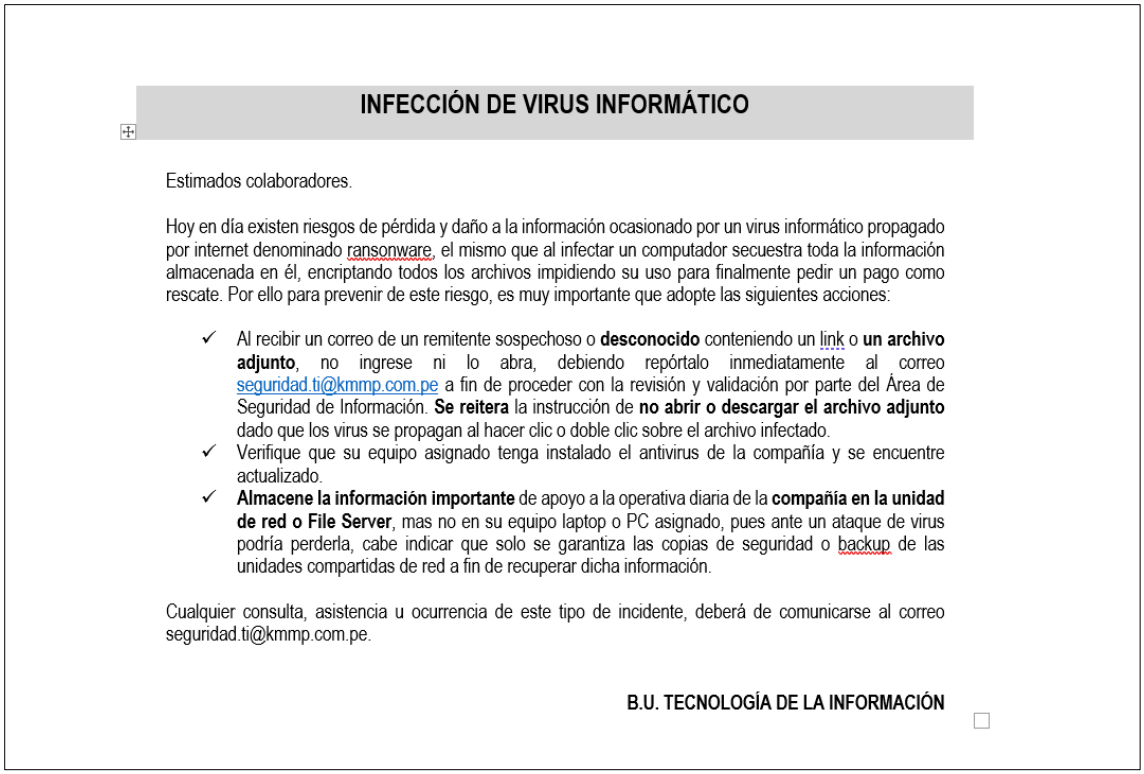
Estrategia	Objetivo	Actividad	Responsable
Estrategia 1: Plan de difusión comunicados de Seguridad de la Información.	Utilizar los medios de comunicación corporativa para capacitar y comunicar aspectos importantes y recomendaciones de Seguridad de la información.	• Redactar comunicados de seguridad de la información, ciberseguridad y trabajo seguro con dispositivos finales. • Crear una programación de difusión de comunicados. • Coordinar con el área de comunicaciones corporativas la correcta redacción de los comunicados y la programación de difusión. • Presentar a la Gerencia de TI, la programación y solicitar el visto bueno para su ejecución.	Carrasco Ramirez, David Agusto.
Estrategia 2: Campañas de simulación de ataques de ingeniería social con concientización instantánea.	Concientizar en base a ejemplos de ataques cibernéticos de ingeniería social a los colaboradores de la compañía.	• Ejecutar las campañas de simulación mensualmente. • Cada colaborador víctima recibirá un mensaje de concientización instantánea. • Los colaboradores víctimas recibirán un correo de parte de la Sub – Gerencia de Seguridad de la Información o la Gerencia de TI, indicando que ha sido víctima de una simulación de ataque y dándole recomendaciones para una futura ocasión. • Los colaboradores reincidentes en 3 oportunidades de manera consecutiva recibirán una amonestación formal de parte de la Sub – Gerencia de Seguridad de la Información o la Gerencia de TI, indicando que ha atentado contra los lineamientos de la Normativa Interna de Seguridad de la Información.	Carrasco Ramirez, David Agusto.

		• Los colaboradores reincidentes recibirán una llamada de parte del personal del área de Seguridad de información para capacitarlo de manera particular.	
Estrategia 3: Publicación de contenido audiovisual de Seguridad de la Información.	Informar, concientizar y capacitar en seguridad de la información y ciberseguridad mediante vídeos cortos difundidos por los medios de comunicación corporativa.	• Redactar el guion. • En coordinación con Comunicaciones corporativas realizar la grabación de los vídeos. • Solicitar el visto bueno para difusión del contenido. • Difundir los contenidos mediante los medios de comunicación corporativa.	Carrasco Ramirez, David Agusto.
Estrategia 4: Inducciones Corporativas	Capacitar y concientizar a todos los nuevos ingresos de la compañía.	• Diseñar y redactar una presentación que esté alineada a los lineamientos de la Normativa interna de Seguridad de la Información. • Coordinar con el área Recursos Humanos las sesiones de inducción cuando se integren más miembros a la compañía. • Evaluar dentro del tiempo de la sesión el entendimiento de los nuevos colaboradores sobre la capacitación realizada.	Carrasco Ramirez, David Agusto.
Estrategia 5 Monitoreo de efectividad de controles de SI ligados a los recursos humanos.	Evaluar la efectividad de los controles de seguridad de la información que protegen a los activos de información y al factor humano.	• En coordinación con el área de Control Interno, diseñar las evidencias y criterios de evaluación con los que se evaluará la efectividad de controles, según la matriz de riesgos - compañía. • Crear un cronograma y solicitar visto bueno de la Gerencia TI. • Realizar la evaluación de los controles y subsanar las brechas o vulnerabilidades encontradas.	Carrasco Ramirez, David Agusto.

Estrategia 1: Plan de difusión comunicados de Seguridad de la Información.

Actividad: Redactar comunicados de seguridad de la información, ciberseguridad y trabajo seguro con dispositivos finales.

Los comunicados fueron redactados en el software de oficina Microsoft Word, y pasaron por diferentes filtros de revisión antes de ser publicados.



INFECCIÓN DE VIRUS INFORMÁTICO

Estimados colaboradores.

Hoy en día existen riesgos de pérdida y daño a la información ocasionado por un virus informático propagado por internet denominado ransonware, el mismo que al infectar un computador secuestra toda la información almacenada en él, encriptando todos los archivos impidiendo su uso para finalmente pedir un pago como rescate. Por ello para prevenir de este riesgo, es muy importante que adopte las siguientes acciones:

- ✓ Al recibir un correo de un remitente sospechoso o **desconocido** conteniendo un link o **un archivo adjunto**, no ingrese ni lo abra, debiendo repórtalo inmediatamente al correo seguridad.ti@kmmp.com.pe a fin de proceder con la revisión y validación por parte del Área de Seguridad de Información. **Se reitera** la instrucción de **no abrir o descargar el archivo adjunto** dado que los virus se propagan al hacer clic o doble clic sobre el archivo infectado.
- ✓ Verifique que su equipo asignado tenga instalado el antivirus de la compañía y se encuentre actualizado.
- ✓ **Almacene la información importante** de apoyo a la operativa diaria de la **compañía en la unidad de red o File Server**, mas no en su equipo laptop o PC asignado, pues ante un ataque de virus podría perderla, cabe indicar que solo se garantiza las copias de seguridad o backup de las unidades compartidas de red a fin de recuperar dicha información.

Cualquier consulta, asistencia u ocurrencia de este tipo de incidente, deberá de comunicarse al correo seguridad.ti@kmmp.com.pe.

B.U. TECNOLOGÍA DE LA INFORMACIÓN

Actividad: Crear una programación de difusión de comunicados.

Se podrá encontrar la programación en la parte de cronogramas con el nombre “Cronograma de la estrategia, “Plan de difusión comunicados de Seguridad de la Información””.

Actividad: Coordinar con el área de comunicaciones corporativas la correcta redacción de los comunicados y la programación de difusión.

A continuación, mostraremos un ejemplo de los correos de coordinación con el área de comunicaciones corporativas, por cada comunicado publicado se envió una solicitud.

De: David Carrasco Ramirez <david.carrasco@kmmp.com.pe>
Enviado: miércoles, 6 de abril de 2022 10:23
Para: Dayana <dayana.>
Cc: Marcos <marcos.>; seguridad.ti <seguridad.>
Asunto: Solicito difusión de mensaje prevención "INFECCIÓN DE VIRUS INFORMÁTICO"

Señorita Dayana, buen día.

Esperando que se encuentre bien al igual que su familia. Favor su apoyo difundiendo el mensaje adjunto a los colaboradores de toda la Compañía según el flujo de comunicados establecido. Asimismo, favor de enviar el modelo del comunicado.

Gracias.

Atte.

David Carrasco Ramirez
Practicante de Seguridad de la Información
Komatsu-Mitsui Maquinarias Perú S.A.
C. 922564060
www.kmmp.com.pe

RE: Solicito difusión de mensaje prevención "INFECCIÓN DE VIRUS INFORMÁTICO"

David Carrasco Ramirez
Para Dayana
CC Marcos seguridad.ti

Responder | Responder a todos | Reenviar

miércoles 6/04/2022 14:42

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Conforme, proceder con el comunicado.

Gracias.

Atte.

David Carrasco Ramirez
Practicante de Seguridad de la información
Komatsu-Mitsui Maquinarias Perú S.A.
C. 922564060
www.kmmp.com.pe

De: Dayana <dayana.>
Enviado: miércoles, 6 de abril de 2022 13:57
Para: David Carrasco Ramirez <david.carrasco@kmmp.com.pe>
Cc: Marcos <marcos.>; seguridad.ti <seguridad.>
Asunto: RE: Solicito difusión de mensaje prevención "INFECCIÓN DE VIRUS INFORMÁTICO"

Hola @David Carrasco Ramirez
Te remito el modelo de comunicado para tu validación:
https://r.mail.komatsu.pe/mk/mr/D8eULLuqVNIBIJF1zl7_jNdyP7PSgjcByuo2qgJ05bwnNyIeBPLEkBO3-zP-Bdal2jyKlyeqpW7gpkU6jE74u9yCqVXuk5R4UZxf1jaycFuuzoGTtOmILwXlQc_HX5HUog
Me comentas, quedo atenta,

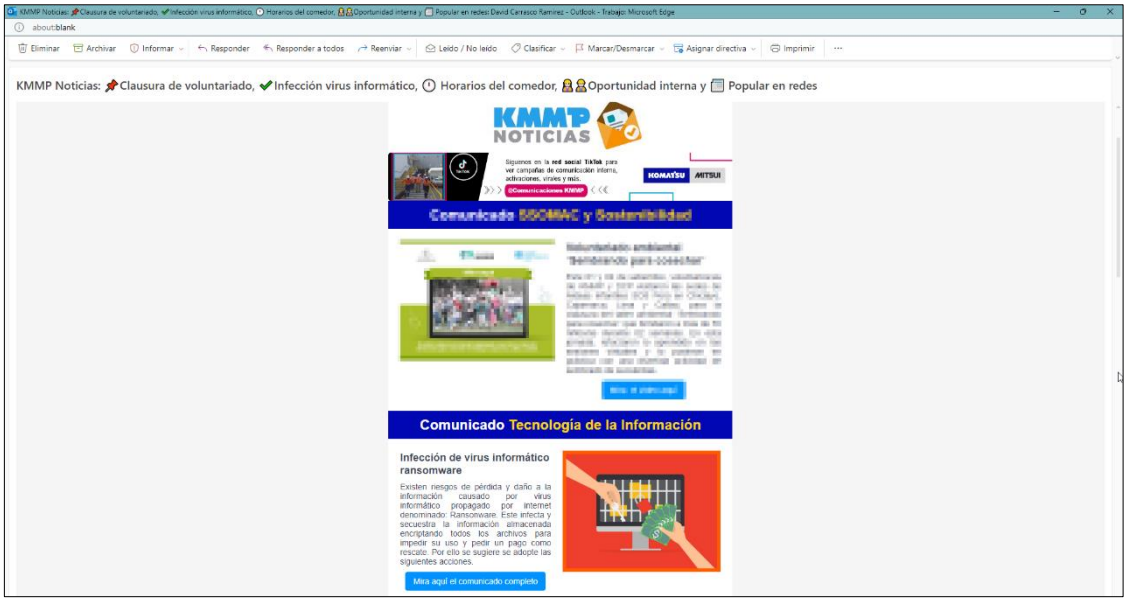
Dayana
Analista de Comunicaciones y Redes
Komatsu Mitsui Maquinarias Perú S.A.
T. (511)
C. (51)
www.kmmp.com.pe

Actividad: Presentar a la Gerencia de TI, la programación y solicitar el visto bueno para su ejecución.

Una vez se tenía el comunicado listo para su difusión se solicitaba el visto bueno de la Gerencia de TI, mostrándole el comunicado resultado; a continuación, un ejemplo:

Actividad: Publicar los comunicados.

Una vez se cumplía todo el proceso se publicaban los comunicados mediante el boletín de noticas KMMP.

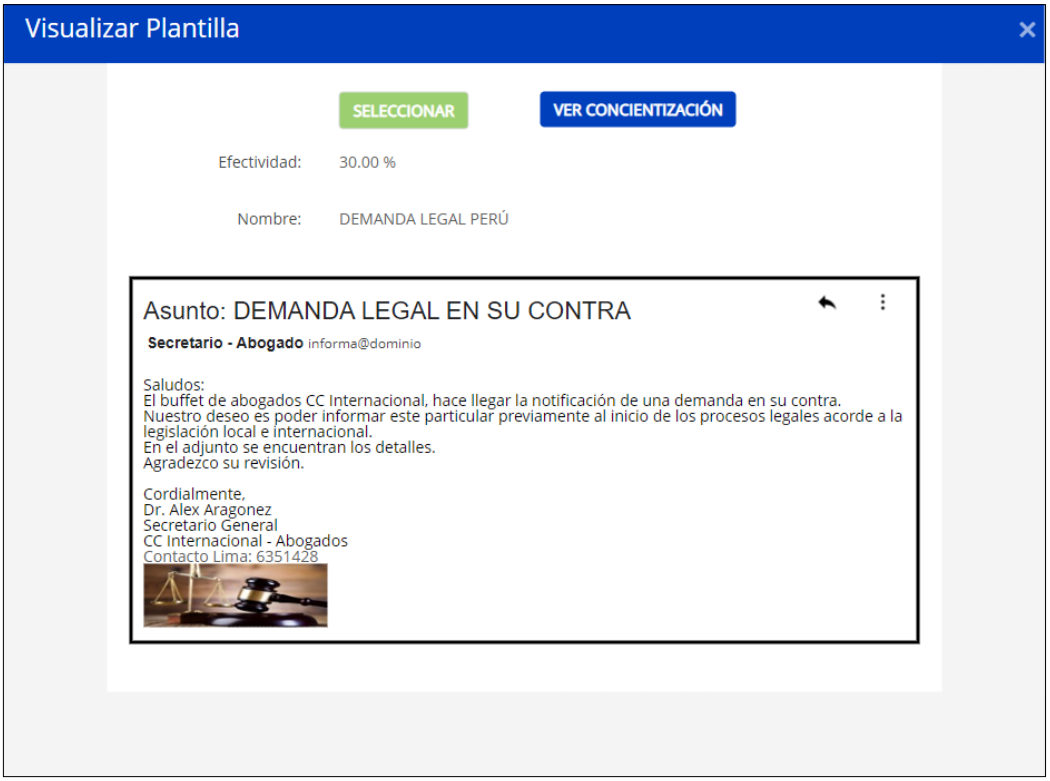


Estrategia 2: Campañas de simulación de ataques de ingeniería social con concientización instantánea.

Actividad: Planificación de la campaña.

Primero preparábamos el contenido que será utilizado en la campaña, realizábamos las pruebas y solicitábamos el visto bueno de la Gerencia de TI.

1. Preparación del contenido.



2. Envío de pruebas al equipo de Seguridad.

TEST03 - EQSEG - NOV22	16/11/2022 12:30	INFECCIÓN (RANSOMWARE)	PERÚ PROMOCIÓN GLOBO AEROSTÁTICO	CORREO ELECTRÓNICO	4	1	25,00
TEST02 - EQSEG - NOV22	16/11/2022 12:30	INFECCIÓN (RANSOMWARE)	PERÚ - SUBSIDIO LUZ - CON ADJUNTO V1	CORREO ELECTRÓNICO	4	2	50,00
TEST01 - EQSEG - NOV22	16/11/2022 12:30	INFECCIÓN (RANSOMWARE)	VISA CONFIRMACIÓN PAGO BLACK FRIDAY CON LINK V1	CORREO ELECTRÓNICO	4	2	50,00

3. Solicitud de visto bueno con el contenido listo para su despliegue.

DEMANDA LEGAL EN SU CONTRA - PROCESO RP00372

Reenvió este mensaje el Vie 23/09/2022 17:33.

SA Secretario - Abogado <informa@xn--goberno-qza.com>

Para: David Carrasco Ramirez

Mié 21/09/2022 9:43

David Carrasco.htm
506 bytes

Defensoría del Pueblo — Mesa de Partes Virtual

Saludos David Carrasco:
El buffet de abogados de la Defensoría del Pueblo, le informa que hemos receptado una demanda presentada en su contra.
Nuestro objetivo es avisarle de este particular previo los procesos legales que se seguirán acorde a la legislación local.
En el adjunto se encuentran los detalles, agradecemos su revisión.

Dr. Fernando Cuadrado Fonseca
Secretario General
21 de Setiembre, 2022

(*) Subsanada la observación y/o aprobado el documento, este se tendrá por recibido en la fecha en la que se depositó en la mesa de partes virtual.

Actividad: Ejecutar las campañas de simulación.

Se envían el contenido preparado a todos los colaboradores activos de la compañía. Recibiendo también sus reportes al grupo de seguridad TI y Mesa de Servicios de TI.

RE: COMPRA - FACTURA 001-5589-001

De: Jhon <jhon.>
Enviado: martes, 22 de marzo de 2022 11:52
Para: seguridad seguridad
Cc: Marcos <marcos.>
Asunto: RV: COMPRA - FACTURA 001-5589-001

Estimado, buenos días.

Por favor su revisión de este correo que aparentemente sería malicioso.

Saludos,

Jhon
Auditor
Komatsu-Mitsui Maquinarias Perú S.A.
www.kmmp.com.pe

De: Facturación <factura@deptsistemas.com>
Enviado: lunes, 21 de marzo de 2022 14:15
Para: Jhon
Asunto: COMPRA - FACTURA 001-5589-001

plazavea

Estimado/a JHON :
Le comunicamos por este medio que usted ha recibido los comprobantes respectivos por su compra, para verificar que los precios están correctos, por favor revise el adjunto.
Por su confianza, estamos muy agradecidos

PLAZAVEA

RE: COMPRA - FACTURA 001-5589-001

JC Jhon
Para: David Carrasco Ramirez; seguri
Mar 22/03/2022 14:11

Gracias,

Saludos,

Jhon
Auditor Especialista - Auditoria
Komatsu-Mitsui Maquinarias Perú S.A.
www.kmmp.com.pe

De: David Carrasco Ramirez <david.carrasco@kmmp.com.pe>
Enviado: martes, 22 de marzo de 2022 12:51
Para: Jhon ;
Asunto: RE: COMPRA - FACTURA 001-5589-001

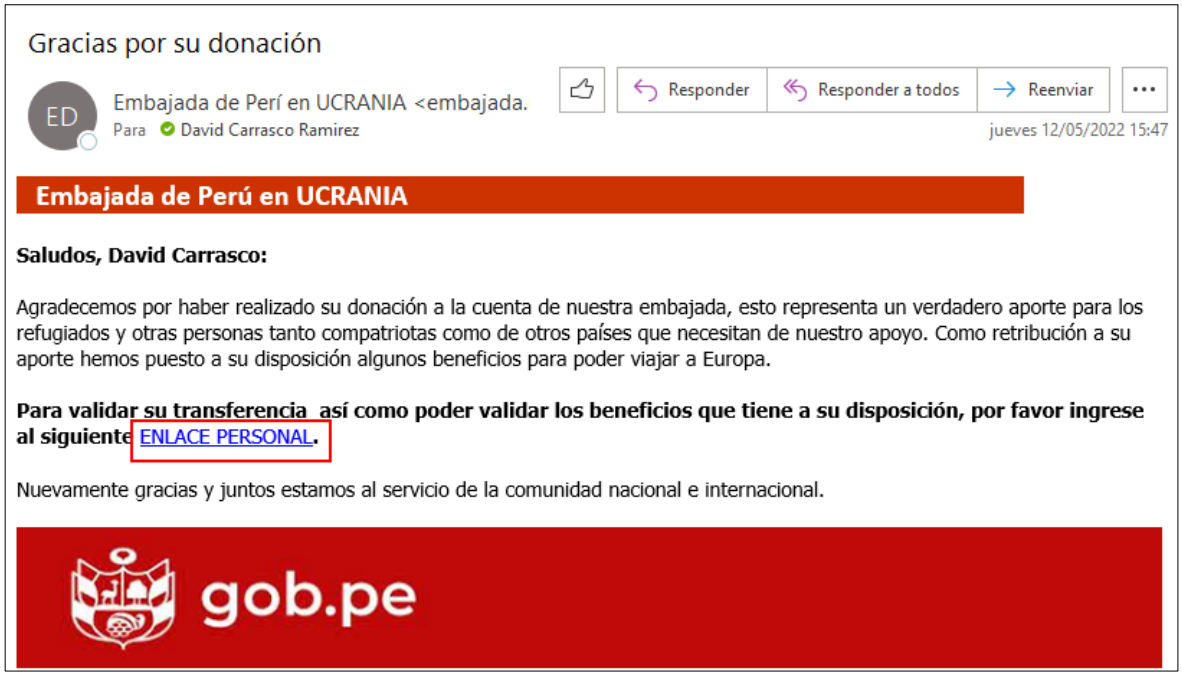
Estimado Jhon.

Agradecemos el reporte del correo confirmando que este tiene todas las características de phishing siendo sospechoso, favor de no abrir el archivo adjunto o link y proceder con su eliminación. Continúe con el reporte de este tipo de correos y gracias por su debida diligencia.

Gracias.

Actividad: Cada colaborador víctima recibirá un mensaje de concientización instantánea.

Los colaboradores que caigan víctimas en la simulación ingresando al link o descargando el archivo adjunto recibirán un mensaje de concientización instantáneo.



Gracias por su donación

ED

Embajada de Perí en UCRANIA <embajada.

Para David Carrasco Ramirez

Responder | Responder a todos | Reenviar | ...

jueves 12/05/2022 15:47

Embajada de Perú en UCRANIA

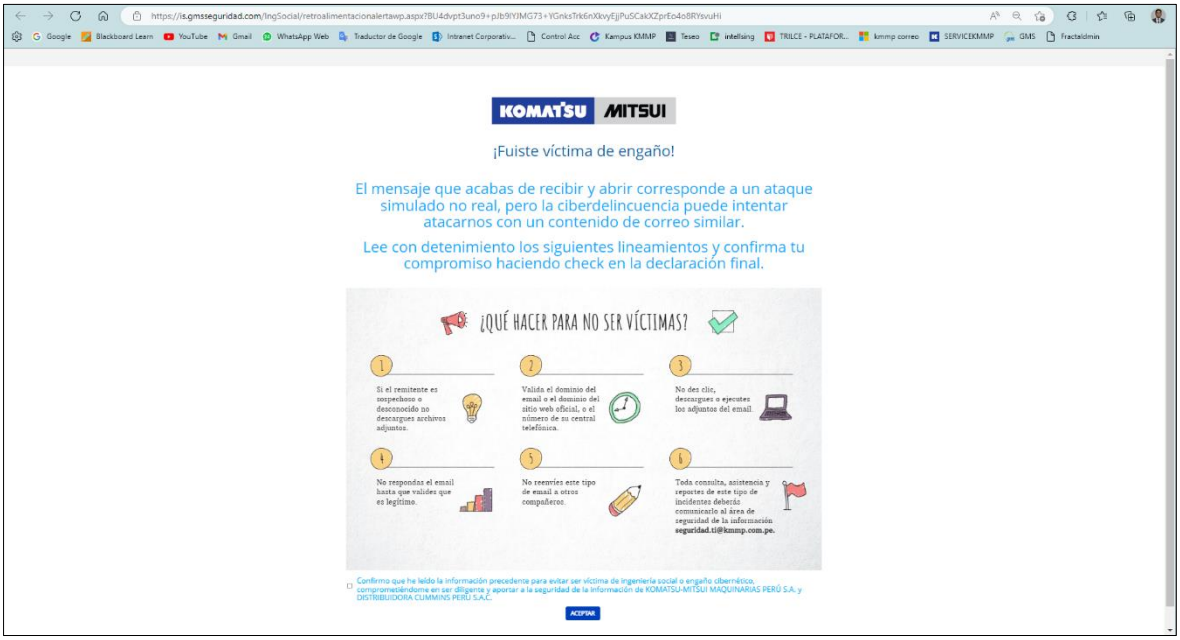
Saludos, David Carrasco:

Agradecemos por haber realizado su donación a la cuenta de nuestra embajada, esto representa un verdadero aporte para los refugiados y otras personas tanto compatriotas como de otros países que necesitan de nuestro apoyo. Como retribución a su aporte hemos puesto a su disposición algunos beneficios para poder viajar a Europa.

Para validar su transferencia así como poder validar los beneficios que tiene a su disposición, por favor ingrese al siguiente ENLACE PERSONAL.

Nuevamente gracias y juntos estamos al servicio de la comunidad nacional e internacional.

gob.pe



KOMATSU MITSUI

¡Fuiste víctima de engaño!

El mensaje que acabas de recibir y abrir corresponde a un ataque simulado no real, pero la ciberdelincuencia puede intentar atacarnos con un contenido de correo similar.

Lee con detenimiento los siguientes lineamientos y confirma tu compromiso haciendo check en la declaración final.

¿QUÉ HACER PARA NO SER VÍCTIMAS?

1. Si el remitente es sospechoso o desconocido no descargues archivos adjuntos.
2. Valida el dominio del email o el dominio del sitio web oficial, o el número de su central telefónica.
3. No des clic, descargues o ejecutes los adjuntos del email.
4. No respondas el email hasta que valides que es legítimo.
5. No reenvíes este tipo de email a otros compañeros.
6. Toda consulta, asistencia y reportes de este tipo de incidentes deberán comunicarlo al área de seguridad de la información **seguridad.ti@kmmp.com.pe.**

Confirmo que he leído la información precedente para evitar ser víctima de ingeniería social o engaño cibernético, comprometiéndome en ser diligente y aportar a la seguridad de la información de KOMATSU-MITSUI MAQUINARIAS PERÚ S.A. y DISTRIBUIDORA CUMMINS PERÚ S.A.C.

ACEPTAR

Actividad: Los colaboradores víctimas recibirán un correo de parte de la Sub – Gerencia de Seguridad de la Información o la Gerencia de TI, indicando que ha sido víctima de una simulación de ataque y dándole recomendaciones para una futura ocasión.

Los colaboradores que caigan víctimas en la simulación ingresando al link o descargando el archivo adjunto recibirán otro mensaje de concientización después de unos días de la acción.

RE: Cumplir con lineamientos de seguridad para evitar ataques cibernéticos.

De: Marcos [redacted]
Enviado: martes, 8 de marzo de 2022 9:15
Asunto: Cumplir con lineamientos de seguridad para evitar ataques cibernéticos.

Estimado(a) colaborador(a),
Saludos.

Semanas atrás recordara haber recibido el siguiente correo sospechoso:

Asunto: Aviso de cobro y sanciones por pagos pendientes

JEFATURA LEGAL

AVISO DE COBRO POR RETRASO EN PAGOS

Saludos cordiales.

Su proveedor de servicios de Telecomunicaciones, le informa que de la revisión de su historial de pagos se registra que usted mantiene una deuda pendiente con nuestra empresa, con el fin de evitar mayores inconvenientes tanto en incremento de intereses por mora así como posibles procesos judiciales, **se detallan en el adjunto los v pendientes y las formas de pago habilitadas, por favor revise la información y evite sanciones más graves.**

Agradecemos su atención y pronta gestión a este asunto.

Gerencia de Asuntos Legales

América Móvil Perú S.A.C.

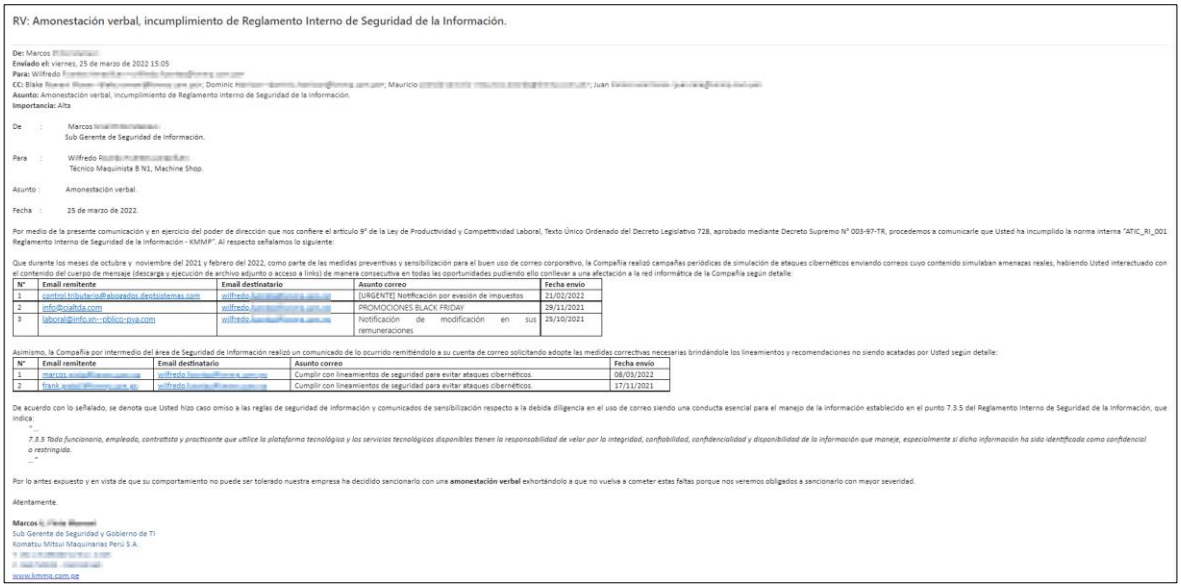
Av. Nicolás Arriola 314 Oficina. 1201 – La Victoria – Lima - Perú

Dicho mensaje formaba parte de una campaña de concienciación que nuestra área de TI viene efectuando a fin de validar el debido cuidado de nuestros colaboradores en el uso del correo electrónico de la Compañía a fin de mitigar riesgos cibernéticos. Dicho correo formaba parte de una simulación de ataque informático Ransomware (software dañino similar a un virus que secuestra información) propagado por correo. En razón de ello, hemos observado que Ud. habría recibido el correo en mención y abierto el archivo adjunto incluido en su contenido, situación que de haber sido un ataque real habría ocasionado perdida de información de su equipo de cómputo asignado así como a la red de la compañía.

Por lo antes indicado se le recalca cumplir con las siguientes lineamientos:

Actividad: Los colaboradores reincidentes en 3 oportunidades de manera consecutiva recibirán una amonestación formal de parte de la Sub – Gerencia de Seguridad de la Información o la Gerencia de TI, indicando que ha atentado contra los lineamientos de la Normativa Interna de Seguridad de la Información.

Los colaboradores que caigan víctimas en la simulación ingresando al link o descargando el archivo adjunto 3 veces de manera consecutiva recibirán una amonestación formal.



RV: Amonestación verbal, incumplimiento de Reglamento Interno de Seguridad de la Información.

De: Marcos
Enviado el: viernes, 25 de marzo de 2022 15:05
Para: Wilfredo
CC: Blake Rowan, Dominic Harrison, Mauricio, Juan
Asunto: Amonestación verbal, incumplimiento de Reglamento Interno de Seguridad de la Información.
Importancia: Alta

De : Marcos
Sub Gerente de Seguridad de Información.

Para : Wilfredo
Técnico Maquinista B N1, Machine Shop.

Asunto : Amonestación verbal.

Fecha : 25 de marzo de 2022.

Por medio de la presente comunicación y en ejercicio del poder de dirección que nos confiere el artículo 9° de la Ley de Productividad y Competitividad Laboral, Texto Único Ordenado del Decreto Legislativo 728, aprobado mediante Decreto Supremo N° 003-97-TR, procedemos a comunicarle que Usted ha incumplido la norma interna "ATIC_RI_001 Reglamento Interno de Seguridad de la Información - KMMP". Al respecto señalamos lo siguiente:

Que durante los meses de octubre y noviembre del 2021 y febrero del 2022, como parte de las medidas preventivas y sensibilización para el buen uso de correo corporativo, la Compañía realizó campañas periódicas de simulación de ataques cibernéticos enviando correos cuyo contenido simulaban amenazas reales, habiendo Usted interactuado con el contenido del cuerpo de mensaje (descarga y ejecución de archivo adjunto o acceso a links) de manera consecutiva en todas las oportunidades pudiendo ello conllevar a una afectación a la red informática de la Compañía según detalle:

N°	Email remitente	Email destinatario	Asunto correo	Fecha envio
1	[redacted]	[redacted]	[URGENTE] Notificación por evasión de impuestos	21/02/2021
2	[redacted]	[redacted]	PROMOCIONES BLACK FRIDAY	29/11/2021
3	[redacted]	[redacted]	Notificación de modificación en sus remuneraciones	29/10/2021

Asimismo, la Compañía por intermedio del área de Seguridad de Información realizó un comunicado de lo ocurrido remitiéndolo a su cuenta de correo solicitando adopte las medidas correctivas necesarias brindándole los lineamientos y recomendaciones no siendo acatadas por Usted según detalle:

N°	Email remitente	Email destinatario	Asunto correo	Fecha envio
1	[redacted]	[redacted]	Cumplir con lineamientos de seguridad para evitar ataques cibernéticos.	08/03/2022
2	[redacted]	[redacted]	Cumplir con lineamientos de seguridad para evitar ataques cibernéticos.	17/11/2021

De acuerdo con lo señalado, se denota que Usted hizo caso omiso a las reglas de seguridad de información y comunicados de sensibilización respecto a la debida diligencia en el uso de correo siendo una conducta esencial para el manejo de la información establecido en el punto 7.3.5 del Reglamento Interno de Seguridad de la Información, que indica:

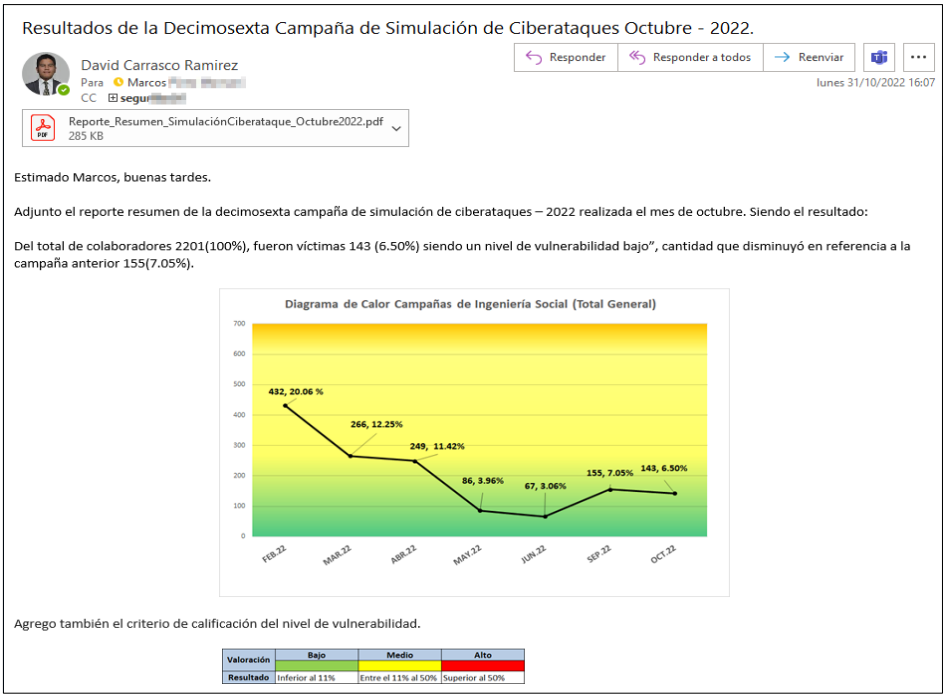
"...
7.3.5 Todo funcionario, empleado, contratista y practicante que utilice la plataforma tecnológica y los servicios tecnológicos disponibles tienen la responsabilidad de velar por la integridad, confiabilidad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información ha sido identificada como confidencial o restringida.
..."

Por lo antes expuesto y en vista de que su comportamiento no puede ser tolerado nuestra empresa ha decidido sancionarlo con una **amonestación verbal** exhortándolo a que no vuelva a cometer estas faltas porque nos veremos obligados a sancionarlo con mayor severidad.

Atentamente.

Marcos
Sub Gerente de Seguridad y Gobierno de TI
Komatsu Mitsui Maquinarias Perú S.A.
www.kmmp.com.pe

Actividad: Reporte de resultados a la Gerencia de TI.
Por cada campaña de simulación ejecutada se realizaba un informe gerencial que permita visualizar los resultados, además de categorizar el nivel de vulnerabilidad.



Resultados de la Decimosexta Campaña de Simulación de Ciberataques Octubre - 2022.

David Carrasco Ramirez
Para Marcos
CC segur

Responder | Responder a todos | Reenviar

lunes 31/10/2022 16:07

Reporte_Resumen_SimulaciónCiberataque_Octubre2022.pdf
285 KB

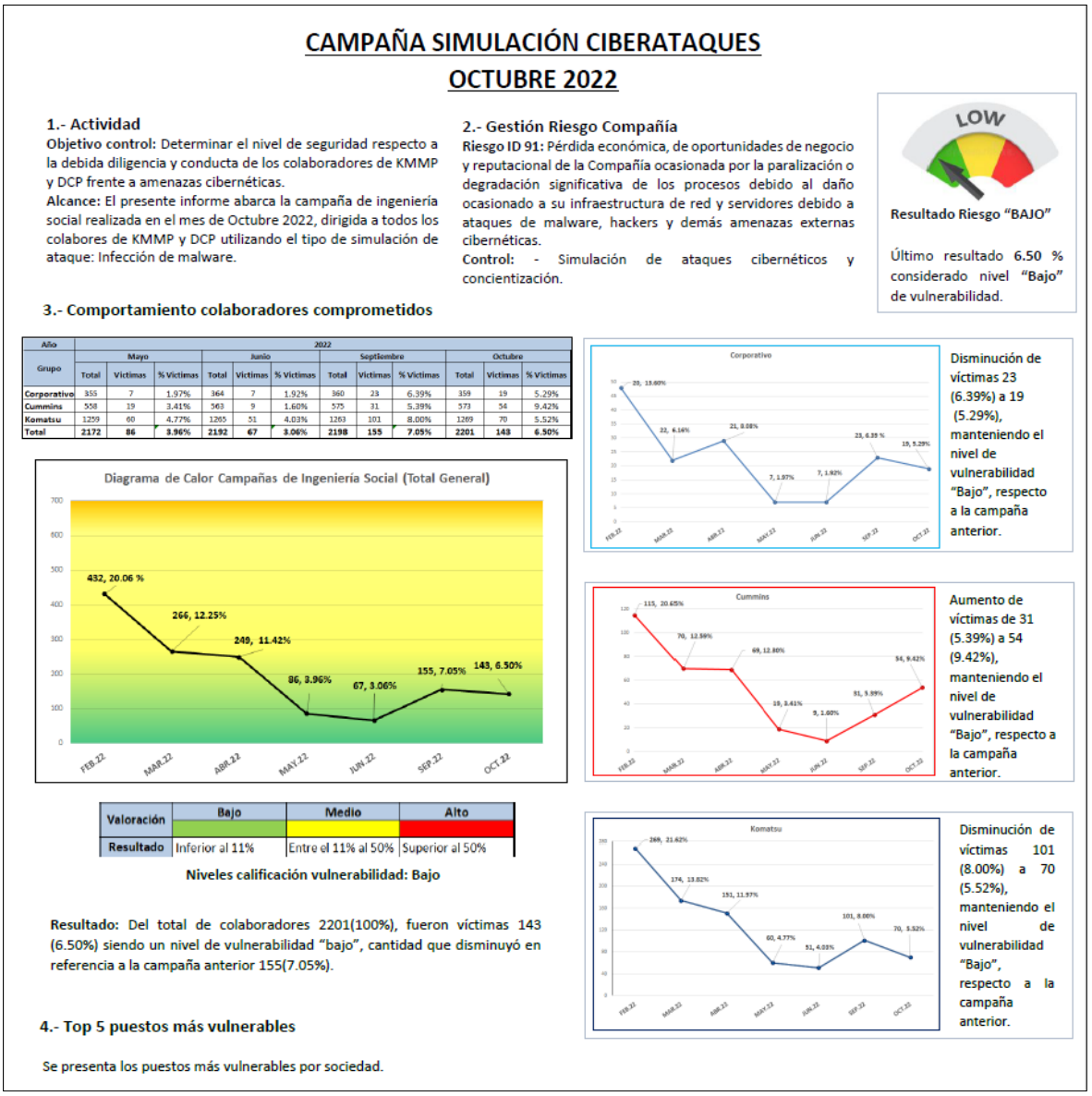
Estimado Marcos, buenas tardes.

Adjunto el reporte resumen de la decimosexta campaña de simulación de ciberataques – 2022 realizada el mes de octubre. Siendo el resultado:

Del total de colaboradores 2201(100%), fueron víctimas 143 (6.50%) siendo un nivel de vulnerabilidad bajo", cantidad que disminuyó en referencia a la campaña anterior 155(7.05%).

Agrego también el criterio de calificación del nivel de vulnerabilidad.

Valoración	Bajo	Medio	Alto
Resultado	Inferior al 11%	Entre el 11% al 50%	Superior al 50%



CAMPAÑA SIMULACIÓN CIBERATAQUES
OCTUBRE 2022

1.- Actividad

Objetivo control: Determinar el nivel de seguridad respecto a la debida diligencia y conducta de los colaboradores de KMMP y DCP frente a amenazas cibernéticas.

Alcance: El presente informe abarca la campaña de ingeniería social realizada en el mes de Octubre 2022, dirigida a todos los colabores de KMMP y DCP utilizando el tipo de simulación de ataque: Infección de malware.

2.- Gestión Riesgo Compañía

Riesgo ID 91: Pérdida económica, de oportunidades de negocio y reputacional de la Compañía ocasionada por la paralización o degradación significativa de los procesos debido al daño ocasionado a su infraestructura de red y servidores debido a ataques de malware, hackers y demás amenazas externas cibernéticas.

Control: - Simulación de ataques cibernéticos y concientización.

LOW

Resultado Riesgo "BAJO"

Último resultado **6.50 %** considerado nivel **"Bajo"** de vulnerabilidad.

3.- Comportamiento colaboradores comprometidos

Año	2022											
Grupo	Mayo			Junio			Septiembre			Octubre		
	Total	Victimas	% Victimas	Total	Victimas	% Victimas	Total	Victimas	% Victimas	Total	Victimas	% Victimas
Corporativo	355	7	1.97%	364	7	1.92%	360	23	6.39%	359	19	5.29%
Cummins	558	19	3.41%	563	9	1.60%	575	31	5.39%	573	54	9.42%
Komatsu	1259	60	4.77%	1265	51	4.03%	1263	101	8.00%	1269	70	5.52%
Total	2172	86	3.96%	2192	67	3.06%	2198	155	7.05%	2201	143	6.50%

Valoración	Bajo	Medio	Alto
Resultado	Inferior al 11%	Entre el 11% al 50%	Superior al 50%

Niveles calificación vulnerabilidad: Bajo

Disminución de víctimas 23 (6.39%) a 19 (5.29%), manteniendo el nivel de vulnerabilidad "Bajo", respecto a la campaña anterior.

Aumento de víctimas de 31 (5.39%) a 54 (9.42%), manteniendo el nivel de vulnerabilidad "Bajo", respecto a la campaña anterior.

Disminución de víctimas 101 (8.00%) a 70 (5.52%), manteniendo el nivel de vulnerabilidad "Bajo", respecto a la campaña anterior.

Resultado: Del total de colaboradores 2201(100%), fueron víctimas 143 (6.50%) siendo un nivel de vulnerabilidad "bajo", cantidad que disminuyó en referencia a la campaña anterior 155(7.05%).

4.- Top 5 puestos más vulnerables

Se presenta los puestos más vulnerables por sociedad.

Estrategia 3: Producción y publicación de contenido audiovisual de Seguridad de la Información.

Actividad: Redactar el guion.

Los guiones fueron redactados en el software de oficina Microsoft Word, y pasaron por diferentes filtros de revisión antes de pasar a la etapa de producción.

GUIÓN DE VÍDEO DE SI

ESCENA 1:

HOLA, SOY DAVID CARRASCO DEL TEAM DE TECNOLOGÍAS DE INFORMACIÓN Y HOY VAMOS A HABLAR SOBRE LOS CORREOS MALICIOSOS:

ESCENA 2:

POR ESO, SI RECIBES UN CORREO ELECTRÓNICO CON ESTÁS CARACTERISITICAS ¡TEN CUIDADO!

1. REMITENTE DESCONOCIDO: ¿ESPERABAS UN CORREO DE ESTA PERSONA O EMPRESA?
2. ASUNTO LLAMATIVO: ¿EL CORREO DICE SER "URGENTE", "IMPORTANTE" O TE DICE QUE "GANASTE" ALGO?
3. ADJUNTO SOSPECHOSO: ¿REALMENTE EL CORREO JUSTIFICA LA DESCARGA DE UN ARCHIVO ADJUNTO?
4. ERRORES ORTOGRÁFICOS: ¿EL CORREO ESTÁ MAL REDACTADO O TIENE ENTRE SUS LÍNEAS PALABRAS MAL ESCRITAS?
5. ENLACES DUDOSOS: ¿EL CORREO TE INDUCE A INGRESAR A UN ENLACE SOSPECHOSO?

Escena 3:

EN ESTA SITUACIÓN ¿QUÉ DEBEMOS HACER?

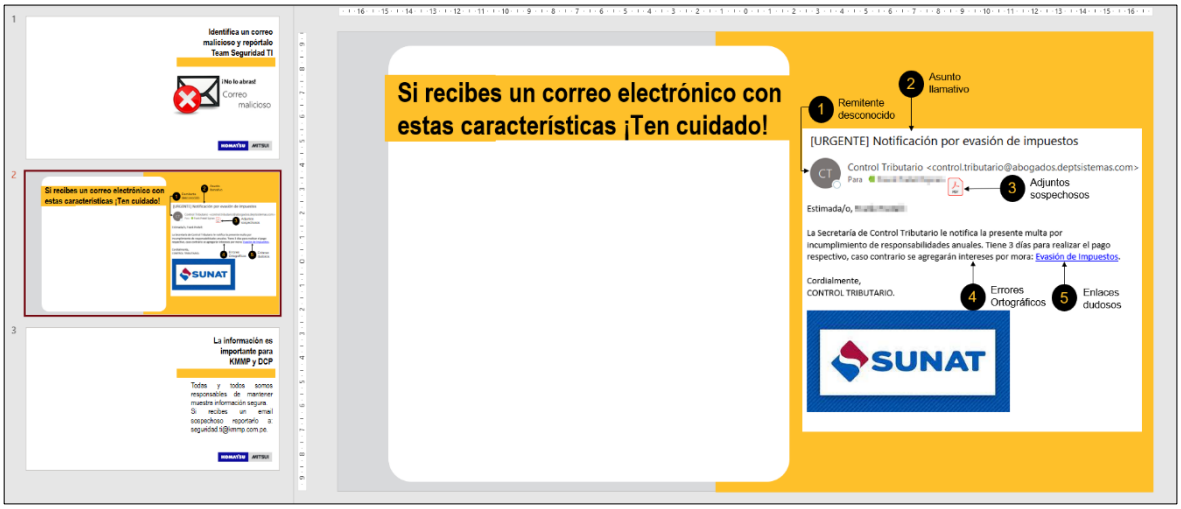
Recuerda que Todas y todos somos responsables de mantener muestra información segura.

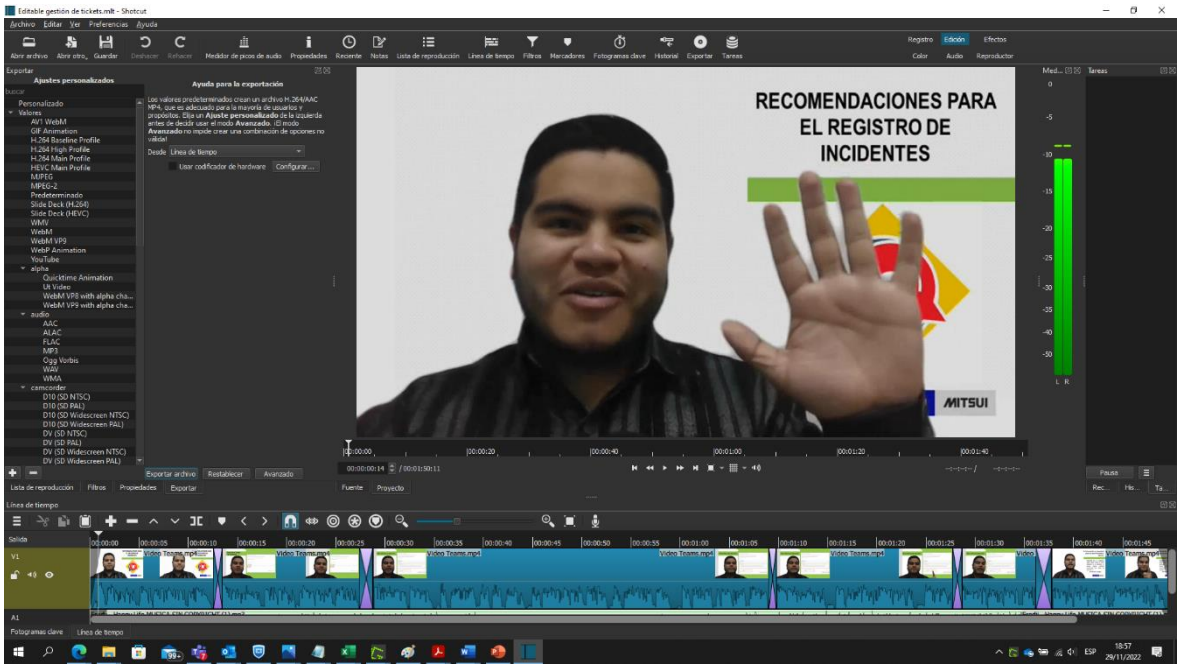
Si recibes un email sospechoso reportarlo a: seguridad [redacted]

¡¡CONTAMOS CONTIGO!!

Actividad: En coordinación con Comunicaciones corporativas realizar la grabación de los vídeos.

Se prepararon los escenarios y se procedió a la grabación del contenido.





Actividad: Solicitar el visto bueno para difusión del contenido.

Con el contenido listo para su difusión se solicitó el visto bueno de las áreas correspondientes.

Inicio de proyecto multimedia Seguridad TI (Estandares de Video)

Dayana [redacted]
Para David Carrasco Ramirez; Marcos [redacted]
CC Juan [redacted] Andrea [redacted]

Responder | Responder a todos | Reenviar | ...

jueves 28/04/2022 11:24

Hola David, Marcos, Juan Carlos y Andrea:
Hemos iniciado con el equipo de seguridad de la información el re diseño de los procesos para elaboración de contenidos con esta inciativa para poder aumentar y asegurar la rapidez de las comunicaciones del equipo. Comparto el archivo en referencia:
Fuente: https://web.microsoftstream.com/embed/video/9d88e0b3-d909-43c3-b812-0d9eeb8a04af?autoplay=true&showinfo=true&st=1
Este hito significa el reemplazo de uso de cámaras especializadas, el uso de la plataforma Teams para el propósito, el diseño de fondos para el expositor y grabación en tiempo récord del spot de 50 segundos. El plazo de entrega se realizó en menos de 1 día.
Este nuevo formato permite que mensajes atemporales utilicen el multimedia en base a los recursos que como compañía disponemos en nuestro soporte Nativo en Stream y Onedrive y facilite la producción masiva.

Agradezco la confianza al equipo que dirige Marcos Pinto y a David por animarse tentar una nueva forma de llegar a sus clientes eficiente y que productivamente es más ágil de diseñar, producir y compartir.

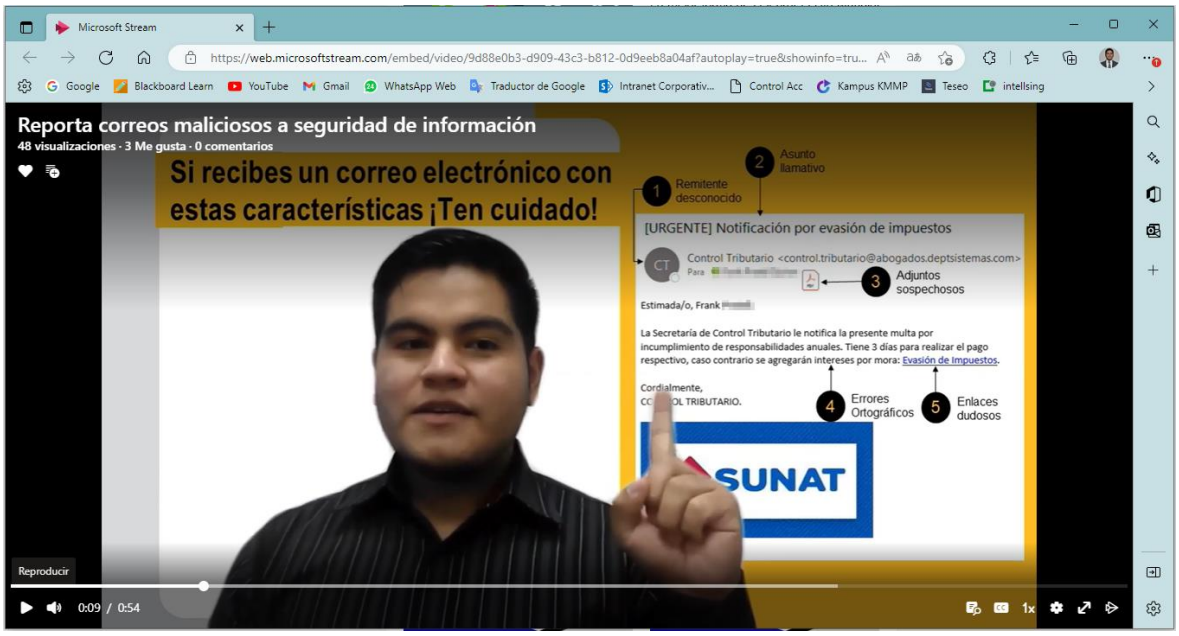
Quedo atenta a las indicaciones para la publicación el día de mañana.
Saludos,

Dayana [redacted]
Analista de Comunicaciones y Redes
Komatsu Mitsui Maquinarias Perú S.A.
[redacted]
www.kmmp.com.pe

KOMATSU MITSUI
Construimos confianza creciendo juntos

Actividad: Difundir los contenidos mediante los medios de comunicación corporativa.

Con el contenido listo para su difusión se solicitó el visto bueno de las áreas correspondientes.



Posted in All Company

Marcos [redacted]
Jun 13

Seen by 306 ···

Somos Ciberseguridad
Tema: Aprende a verificar y actualizar tu antivirus.

Desde el Team de Tecnología de la Información te compartimos un vídeo tutorial importantísimo donde podrás **aprender a verificar el estado y como actualizar el antivirus ESET** en tu equipo 💻 Corporativo 🔐

Si tienes alguna duda comunícate con **Mesa de Servicios TI** al portal [redacted] o vía Teams 🎧 indicando el número de ticket creado a los correos electrónicos [redacted] 👍

#SomosCiberseguridad
#SomosTI

Estrategia 4: Inducciones Corporativas

Actividad: Diseñar y redactar una presentación que esté alineada a los lineamientos de la Normativa interna de Seguridad de la Información.

Se procedió a redactar y diseñar una presentación para el proceso de inducción para los nuevos colaboradores de la compañía.

Actividad: Coordinar con el área Recursos Humanos las sesiones de inducción cuando se integren más miembros a la compañía.

Cada vez que hay nuevos ingresos, el área de Recursos Humanos nos envían la programación para la inducción de Tecnologías de la Información.

Inducción 18.07

AH

Alanis [redacted]

Para [redacted]

CC [redacted]

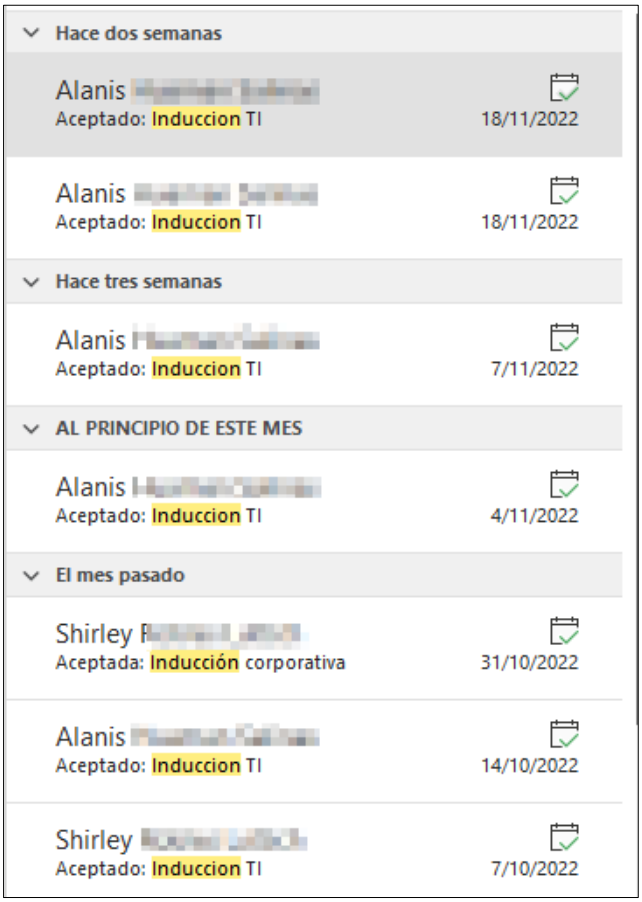
Responder | Responder a todos | Reenviar | ...

viernes 15/07/2022 14:10

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

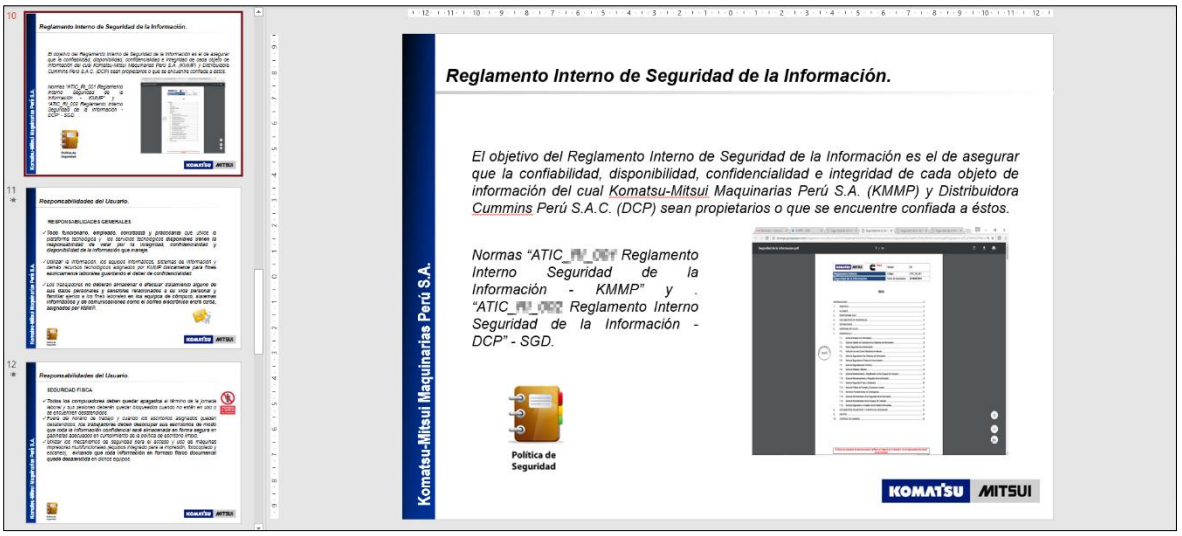
Hola a todos y todas,

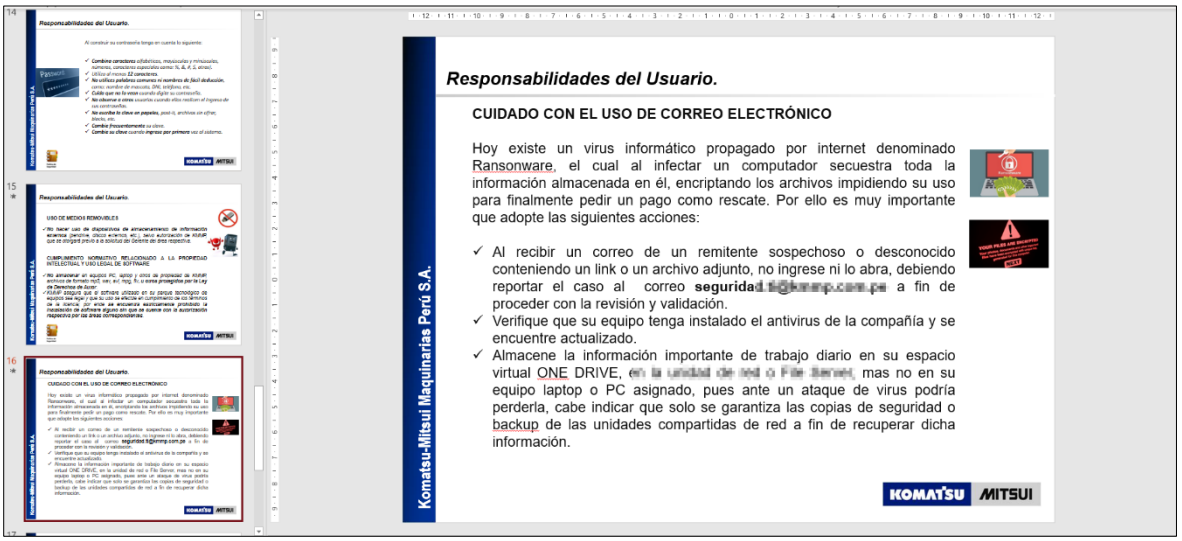
Como parte de la bienvenida a KMMP, el día **18.07** los/as invitamos a participar de nuestra **Inducción Corporativa**, la cual tiene como objetivo sumergirlos/as en la cultura de la empresa, por lo tanto, su participación es indispensable. **La reunión será vía Microsoft Teams (virtual) y ya fue agendada.**



Actividad: Evaluar dentro del tiempo de la sesión el entendimiento de los nuevos colaboradores sobre la capacitación realizada.

Dentro de la inducción se tratan temas cómo los puntos más importantes de la Normativa interna de Seguridad de la Información y recomendaciones de ciberseguridad, por lo que dentro de la sesión evaluamos la atención de los nuevos colaboradores realizando preguntas.





Estrategia 5: Monitoreo de efectividad de controles de SI.

Actividad: En coordinación con el área de Control Interno, diseñar las evidencias y criterios de evaluación con los que se evaluará la efectividad de controles, según la matriz de riesgos - compañía.

Primero se coordinará con el área de Control Interno para que se comparta la información de la matriz de riegos compañía vigente, y se puede diseñar los criterios de evaluación específicos para los controles que tratan riegos cibernéticos.

ESTOR DEL RIESGO	CÓDIGO DE CONTROL	TÍTULO DEL CONTROL	DESCRIPCIÓN DEL CONTROL	PERIODICIDAD DEL CONTROL	EVIDENCIA DEL CONTROL	TIPO DE CONTROL (preventivo, detectivo o
Tecnología de la Información	C99	Detección de malware	Herramienta antimalware avanzada implementada para proteger equipos críticos de usuarios (Alta dirección, proceso de pagos y TI) y servidores(outsourcing data center - Canvia).	Cada vez que ocurra	Informe de evaluación y monitoreo de efectividad de controles.	Detectivo
Tecnología de la Información	C237	Firewall de servicios TI en internet	-Firewall CANVIA, para el control de publicaciones de servicios TI en internet	Mensual	Informe de evaluación y monitoreo de efectividad de controles.	Preventivo
Tecnología de la Información	C242	Proceso de actualización de software y gestión de vulnerabilidades	El área de Tecnologías de la Información cuenta con un proceso de gestión de parches y vulnerabilidades para garantizar la disponibilidad e integridad de los sistemas informáticos, ejecutando: 1. Listado de sistemas a parchar 2. Programación y despliegue de ejecución de parches 3. Uso de sistemas para la gestión de vulnerabilidades	Semestral	Informe de evaluación y monitoreo de efectividad de controles.	Preventivo y Correctivo
Tecnología de la Información	C236	Zona desmitalirizada de TI	- Zona desmilitarizada DMZ está configurada solo en CANVIA para la publicación de sistemas de la Compañía hacia Internet, esta infraestructura de red diferente a nuestra LAN contiene los servidores donde se publican recursos TI (IP's, puertos y protocolos de servicios) hacia internet, evitando el acceso a nuestra red.	Mensual	Informe de evaluación y monitoreo de efectividad de controles.	Preventivo

- Diseñar las evidencias y criterios de evaluación con los que se evaluará la efectividad de controles.
- Solicitar visto bueno de la Gerencia de TI.

Realizar la evaluación de los controles y subsanar las brechas o vulnerabilidades encontradas.

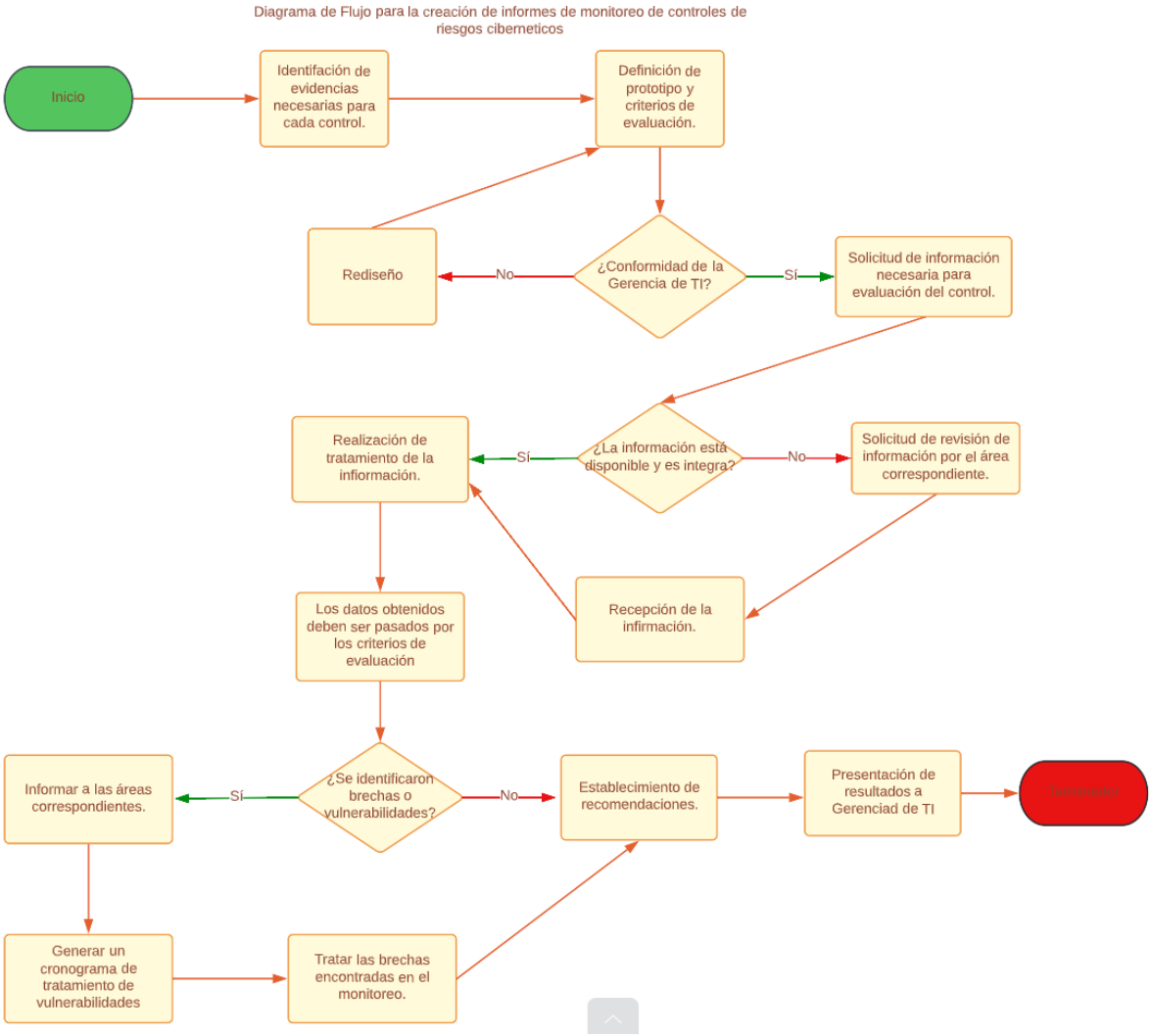
Actividad: Crear un cronograma y solicitar visto bueno de la Gerencia TI.

Crear un cronograma de ejecución de los monitoreos y asignarles una periodicidad, una vez realizado se solicita el visto bueno de la Gerencia de TI para proceder con la ejecución.

N°	Monitoreo	Control Relacionado	Descripción	Periodicidad	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC	Reporte resultados a
1	Detección de Malware	C99	Monitoreo de software AntiMalware para los equipos de la compañía	Trimestral									Gerencia TI y Gerencia Control Interno.
2	Proceso de actualización de software y gestión de vulnerabilidades de servidores	C242	Monitoreo de actialización de software base para los equipos de la compañía.	Semestral									Gerencia TI y Gerencia Control Interno.
3	Red Perimetral	C237 C236	Monitoreo de navegación y las políticas de Firrewal y DMZ de la compañía y del proveedor del servicio de hosting.	Mensual									Gerencia TI y Gerencia Control Interno.

Actividad: Realizar la evaluación de los controles y subsanar las brechas o vulnerabilidades encontradas.

Realizar el monitoreo de los controles de seguridad y remediar las brechas o vulnerabilidades encontradas con las áreas correspondientes. Con el siguiente flujo:



Una vez terminado el flujo se presenta el resultado a la Gerencia de TI para el informe al área de Control Interno y a la directiva de la compañía.

REVISIÓN DE SOFTWARE ANTIMALWARE EN EQUIPOS DE USUARIOS Y SERVIDORES KMMP Y DCP JUNIO, JULIO Y AGOSTO 2022

1.- Objetivo

Corroborar que la efectividad de los controles antimalware para equipos del tipo:

- Servidores KMMP, DCP, Canvia y Nube Azure.
- Equipos microinformáticos KMMP y DCP

2.- Alcance

a) Infraestructura de TI.

- ✓ Todos los equipos de usuarios finales.
- ✓ Todos los servidores.

b) Normativa relacionada.

N°	Nombre	Código Norma KMMP	Código Norma DCP
01	Seguridad de la Información KMMP.	ATIC_RI_01	ATIC_RI_02
02	Gestión de Incidentes y Vulnerabilidades de Seguridad de la Información	ATIC_PR_021	ATIC_RP_032
03	Copias de seguridad, protección contra software malicioso y derechos de propiedad	ATIC_PR_028	ATIC_PR_029

3.- Riesgos relacionados

N°	Fuente	Área	Proceso	Tipo Riesgo	Descripción Riesgo	Nivel Riesgo Inherente
R91	Riesgo compañía	TI	Seguridad de Información	Operacional	Medidas contra amenazas externas cibernéticas implementadas de manera inadecuada.	ALTO

3.- Controles de seguridad de información

N°	Controles	Tipo	Madurez de control	Desempeño	Riesgo tratado
1	Objetivo: Controles de seguridad antimalware. Se cuenta con herramientas antimalware implementadas para proteger equipos de usuarios y servidores. 1.- Equipos usuarios: Reportes desempeño y monitoreo Eset y Cylance. 2.- Servidores: Reportes desempeño y monitoreo Trend Micro y McAffe.	Detectivo	Control monitoreado y medido.	100% equipos y servidores	R91

4.- Conclusión:

a) Como resultado de la presente revisión se determinó que hasta el 31.AGO, los controles antimalware vienen operando en los equipos microinformáticos y servidores de la Compañía aun nivel aceptable, pero con brechas.

b) Debido al nivel obtenido y considerando las pre - condiciones presentadas en la evaluación, esperamos en el siguiente informe de monitoreo las brechas sean subsanadas.

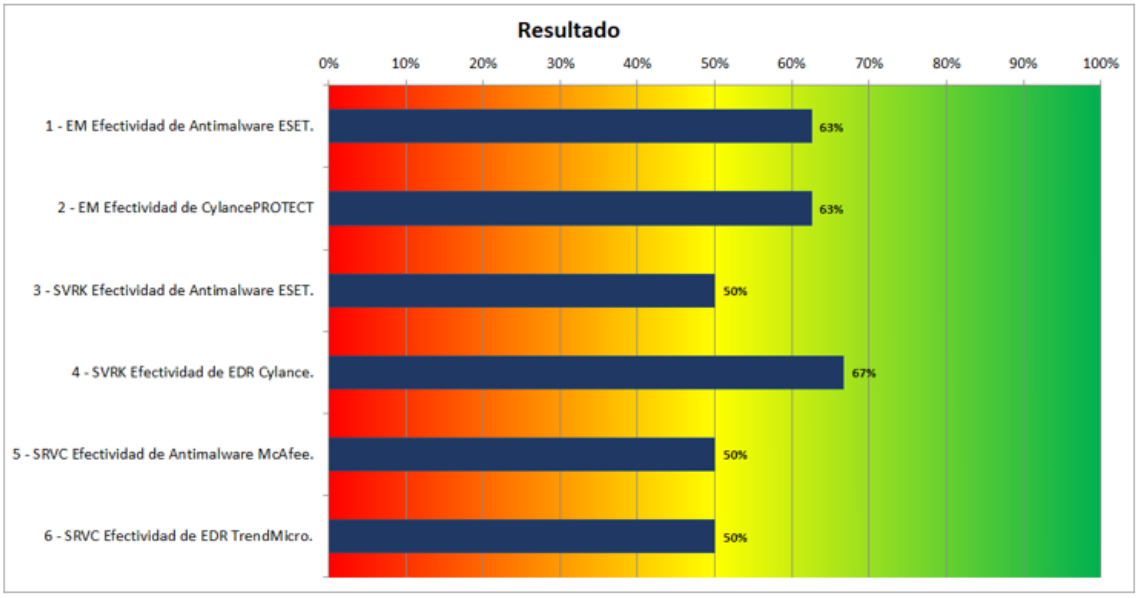
5.- Resultado

Aceptable, pero existen brechas relevantes.

Los riesgos indicados en la sección "3.- Riesgos relacionados", se vienen mitigando moderadamente. Siendo el nivel de riesgo residual a la fecha: "Medio".

Los indicadores de desempeño obtenido de los controles actualmente establecidos son:

Criterios Evaluación	Resultado
1 - EM Efectividad de Antimalware ESET.	63%
2 - EM Efectividad de CylancePROTECT	63%
3 - SVRK Efectividad de Antimalware ESET.	50%
4 - SVRK Efectividad de EDR Cylance.	67%
5 - SRVC Efectividad de Antimalware McAfee.	50%
6 - SRVC Efectividad de EDR TrendMicro.	50%



Obteniéndose un resultado general de:

RESULTADO PROMEDIO GENERAL		
TOTAL	58%	ACEPTABLE, PERO EXISTEN BRECHAS RELEVANTES.

Resultado del Monitoreo de Efectividad del Control C242 "Proceso de actualización de software y gestión de vulnerabilidades de servidores" - INF-SI-2022-018_Monitoreo_ParchesVulnerabilidades

David Carrasco Ramirez
Para: Marcos Pinto Mamani
CC: **seguridad.ti**

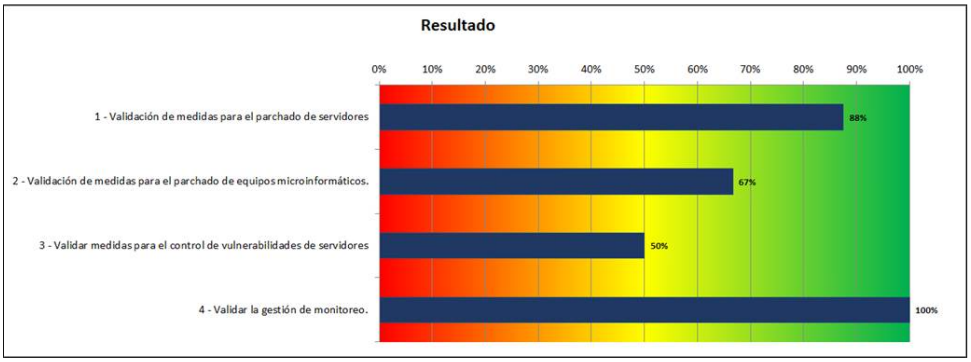
Jue 29/09/2022 13:26

INF-SI-2022-018_Monitoreo_...
2 MB

Estimado Marcos,
Saludos.

Con el fin de corroborar la correcta operación y efectividad de los controles destinados al proceso de actualización de software y gestión de vulnerabilidades para mitigar los riesgos cibernéticos conforme a la Matriz de Riesgos Compañía, le presento los resultados de la evaluación del control C242 "Proceso de actualización de software y gestión de vulnerabilidades de servidores" cuyo alcance cubre todos los equipos microinformáticos y servidores de la Compañía, el informe cubre desde mes de abril hasta agosto a la fecha de corte 31.AGO.2022, siendo el resultado:

RESULTADO PROMEDIO GENERAL		
TOTAL	75%	ACEPTABLE CON BRECHAS



Como se puede apreciar, se obtuvo un nivel **aceptable, con brechas (75%)**, situación que evidencia la operación con la necesidad de subsanar debilidades, por ello el equipo de Seguridad de la Información efectuara el proceso de seguimiento de gestión de vulnerabilidades con las respectivas Jefaturas y proveedores esperando en el próximo informe de monitoreo obtener un mejor resultado.

RE: Evidencias de monitoreo de controles y vulnerabilidades encontradas

David Carrasco Ramirez
Para: Denisse ; Angel ; **seguridad.ti**; Frank
CC: Paul Juan Berrocal Cancino

Lun 21/11/2022 17:11

Comparativo - ControlAntiM...
10 MB

KOMATSU - Informe de Vuln...
1 MB

KOMATSU - Formato Registr...
86 KB

3 archivos adjuntos (12 MB) Guardar todo en OneDrive - Komatsu Mitsui Maquinarias S.A.A Descargar todo

Estimada Denisse, buenas tardes.

Con respecto a las vulnerabilidades encontradas en el informe de monitoreo de control Antimalware INF_SI_016, comparto el excel donde se detalla cada criterio de evaluación encontrado en el informe, cada hoja tiene como nombre el criterio al cuál se refiere.

Con respecto a las vulnerabilidades N°156 y N°160 con necesidad de detalle encontradas en el informe de monitoreo de parches y vulnerabilidades INF_SI_018 aquí el detalle:

N°156 Once servidores Windows no cuentan con system center.

N°	HOST	IP	Control SystemCenter	Comentario
17			#N/D	Observado: Servidor Windows
21			#N/D	Observado: Servidor Windows
22			#N/D	Observado: Servidor Windows
29			#N/D	Observado: Servidor Windows
32			#N/D	Observado: Servidor Windows
34			#N/D	Observado: Servidor Windows
36			#N/D	Observado: Servidor Windows
43			#N/D	Observado: Servidor Windows 2008
49			#N/D	Observado: Servidor Windows
60			#N/D	Observado: Servidor Windows
66			#N/D	Observado: Servidor Windows

N°157 Brechas de seguridad identificadas en el reporte de Rapid7.
Comparto el informe emitido por el proveedor Canvia y el excel de detalle de vulnerabilidades identificadas por Rapid7.

Quedo atento ante cualquier consulta, duda o necesidad.

Gracias.

Atte.

VII. Cronograma

Cronograma de la estrategia, "Plan de difusión comunicados de Seguridad de la Información".

Mes	N°	Titulo	Fecha	Estado
Abril	1	Cuidado con el ransomware	1.04	Enviado
	2	Infección de virus informático	07.04 y 11.04	Enviado
	3	CUIDADO EN LA MANIPULACIÓN DE EQUIPOS DE COMPUTO - SIG	13.04	Enviado
	4	Aprende a liberar la sobrecarga de tu equipo de cómputo.	19.04	Enviado
	5	USO CORRECTO DE USUARIOS Y CONTRASEÑAS	22.04	Enviado
	6	DEBER DE CONFIDENCIALIDAD Y CUIDADO DE LA INFORMACIÓN	26.04	Enviado
	7	Recomendaciones de ciberseguridad para el trabajo remoto	29.04	Enviado
Mayo	8	Seguridad de equipos laptop	4.05	Enviado
	9	PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y CONFORMIDAD DE LOS DERECHOS DE PROPIEDAD INTELECTUAL	9.05	Enviado
	10	CUIDADO DE INFORMACIÓN IMPORTANTE PARA LA OPERATIVA	11.05	Enviado
	11	COMUNICADO EXPOSICIÓN DE DATOS PERSONAL	13.05	Enviado
	12	GESTIÓN Y USO CORRECTO DE EQUIPOS DE COMPUTO	16.05	Enviado
	13	CREACIÓN, MODIFICACIÓN, ELIMINACIÓN Y MONITOREO DE CUENTAS DE USUARIOS SAP	19.05	Enviado
	14	CUIDADO EN LA MANIPULACIÓN DE EQUIPOS DE COMPUTO - SIG	25.05	Enviado
Junio	15	Aprende a liberar la sobrecarga de tu equipo de cómputo.	2.06	Enviado
	16	Correos electrónicos de estafadores	9.06	Enviado
	17	COMUNICADO ALERTA: MENSAJES DE ENGAÑO POR REDES SOCIALES	9.06	Enviado
	18	Recomendaciones de ciberseguridad para el trabajo remoto	17.06	Enviado

	19	Responsabilidad Privacidad de Información.	28.06	Enviado
	20	LDPD: Recopilación de la información	30.06	Enviado
Julio	21	Infección de virus informático	5/07/2022	Enviado
	22	USO CORRECTO DE USUARIOS Y CONTRASEÑAS	7/07/2022	Enviado
	23	DEBER DE CONFIDENCIALIDAD Y CUIDADO DE LA INFORMACIÓN	12/07/2022	Enviado
	24	Seguridad de equipos laptop	14/07/2022	Enviado
	25	PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y CONFORMIDAD DE LOS DERECHOS DE PROPIEDAD INTELECTUAL	21/07/2022	Enviado
	26	CUIDADO DE INFORMACIÓN IMPORTANTE PARA LA OPERATIVA	25/07/2022	Enviado
	27	GESTIÓN Y USO CORRECTO DE EQUIPOS DE COMPUTO	27/07/2022	Enviado
Agosto	28	CUIDADO EN LA MANIPULACIÓN DE EQUIPOS DE COMPUTO - SIG	2/08/2022	Enviado
	29	Aprende a liberar la sobrecarga de tu equipo de cómputo.	9/07/2022	Enviado
	30	Recomendaciones de ciberseguridad para el trabajo remoto	11/08/2022	Enviado
	31	CREACIÓN, MODIFICACIÓN, ELIMINACIÓN Y MONITOREO DE CUENTAS DE USUARIOS SAP	18/08/2022	Enviado
	32	Correos electrónicos de estafadores	22/08/2022	Enviado
	33	Responsabilidad Privacidad de Información.	25/08/2022	Enviado
	34	LDPD: Recopilación de la información	29/08/2022	Enviado
Septiembre	35	Infección de virus informático	8/09/2022	Enviado
	36	USO CORRECTO DE USUARIOS Y CONTRASEÑAS	12/09/2022	Enviado
	37	DEBER DE CONFIDENCIALIDAD Y CUIDADO DE LA INFORMACIÓN	14/09/2022	Enviado
	38	Seguridad de equipos laptop	20/09/2022	Enviado
	39	Correos electrónicos de estafadores	22/09/2022	Enviado
	40	PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y CONFORMIDAD DE LOS DERECHOS DE PROPIEDAD INTELECTUAL	28/09/2022	Enviado
	41	ALERTA MENSAJES DE TEXTO DE ENGAÑO	30/09/2022	Enviado
Octubre	42	CUIDADO DE INFORMACIÓN IMPORTANTE PARA LA OPERATIVA	7/10/2022	Enviado

	43	GESTIÓN Y USO CORRECTO DE EQUIPOS DE COMPUTO	19/10/2022	Enviado
	44	CREACIÓN, MODIFICACIÓN, ELIMINACIÓN Y MONITOREO DE CUENTAS DE USUARIOS SAP	20/10/2022	Enviado
	45	Aprende a liberar la sobrecarga de tu equipo de cómputo.	25/10/2022	Enviado
	46	Correos electrónicos de estafadores	26/10/2022	Enviado
	47	Responsabilidad Privacidad de Información.	28/10/2022	Enviado
	48	LDPD: Recopilación de la información	31/10/2022	Enviado
Noviembre	49	Infección de virus informático	7/11/2022	Enviado
	50	CUIDADO EN LA MANIPULACIÓN DE EQUIPOS DE COMPUTO - SIG	10/11/2022	Enviado
	51	Aprende a liberar la sobrecarga de tu equipo de cómputo.	18/11/2022	Enviado
	52	USO CORRECTO DE USUARIOS Y CONTRASEÑAS	25/11/2022	Enviado
	53	Recomendaciones de ciberseguridad para el trabajo remoto	28/11/2022	Enviado
	54	DEBER DE CONFIDENCIALIDAD Y CUIDADO DE LA INFORMACIÓN	29/11/2022	Enviado
	55	Seguridad de equipos laptop	30/11/2022	Enviado

Cronograma de la estrategia, “Campañas de simulación de ataques de ingeniería social con concientización instantánea”.

N - 0	N - 1	Actividad	Duración	Inicio	Fin	Avance	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	**NOV**
1	1	CAMPAÑAS DE SIMULACIÓN DE CIBERATAQUES - 2022 (Concientización)	281 días	10/02/2022	18/11/2022	100%										
1	1.1	PRIMERA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - FEB 2022	22 días	10/02/2022	4/03/2022	100%										
1	1.2	SEGUNDA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - MAR 2022	27 días	8/03/2022	4/04/2022	100%										
1	1.3	TERCERA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - ABR 2022	30 días	4/04/2022	4/05/2022	100%										
1	1.4	CUARTA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - MAY 2022	24 días	9/05/2022	2/06/2022	100%										
1	1.5	QUINTA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - JUN 2022	27 días	11/06/2022	8/07/2022	100%										
1	1.6	SEXTA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - JUL 2022	25 días	18/07/2022	12/08/2022	100%										
1	1.7	SÉPTIMA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - AGO 2022	28 días	8/08/2022	5/09/2022	100%										
1	1.8	OCTAVA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - SEP 2022	25 días	12/09/2022	7/10/2022	100%										
1	1.9	NOVENA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - OCT 2022	28 días	14/10/2022	11/11/2022	100%										
1	1.9	DÉCIMA CAMPAÑA DE SIMULACIÓN DE CIBERATAQUES - NOV 2022	16 días	2/11/2022	18/11/2022	100%										
2	2	Proceso disciplinario de colaboradores según resultados de campañas de simulación (Concientización - Educación)	276 días	4/03/2022	5/12/2022	100%										
2	2.1	Correos de cumplimiento a colaboradores víctimas de cada campaña	217 días	2/05/2022	5/12/2022	100%										
2	2.2	Correos de amonestación a colaboradores reincidentes en 3 o más campañas de simulación de manera consecutiva	276 días	4/03/2022	5/12/2022	100%										

Cronograma de la estrategia "Producción y publicación de contenido audiovisual de Seguridad de la Información".

TIPO	N°	Titulo	Fecha	Estado	Avance
Vídeo tutorial	1	Reconoce correos maliciosos.	30/04/2022	Enviado	100%
Vídeo tutorial	2	Actualiza tu AV.	17/06/2022	Enviado	100%
Vídeo informativo	3	Reinicia tu equipo.	30/06/2022	Enviado	100%
Vídeo informativo	4	Reporta Correos Maliciosos	29/07/2022	Enviado	100%

Cronograma de la estrategia "Monitoreo de efectividad de controles de SI ligados a los recursos humanos".

N°	Monitoreo	Control Relacionado	Descripción	Periodicidad	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC	Reporte resultados a
1	Detección de Malware	C99	Monitoreo de software AntiMalware para los equipos de la compañía	Trimestral									Gerencia TI y Gerencia Control Interno.
2	Proceso de actualización de software y gestión de vulnerabilidades de servidores	C242	Monitoreo de actialización de software base para los equipos de la compañía.	Semestral									Gerencia TI y Gerencia Control Interno.
3	Red Perimetral	C237 C236	Monitoreo de navegación y las politicas de Firrewal y DMZ de la compañía y del proveedor del servicio de hosting.	Mensual									Gerencia TI y Gerencia Control Interno.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, NECOCHEA CHAMORRO JORGE ISAAC, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Implementación del dominio "Seguridad de la Información Ligada a los Recursos Humanos" según la ISO 27001:2013 en la empresa Komatsu – Mitsui Maquinarias Perú S.A.", cuyo autor es CARRASCO RAMIREZ DAVID AGUSTO, constato que la investigación tiene un índice de similitud de 24.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 29 de Noviembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
NECOCHEA CHAMORRO JORGE ISAAC **DNI:** 18167347 **ORCID:** 0000-0002-3290-8975	Firmado electrónicamente por: JNECOCHEA el 29-11-2022 16:58:28

Código documento Trilce: TRI - 0461428

INVESTIGA UCV