**Decanato de Ciencias Económicas y Empresariales**
**Escuela de Administración**

# *Estudio Sobre Peligros Digitales y Su Impacto en el Ámbito de Gestión Humana en una Organización*

***Sustentantes***:

Raquel Patricia Rosario Pérez 2013-2969

Lisbeth Jazmín Suero 2014-0349

Yafrell David Méndez Cabral 2015-0442

***Asesores***:

Sr. Víctor Herrera

Sra. Laura Sánchez

Monografía para optar por el título de Licenciado(a) en Administración de Empresas

*Distrito Nacional, República Dominicana*
*2020*

# Tabla de Contenido

# Dedicatorias

Este trabajo final de monográfico, se lo dedico de manera especial a mis padres, Galo M. Rosario y Miguelina Pérez, a mis hermanos, Susana, Rocio, Galo, Sarah y Lisbeth, por brindarme el apoyo necesario para no abandonar mis estudios, por ser mis consejeros y darme los valores, para convertirme en la profesional que soy hoy.

Papi, te dedico este trabajo final de grado, porque si no hubiera sido porque me agarraste, literalmente de la mano para que entrara a la universidad, desde que Salí del colegio, hoy en día lo más seguro es que no hubiese alcanzado esta meta que un día me propuse, esta es solo la razón principal por la cual te hago esta dedicatoria, siempre has sido un padre muy preocupado por los estudios de tus hijos, dispuesto a explicar y aportar tus conocimientos , con el fin de que nos vaya bien en nuestra labor, siempre recordare lo que me decías al inicio de esta etapa universitaria “tu principal deber es estudiar, enfócate en eso, que lo demás viene por añadidura” un consejo que puede parecer sencillo, pero dado en el momento correcto es un consejo maravilloso.

A mi mami, por siempre ser mi apoyo incondicional, le dedico este trabajo final de grado, porque siempre has estado presente en las decisiones que he tomado en lo largo de mi carrera, si no hubiese tenido tu apoyo y la motivación que me has dado, cuando quería rendirme, no hubiese logrado terminar mi carrera, siempre me has inculcado que debo hacer y dedicarme a lo que realmente

quiero y nunca olvidare que en cada decisión difícil que tuve que tomar, siempre me preguntabas que es lo que realmente yo quiero y me alentabas a seguir eso, para mi es la mayor enseñanza ya que somos buenos en las cosas que nos gustan, esto lo he aprendido gracias a ti. También te hago esta dedicatoria porque siempre creíste en mí y en que puedo lograr todo lo que me proponga

A mis hermanos, que siempre me han demostrado su apoyo, en diferentes aspectos de la vida, le dedico este trabajo como ejemplo de constancia, que no importa que tiempo pase, lo importante es mantenerse enfocado en la meta, les hago esta dedicatoria para que les sirva de motivación cuando se quieran rendir o abandonar un sueño o proyecto, nunca será fácil, pero les garantizo que vale la pena.

Para finalizar gracias a ustedes, mi familia, por siempre creer en mí y darme el aliento que he necesitado en cada momento de mi vida, les dedico mi trabajo de monográfico con mucho amor y deseándoles lo mejor para ustedes. Muchas bendiciones y que todo lo que se propongan a lo largo de la vida, lo puedan alcanzar.

*Raquel Rosario*

Para mi madre y hermano: Si alguien sabe el camino que me tocó recorrer para lograr este título eres tú mami y por eso te dedico hoy mi monografía. Gracias por siempre estar ahí para mí, por tus buenos consejos y por ser ese motor que me impulsa a luchar por mis sueños. Me enseñaste que la vida no es fácil, pero con esfuerzo toda meta que me proponga puede ser alcanzada. Este logro es de las dos, porque tú también luchaste y trabajaste arduamente para que hoy tu hija pueda decir con orgullo que es Licenciada en Administración de Empresas. No me alcanza la vida para agradecerte tus palabras sabias cuando me sentía turbada, el que siempre me motivaras a seguir adelante sin importar el tiempo que pasara, tus ocurrencias para hacerme reír cuando me veías decaída y tus cuidados cuando me sentía agotada.

Gracias a ti manito por adoptarme como tu hija desde el primer día, por preocuparte siempre por mis estudios, salud y bienestar. Eres un pilar importante en mi vida, por lo que sin ti colapsaría; hoy te agradezco el que hayas trabajado para aportar en mis estudios, por poner mi progreso como prioridad en tu día a día y, sobre todo, por demostrarme que puedo contar contigo, sin importar las adversidades que enfrentaría.

*Lisbeth Suero*

Quiero dedicarle este trabajo, primero que todo, a mis padres Zayda Cabral y Ángel Méndez, que me permitieron tomar cada decisión de acuerdo a los criterios que ellos me han enseñado, guiado, y como me han criado. Por ser la persona que soy en la actualidad y por velar cada paso que he dado en mi vida incluyendo este, mi meta final.

A mis hermanas, Pieri y Sabrina Méndez, por ser los pinceles de cada cuadro pintado que, durante esta trayectoria, sin ellas no hubiese logrado pintar y hacer que cada paisaje sean mejores cada día más mientras estuve creciendo y formándome como profesional.

A mi abuela, Mireya Rodríguez, quien antes de fallecer me motivó a convertirme en un profesional excelente y de bien, realizar las ocupaciones con ganas y enseñarme a mantener una sonrisa ante cualquier adversidad.

A mi novia, Aida Guzmán, quien ha servido como lienzo pintoresco desde mediados de mis estudios y formación técnica de mi carrera. Por estimularme, sostenerme y empujarme a obtener mayores logros que hoy en día no hubieran sido posible sin las palabras de motivación dedicadas.

*Yafrell Méndez*

# Agradecimientos

Gracias a mi familia, Mami, papi, mis hermanos, gracias a mis tíos, en especial Frank y Henry, por los consejos y el apoyo recibido en esta etapa de mi vida.

Gracias a mi amiga Alexa Núñez (Ray), por el apoyo emocional desde el comienzo de esta gran vivencia.

Agradezco de manera especial al Sr. Cesar caracas, quien ha sido mi consejero y asesor en esta larga carrera universitaria.

Gracias a todos mis maestros, por aportar a los conocimientos que hoy en día forman parte de mi preparación profesional.

A mis compañeros universitarios que estuvieron conmigo, día tras día, superando juntos todos los desafíos.

Agradezco de manera especial a mis asesores de monográfico (profesora Laura y profesor Víctor) por la dedicación y entrega.

Gracias a mis compañeros de monográfico Lisbeth Suero y Yafrell Méndez, por su compañerismo y trabajo en equipo.

Para finalizar gracias a todos los que apostaron a que lo lograría, gracias por sus buenos deseos y gracias a todos aquellos que en algún momento de mi carrera me sirvieron de apoyo y bastón.

*Raquel Rosario*

Ante todo, agradezco a Dios porque en Su nombre todo propósito puede ser logrado, sin importar lo imposible que nosotros como seres humanos lo consideremos. Siempre me he sentido agradecida por el apoyo por parte de mi familia, desde el día en que nací se han preocupado por mí, me han enseñado a luchar y salir victoriosa ante los retos de la vida. Veinticuatro años después sus enseñanzas no cesan y gracias a todo el apoyo moral y financiero que he recibido por su parte, hoy estoy aquí con un nuevo logro alcanzado. Gracias por sus consejos y por poner toda su fe en que sí lo lograría.

De igual forma reconozco y agradezco el apoyo brindado por mis amigos, en especial por parte de Katherine, Kimberly y Rhabeli quienes fueron un soporte fundamental en esta etapa que hoy culmino.

Me siento agradecida de mis asesores el Sr. Víctor Herrera y la Sra. Laura Sanchez por iluminarnos y guiarnos con sus conocimientos en esta carrera final hacia la meta.

Asimismo, agradezco a mis compañeros de monográfico, Yafrell Méndez y Raquel Rosario por acompañarme y ser parte de esta experiencia de trabajo en equipo.

*Lisbeth Suero*

En primer lugar, quiero agradecerle a Dios por derramar bendiciones sobre cada objetivo y dificultad superada.

Al profesor Víctor J. Herrera García y la profesora Laura Sánchez por guiarme en el desarrollo de este trabajo de investigación para obtener mi título de Lic. En Administración de Empresas.

A todos los docentes de la familia de UNAPEC, quienes ayudaron en mi formación como profesional durante la trayectoria de mi carrera.

A toda mi familia por estar siempre presente cuando necesite de ellos, y servir como como medio para alcanzar las metas establecidas.

A todos los compañeros de clase por haberse convertido en mis amigos y colegas de profesión, quienes compartieron alegrías, momentos brillantes y penas en esta experiencia de nuestras vidas.

A mis compañeras, Lisbeth Suero y Raquel Rosario, por haber compartido este camino conmigo y superar cada obstáculo para lograr nuestros objetivos de manera en común.

A todos ellos quiero agradecerles, y a todas las demás personas que de alguna manera u otra, me ayudaron a alcanzar este logro en mi carrera profesional y en mi vida personal.

*Yafrell Méndez*

# Resumen Ejecutivo

Los peligros digitales son delitos que una serie de individuos u organizaciones se encargan de realizar a un ente predeterminado, provocando daños digitales y extraen información de las entidades acertadas. En tal sentido, el propósito de esta investigación fue analizar el desarrollo de ocurrencia de los delitos o ciberataques que las organizaciones de la República Dominicana enfrentan mediante la era digital, con el fin de determinar cuál es el nivel o grado de consecuencias que estos han causado al área de Gestión Humana, así como, cuáles han sido las medidas o posibles soluciones ofrecidas por los entes especializados en el área.

La metodología empleada en el desarrollo de esta investigación fue el método deductivo y se utilizaron las técnicas descriptivas y documentales.

La aplicación de dicha metodología permitió a los implicados obtener una visión amplia de cómo ha sido la evolución y desarrollo de los distintos ciberataques en la organización utilizada como foco de investigación y las posibles soluciones que deberían ser implementadas.

# Introducción

Hoy en día en la República Dominicana las organizaciones no cuentan con la defensa requerida en cuanto a ciberseguridad se refiere y se ven regularmente expuestas a peligros digitales. En atención a lo cual las empresas u organizaciones buscan poder detener estos tipos de peligros o ciberataques, a consecuencia de que un solo acto delictivo puede causar en cualquier intento circunstancias desfavorables trayendo consecuencias negativas en cuanto al funcionamiento de la institución, provocando indisponibilidad.

Una de las áreas fundamentales dentro de la compañía es la de Gestión Humana, debido a que posee información confidencial y de suma importancia sobre el personal de la empresa; por lo cual es una de las áreas más propensas a ser afectadas por este tipo de peligros. Por tal razón, el objetivo principal de esta investigación es identificar los peligros digitales y su impacto en el ámbito de gestión humana en una organización de la República Dominicana y generar recomendaciones para mitigar los riesgos junto al área especializada de tecnología con los parámetros requeridos ante las situaciones de peligros digitales que se presenten al año 2020.

En la monografía presentada a continuación podrá visualizar la siguiente estructura; En el capítulo No.1 se presenta una explicación sobre el tema de los ataques cibernéticos en general y su repercusión en la República Dominicana. De

igual forma se hace mención del DICAT, laboratorio nacional que se encarga de dar el seguimiento oportuno a estas infracciones y la forma en la que el delito más mínimo puede asociarse a un ciberataque. En cambio, el capítulo No.2 refleja una reseña sobre la empresa en la que nos hemos enfocado para la investigación pertinente y reflejar los resultados obtenidos en el capítulo No.3.

Finalizando detallando las recomendaciones y conclusiones oportunas.

# Capítulo 1: Peligros digitales en las empresas de la República Dominicana

Las organizaciones de República Dominicana hoy en día no cuentan con la defensa requerida en cuanto a ciberseguridad se refiere y se ven regularmente expuestas a peligros digitales. Según el glosario de términos del Ciber-Observatorio del Centro Nacional de Seguridad de Ciberseguridad de la Rep. Dom. define como Ciberataques o Cibercrimen “Los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos”. Sin embargo, muchos de estos peligros digitales están dirigidos hacia el robo de informaciones sensibles de las organizaciones más que el daño de estas.

Cada día es mayor la cantidad de instituciones e individuos que se ven afectados ante un ataque cibernético debido al incremento del uso de redes digitales en los últimos tiempos. Según un estudio realizado por Bromium, que muestra cómo los ingresos por delitos digitales han aumentado a 1,5 billones de dólares anuales en ganancias ilícitas.

Son muchos los sitios web populares que se enfrentan a ataques de mayor envergadura y de alta tecnología todos los días, siendo víctimas de la creciente tendencia del ciberataque. Enfocándonos en el incremento de los últimos meses del teletrabajo, clases virtuales y el contacto con personas a través de dispositivos

electrónicos por motivo del estado de emergencia en el que nos encontramos, las autoridades han detectado un aumento en estafas cibernéticas.

De acuerdo con las estadísticas emitidas por el Centro Nacional de Ciberseguridad, pudieron visualizar un incremento de un 150% en dominios utilizados para generar actividades maliciosas, 140% de phishing o mejor conocido como enlaces maliciosos y un 180% en divulgación de noticias falsas, siendo una gran parte dirigidas a las organizaciones empresariales que se encuentran operando remotamente por lo que se puede especular que una muestra de esta parte fue dirigida a órganos esenciales incluyendo Recursos Humanos.

Por otra parte, según un informe presentado por la Compañía de Ciberseguridad Fortinet, en el año 2019 la Rep. Dom. sufrió más de 106 millones de ciberataques siendo las amenazas principales que fueron dirigidas a la red: descargas no deseadas, cripto hacking, explotación de vulnerabilidades, malware y troyanos; quienes se encargan de buscar información y robarlas a usuarios. No obstante, la prevalencia de estos ataques ya es conocida por los receptores y de los cuales tienen remediación, por lo que esto da a demostrar que aún es necesario el desarrollo de prevenciones ante malwares o ataques.

Tenemos como propósito de esta investigación identificar los distintos niveles de peligro que han atacado a las áreas de gestión humana en las organizaciones

empresariales de la República Dominicana a nivel digital, de igual manera, medir el impacto que causan estos riesgos al ser incorporarse a los sistemas tecnológicos de dicha área. Así también, identificar qué posibles medidas han tomado las áreas u organizaciones para combatir este ente y fomentar una mayor seguridad para las organizaciones. En la actualidad las empresas u organizaciones corren un sin números de riesgos al querer transformarse a la era tecnológica o simplemente migrar informaciones a sistemas digitales. De acuerdo con Unirse vista (2019), intentar aplicar un proceso de transformación en las empresas requiere un cambio de mentalidad antes de ir a la acción, esto exige analizar el estado del cual se parte. Ser digital en una empresa implica conocer los riesgos, amenazas y posibles sanciones que pueden ocurrir al desarrollar la actividad.

Por tal razón, nuestro objeto de estudio es poder identificar estos tipos de riesgos o peligros para poder medir la gravedad del impacto que esta causa en las áreas de Gestión Humana de una organización.

### 1.1 Laboratorios Especializados

Nuestro país cuenta con la Procuraduría Especializada en Crímenes y Delitos de Alta Tecnología (PEDATEC) desde el año 2013, la cual tiene como objetivo dar seguimiento a todos los hechos punibles donde se detectan el uso de dispositivos electrónicos y dar apoyo a las fiscalías a nivel nacional. Esta dependencia de la

Procuraduría General de la República está dirigida por el procurador de la Corte, quien afirma que todo delito normal o fuera de lo normal hoy en día, implica un dispositivo tecnológico que deja rastro.

De los más comunes se pueden mencionar:

- Crimen organizado.
- Lavado de activos.
- Corrupción.
- Secuestros y asesinatos.
- Robos y asaltos en la vía pública.

Asimismo, posee laboratorios preparados y certificados para la investigación y seguimiento de los delitos anteriormente mencionados, donde se vea involucrado el uso de dispositivos sencillos como el celular, computadora, Tablet o tan solo el internet; estos laboratorios son el Instituto Nacional de Ciencias Forenses y la Dirección de Alta Tecnología de la Policía (DICAT).

El DICAT se crea en noviembre del 2005 como consecuencia del incremento de delitos electrónicos que presentó la República Dominicana, así como el surgimiento de nuevas formas de los delitos tradicionales a través de medios informáticos; otro de sus objetivos principales fue la integración de la Policía Nacional dominicana en esquemas internacionales para combatir el ciberataque.

Está regido por el marco legal de la Ley 53-07 contra crímenes y delitos de alta tecnología y departamentos, o mejor conocidos como unidades son:

- Sección de Investigaciones.
- Sección de Inteligencia Electrónica.
- Sección de Fraude a Empresas.
- Sección de Fraudes Bancarios.
- Sección de Evidencia Electrónica.
- Sección de Análisis Forense Equipos Electrónicos.
- Sección de Análisis Forense Imágenes / Videos
- Sección de Llamadas Molestosas y/o Amenazantes.

Sobre las redes sociales y el espionaje telefónico, nos alertan de que se debe tener sumo cuidado con lo que publicamos ya que es un acercamiento que le ofrecemos a la sociedad de nuestra vida privada y que además pasa a ser propiedad del dueño de la red y el público en general. Con respecto al espionaje, la Ley 53-07 castiga la intercepción ilegal de llamadas.

### 1.2 Preguntas de la Investigación

Del propósito de estudio que justifica esta investigación se derivan las siguientes preguntas de investigación:

1. ¿A qué se debe el alto nivel de ataques que causa este peligro en las áreas de Gestión Humana?

2. ¿Cuáles medidas han adoptado las organizaciones para evitar estos tipos de riesgos?
3. ¿Cuáles son los efectos que causaría a las organizaciones el establecer parámetros para frenar este riesgo?

### 1.3 Diagnóstico

De acuerdo con datos divulgados por la firma global Ernst & Young (2018), organización que se encarga en auditar impuestos, transacciones y legal, indica que las empresas más atacadas se encuentran aquellas que cuentan con un vínculo directo con el consumidor, como, la banca, telecomunicaciones, salud, educación y de igual manera, hotelería. De acuerdo con una encuesta general dictada por la firma denominada “Encuesta Global de Seguridad de la Información”, indica que, la ciberseguridad es un tema al que se debe darle prioridad de parte de las empresas, pues 8 de cada 10 organizaciones no cuentan con los recursos suficientes para enfrentar las amenazas.

Siguiendo con Omar Quesada, Gerente Senior de Ciberseguridad de EY para Centroamérica, Panamá y República Dominicana, citó para la revista digital El Dinero (2019) “mientras más avance la era de la transformación digital, se abre un abanico de oportunidades, pero también de amenazas, donde la ciberseguridad debe hacer frente. Sin embargo, solo el 13% de las empresas encuestadas maneja un presupuesto de ciberseguridad acorde con sus

necesidades. En Latinoamérica, 29% de los encuestados dijeron tener un aumento en el presupuesto este año, mientras que un 42% prevé un aumento en su presupuesto para el año 2020”.

Por otro lado, Rafael Ovalles, director general del Instituto Nacional de Formación Técnico Profesional (INFOTEP), indica que la República Dominicana pese haber recibido más de 24 millones de ciberataques, se encuentra posicionada dentro de los 10 países que cuentan con un mecanismo de seguridad cibernética. No obstante, la utilización de dispositivos digitales por parte de los Recursos Humanos dentro de las empresas dominicanas multiplica los niveles de riesgos y captación de diversos ataques cibernéticos. Es por tal, que es de mayor importancia el concientizar la utilización de los mismo con relación al trabajo que se realiza y protección.

De acuerdo con los datos provistos previamente, es de mayor importancia para las organizaciones, en especial las Áreas de Gestión Humana, realizar con medidas buenas prácticas de ciberseguridad. Es por tal sentido que, se justificará el resultado de la investigación con distintas fuentes que den soporte a los medios e ideas que se utilizaran para la disminución de los riesgos dirigidos a esta área. La mitigación de los peligros digitales se logrará mediante las buenas prácticas de ciberseguridad, creación de estrategias y aplicación de medidas dirigidas por los recursos humanos.

## 1.3 Valoración

El problema consiste en que las organizaciones de la República Dominicana han mostrado un desperfecto en los niveles para el desarrollo de una figura de estrategias e implementación de marcos para que, en cuestión de intentos del acto delictivo digital, dígase “ciberataque”, haya un lapso de respuesta y una reacción. Por tal, para lograr la posibilidad de rastrear dichos sucesos para contrastar el hecho, las empresas dominicanas y los órganos de Gestión Humana que estas administran deben aplicar los tipos de tácticas escasas.

Por consiguiente, los datos citados anteriormente, exponen claramente que el avance de las defensas contra los peligros digitales dentro de una organización en la República Dominicana en contexto con sus pares muestra una gran deficiencia, lo que retrasa el desarrollo de un marco de protección para la disminución de intentos de ataques digitales hacia órganos de importancia como lo son los Recursos Humanos. Dicho mecanismo serviría como fuente de desarrollo de tácticas, o para ser más específicos, estrategias constantes para la Gestión Humana de una organización, obrar como alternativa de planes para el cuidado y ahorro de gastos producidos por daños, y proveer módulos de contingencias para mitigar riesgos que permitan que la protección se realicen a la brevedad posible.

De igual forma, la presencia de un marco de estrategias que proteja los recursos y datos de Gestión Humana es una de las principales manifestaciones de desarrollo de habilidades pujantes, puesto que revela la presencia de varias alternativas efectivas para la canalización de los posibles peligros y así atenuar, por otra parte, revela la garantía hacia la inversión y ayuda en áreas productivas relacionadas a dicho órgano. En Rep. Dom. Algunas entidades, incluyendo las mencionadas anteriormente, así como reguladores han mostrado gran interés en implementar las medidas de lugar que permitan el progreso de un ambiente digital protegido y organizado, encontrando dificultades, específicamente en la puesta en funcionamiento a destrezas que convaliden alcancen tales aspiraciones.

# Capítulo 2: Universidad APEC Como Foco de Estudio

Para la realización de la investigación del informe, se tomó como objeto de estudio a la Universidad Acción Pro-Educación y Cultura (UNAPEC), la cual facilitó la recolección de datos necesarios.

La Universidad APEC es la Institución primogénita de Acción Pro-Educación y Cultura (APEC), constituida en 1964 cuando empresarios, comerciantes, profesionales y hombres de iglesia, deciden crear una entidad sin fines de lucro, impulsadora de la educación superior en la República Dominicana.

Nace con el nombre de Instituto de Estudios Superiores (IES), y, en septiembre de 1965, crea su primera Facultad con las Escuelas de Administración de Empresas, Contabilidad y Secretariado Ejecutivo Español y Bilingüe.

En 1968, mediante Decreto No.2985, el Poder Ejecutivo le concede el beneficio de la personalidad jurídica para otorgar títulos académicos superiores, con lo cual la Institución alcanza categoría de Universidad.

El 11 de agosto de 1983, el Consejo Directivo de APEC, mediante la Resolución No. 3, adopta de un nuevo símbolo para la Institución y su identificación como Universidad APEC (UNAPEC). Posteriormente, el Poder Ejecutivo autorizó este cambio de nombre por medio del Decreto No. 2710, del 29 de enero de 1985.

UNAPEC, cuenta con 3 campus en el distrito nacional, el campus principal de la Av. Máximo Gómez, el campus ubicado en la Av. 27 de febrero esq. Caonabo y el campus ubicado en la Av. Bolívar. El campus principal posee cinco (5) edificios que se utilizan como aulas de clases, un edificio administrativo, una cancha de recreación, cafetería, centro de impresión, enfermería, área de admisiones, salones de eventos y el edificio que pertenece a APEC, conocido como la casona.

También el campus principal, que es en donde se realizó esta investigación, cuenta con áreas de parqueo, distribuidas dentro y fuera del campus.

Todo el campus está rodeado de mucha vegetación, apoyando la iniciativa de un lugar verde y dándole un aire de confort y comodidad a la universidad.

### 2.1 Principales Actividades que Realiza

Dentro de las actividades que se realiza en el entorno universitario, UNAPEC, realiza las siguientes:

- Imparte docencia en los niveles, de grado, postgrado, idiomas, centros asociados y educación continuada.
- Realiza conferencias, con profesionales de distintos sectores productivos.
- A través de su departamento de extensión cultural, realiza deportes, danza, bailes, teatros, entre otras actividades.

- Apoya los proyectos emprendedores a través de los diferentes decanatos y con la dependencia CEMPRENDE, que pertenece a la universidad.
- Participa en programas de intercambio estudiantil, esto se logra a través del departamento de vinculación.
- Coloca a egresados y estudiantes activos en empresas que poseen vacantes disponibles, por medio de la instancia de colocación laboral y egresados.
- Participa en ferias empresariales, a través del decanato de gestión de proyectos y programas.

Estas son algunas de las actividades que realiza la empresa UNAPEC, entre otras actividades secundarias no mencionadas, que la universidad realiza como complemento y apoyo al desarrollo empresarial del país.

### 2.2 Operación y Comercialización

La Universidad APEC, realiza varias estrategias para comercializar y mantener la operación de sus productos y servicios, se pueden mencionar las siguientes:

- Promoción en las redes sociales, tanto externas como internas a la universidad.
- Apoyo del departamento de mercadeo institucional, para la promoción de las distintas áreas de la universidad.

- Realiza actividades con los estudiantes de colegios que están cursando su último año, como es el conocido “PUERTAS ABIERTAS” en donde se les muestra el campus y también las opciones de carreras que la universidad brinda.
- Paga publicidad en los medios de comunicación, como son los periódicos, la radio, televisión, entre otros.
- Realiza Volanteos.
- Mantiene las opciones de pagos y financiamientos como es el que se realiza a través de FUNDAPEC.

Por otro lado, el público que persigue la universidad es un público de clase media, que esté motivado a crecer a nivel profesional, va desde 18 a 65 años, según los objetivos están alineados a un público que tenga la necesidad de aprender y desarrollar a nivel académico, la universidad suple esa necesidad con los programas académicos de calidad y certificados por instituciones internacionales reconocidas.

El modelo o estructura organizacional se define como la forma en la que se distribuyen los departamentos, actividades, grupos y profesionales en una empresa. Así lo indica Stephen Robbins en su libro Comportamiento Organizacional, en el que resalta que cada área de una compañía debe estar alineada según sus objetivos en común. (ROBBIN, 20014)

El autor explica que dicho modelo debe basarse en seis pilares:

- La especialización del trabajo.
- La departamentalización según las funciones, agrupaciones o ubicación geográfica de la organización.

### 2.3 Cadena de Mando

La cadena de mando, que se rige bajo un sistema de jerarquía en beneficio de las comunicaciones y coordinaciones en la organización.

- El alcance de control
- La centralización o descentralización
- La formalización del modelo

El organigrama de UNAPEC, va desde las máximas autoridades, las cuales se dividen de la siguiente manera, según la naturaleza de esta institución:

**Primer Nivel:**

La Junta de Directores está conformado por once (11) miembros: un presidente, un vicepresidente, un Tesorero, un secretario y siete miembros; en el cual se generan las orientaciones y políticas para toda la institución. El presidente de la Junta es elegido directamente por la Asamblea General Ordinaria de APEC; los

demás miembros son designados por el Consejo de Directores de APEC; todos ejercen sus funciones por un período de dos (2) años.

**Segundo Nivel:**

La Rectoría constituye el más alto nivel ejecutivo. El Rector es el funcionario de mayor jerarquía en la Universidad, representa a la institución en lo concerniente a su vida académica y administrativa, y desempeña sus funciones por períodos de dos (2) años, que pueden ser renovables hasta un total de tres períodos, es decir, seis años. De la Rectoría dependen la Vicerrectoría Académica, Vicerrectoría de Internacionalización y Vinculación Nacional, Vicerrectoría de Investigación, Innovación y Desarrollo Estratégico y la Vicerrectoría Administrativa Financiera. Bajo su tutela directa también se encuentran otras dependencias, como lo son el Centro Internacional de Altos Estudios y la Dirección de Comunicación y Mercadeo Institucional.

**Tercer Nivel:**

El Consejo Académico es la máxima instancia de decisión para asuntos académicos. Sus decisiones y resoluciones sólo pueden ser modificadas por el propio Consejo. En caso de divergencias, estas deben ser discutidas en la Junta de Directores.

**Cuarto Nivel:**

Este nivel de autoridad reposa en las vicerrectorías, que dirigen la gestión interna de la institución. Actualmente existen las Vicerrectoría Académica (VAC), la Vicerrectoría de Investigación, Innovación y Relaciones Internacionales (VIIRI), la Vicerrectoría de posgrado y la Administración General (AG).

**Quinto Nivel:**

Lo integran los funcionarios ejecutivos, intermedios u operacionales: Decanos, Directores departamentales Académicos y Administrativos.

**Sexto Nivel:**

Este último nivel lo componen los profesores, el personal de apoyo administrativo y los estudiantes.

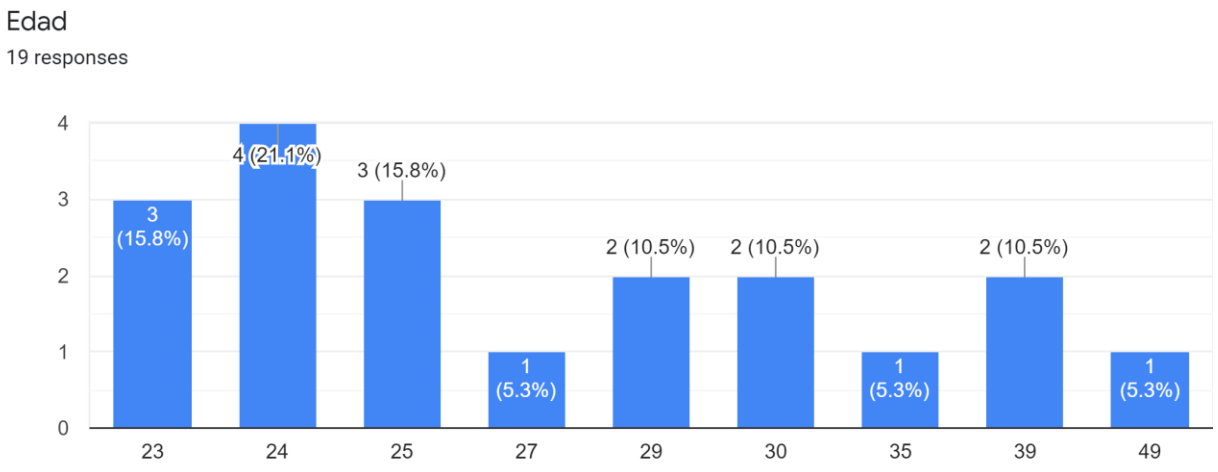
# Capítulo 3: Resultados de la Investigación

La figura de los ciberataques ha sido un fenómeno que se ha desarrollado y mantenido durante los últimos años en la comunidad y diferentes sectores de la República Dominicana, sin embargo, el Área de Gestión Humana al haberse incorporado durante el tiempo hacia la era moderna trayendo consigo diferentes métodos de trabajo, así como, la utilización de algunos medios digitales para la realización de las labores ha concebido la entrada a diversos peligros digitales comunes. Cada uno de estos peligros caracterizan un fin distinto al otro, no obstante, el objetivo principal ha sido la captación de información sobre riesgos y daños al órgano funcional de la Gestión Humana al igual que otras áreas de las organizaciones.

Mediante un estudio de sondeo se lograron identificar los distintos tipos que han experimentado el área de Recursos Humanos, así como, otras áreas a fines de la investigación en la Universidad APEC (UNAPEC). Este estudio ayudó a la identificación de posibles causas o métodos utilizados para la compenetración y captación de informaciones o daños al usuario objetivo por los medios, asimismo, se enumeraron algunos medios utilizados por los usuarios que tuvieron las diferentes formas de ataques.

Este análisis permitió observar la concentración en los diferentes escenarios compuestos en el presente cuestionario apoyado por la investigación realizada a las distintas figuras del área de Recursos Humanos y áreas semejantes de la Universidad APEC (UNAPEC) mediante la herramienta utilizada, Google Forms. Por consiguiente, se detallarán de manera gráfica los distintos escenarios compilados en el formulario esquematizados de forma tabular, gráficos pastel y barras; para una mejor comprensión y entendimiento de los resultados obtenidos.

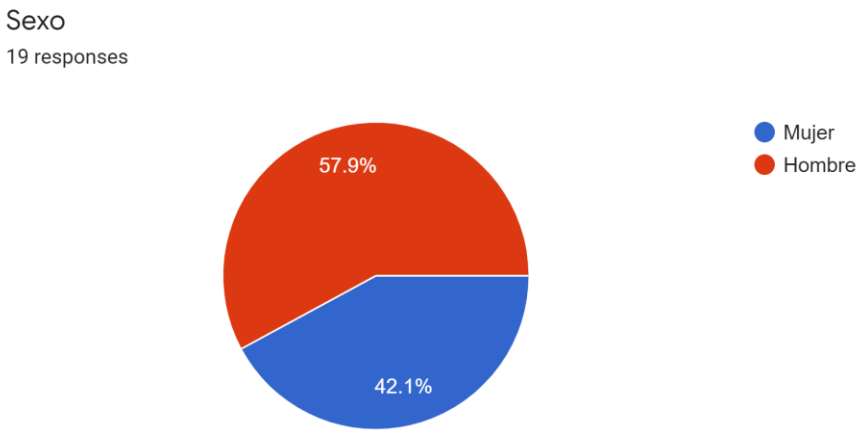
**Gráfico a1:** Edad




De acuerdo con la indagación realizada, las personas encuestadas cuentan entre 23 y 49 años de edad, concediendo un rango positivo para nuestra investigación acorde a la experiencia obtenida por los individuos interrogados. De esta manera,

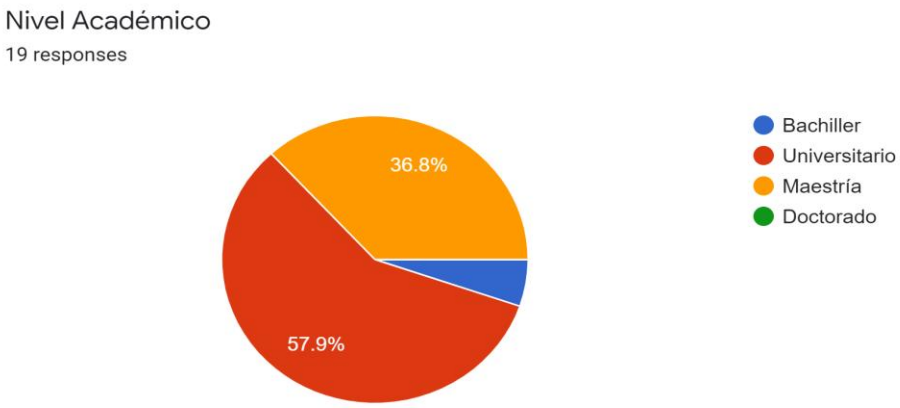
la ampliación en el tema del sujeto de estudio está sostenido por los conocimientos adquiridos del grupo preguntado.

**Grafico a2:** Sexo




De las personas encuestadas el 57.90% proviene del sexo Femenino, siendo la parte predominante en la investigación y de mayor casualidad ante el sujeto estudiado. Por otra parte, el 42.10% pertenece al sexo Masculino el cual ha sido la parte menor de esta investigación.

**Gráfico b1:** Nivel académico




Esta fracción de la encuesta está compuesta por distintos niveles de estudios incluyendo estudios superiores. La mayor parte encuestada es de nivel universitario siendo el 57.90% mientras que el 36.80% proviene del nivel magíster o máster, finalmente el 5.30% proviene del nivel bachiller. Esto implica una diversidad de conocimiento ante el sujeto de estudio lo que hace el nivel de respuesta distinto de acuerdo con el nivel de experiencia.

**Gráfico c1:** Experiencia

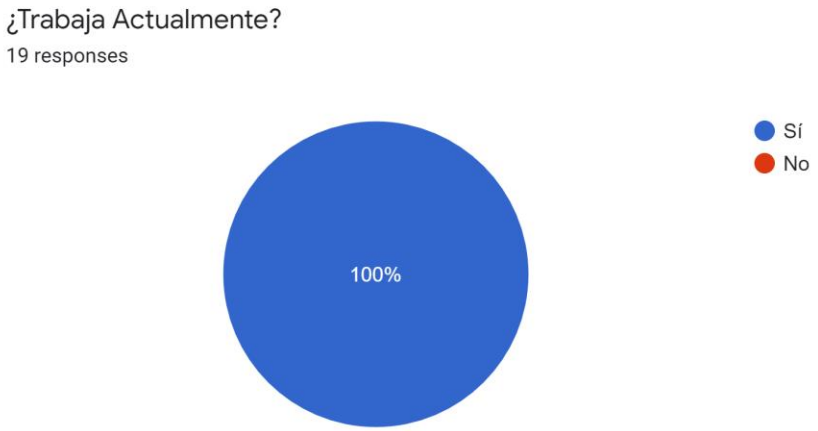
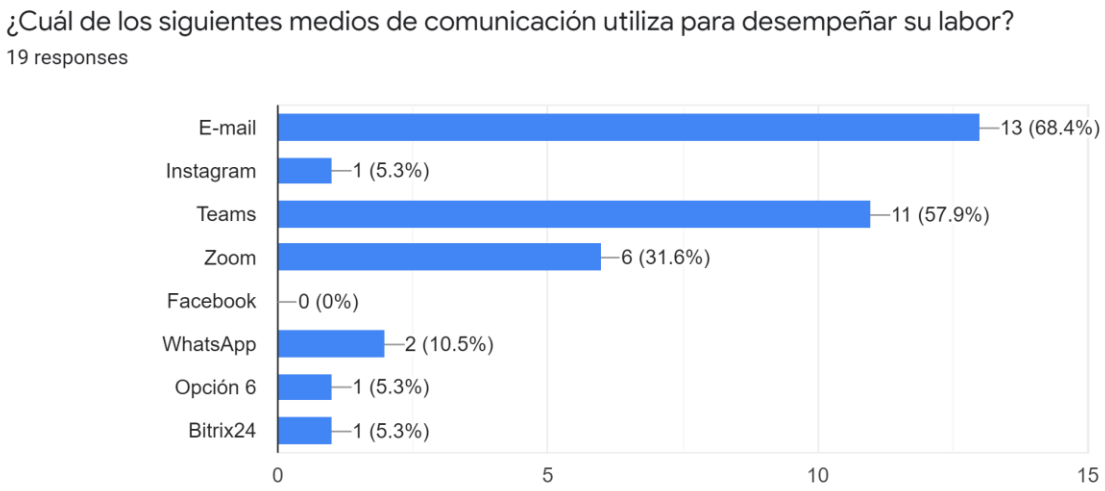



**Gráfico c2:** Relación Recursos Humanos


De acuerdo con la gráfica presentada, nuestra investigación cuenta con un 26.30% de empleados que se dedican a los Recursos Humanos siendo 5 personas con experiencias en Gestión Humana con acercamientos a peligros digitales dentro de sus labores. Por otra parte, el 73.70% pertenece a las 14

personas restantes de las cuales sus labores van acorde a nuestra investigación para fines de recolectar información, en tal sentido, esto ayudó a la ampliación de la toma de muestra y resultados.

**Gráfico b1:** Medios Digitales




De los individuos encuestados, la mayoría siendo el 68.40% utiliza de manera común correos electrónicos para realizar sus labores perteneciendo a 13 de los 19 encuestados; como mencionamos anteriormente en una de nuestras búsquedas citadas en el anteproyecto (Anexo I), la mayor parte de los ciberataques provienen y se dan origen a través de los correos electrónicos debido a que es la herramienta más utilizada y con mayor concentración para la propagación de los daños que causa.  Dentro de otros medios utilizados

actualmente, Zoom conlleva un 31.60%; durante el primer cuarto del año fuentes norteamericanas habían reportado algunos tipos de ataques y robo de datos e identidad que provenían de la red social Zoom, estos tipos de ataques surgieron debido al incremento en los teletrabajos y movilización de las personas hacías sus hogares para realizar otras labores.

Por otra parte, son utilizadas redes sociales; populares, de las cuales son objetivos para el ciberataque como Instagram con un 5.30% y WhatsApp que abarca un 10.50%. Durante los últimos dos años estas redes han reportado incidentes sobre la duplicidad de credenciales e intentos de robo de información de los usuarios.

En el resto se sitúan Microsoft Teams con un 57.90%, una herramienta que se caracteriza por su fluidez y seguridad ha sido la segunda red más utilizada luego del establecimiento de los teletrabajos y realización de otras labores. Por otro lado, en el tramo final se encuentra Bitrix24 con un 5.30%, es una plataforma similar a la de Zoom o Microsoft Teams; es utilizada para realizar actividades comunes en conjunto y la cual es útil para la gestión de personal.

**Gráfico d1:** Utilización de las Redes

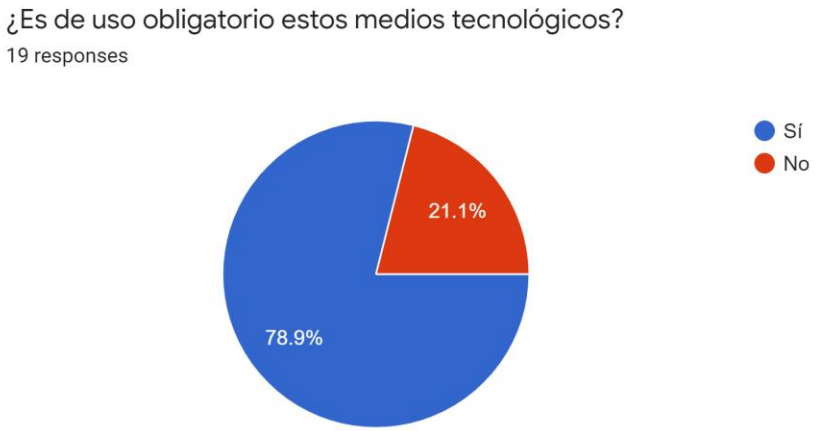
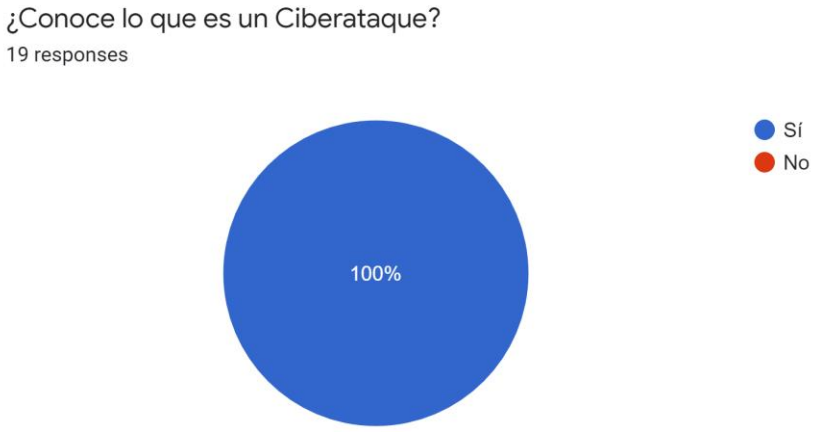


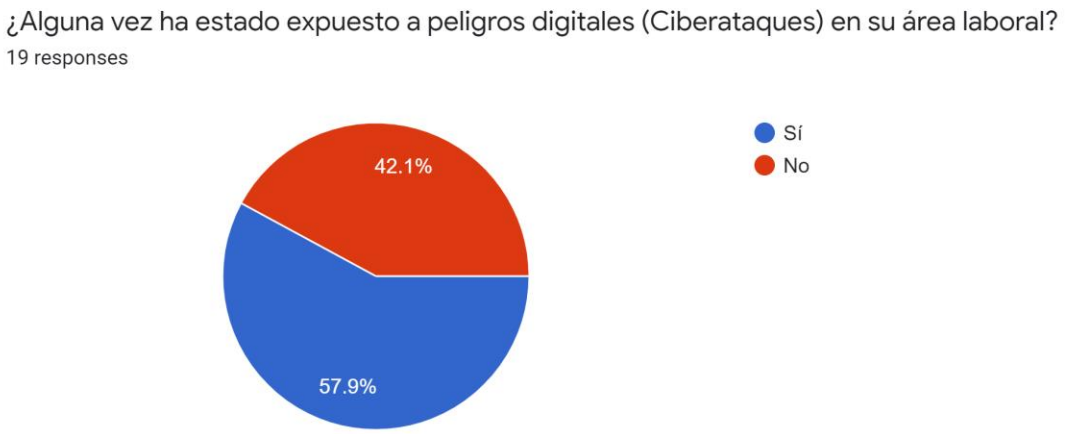

**Gráfico f1:** Conocimiento Ciberataque




Las 19 personas encuestadas tienen conocimiento acerca de lo que es un Ciberataque, esto ha sido positivo debido a que para nuestros fines de

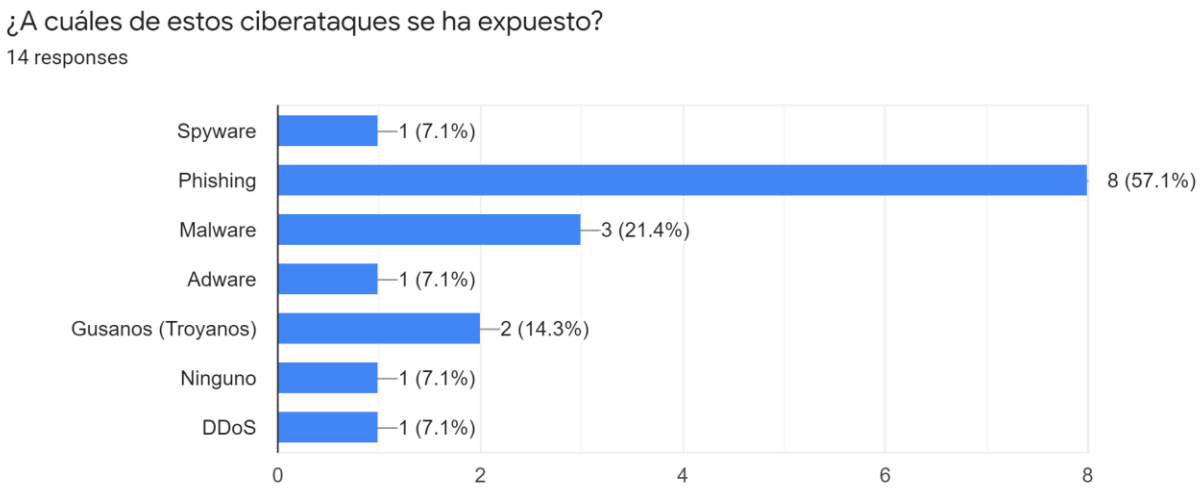
investigación se aprovechó la cognición de los individuos con relación a los ciberataques para la ampliación del campo de estudio, esto en cuestión a resultados y recomendaciones será una vertiente un tanto efectivo.

**Gráfico f2:** Exposición Ciberataque




Por consiguiente, solo el 42.10% de las personas sondeadas se han visto expuestas a los peligros digitales mientras practicaban sus labores, esto deja evidenciado la recurrencia actual de estos ciberataques. De acuerdo con este criterio, servirá de apoyo para las recomendaciones necesarias planteadas a continuación en el presente trabajo. El 57.90% de los individuos restantes no se han visto afectados por los ciberataques en sus labores, no obstante, a sus acercamientos a estos fenómenos fuera de sus trabajos.

**Gráfico c1:** Tipos de Ciberataques

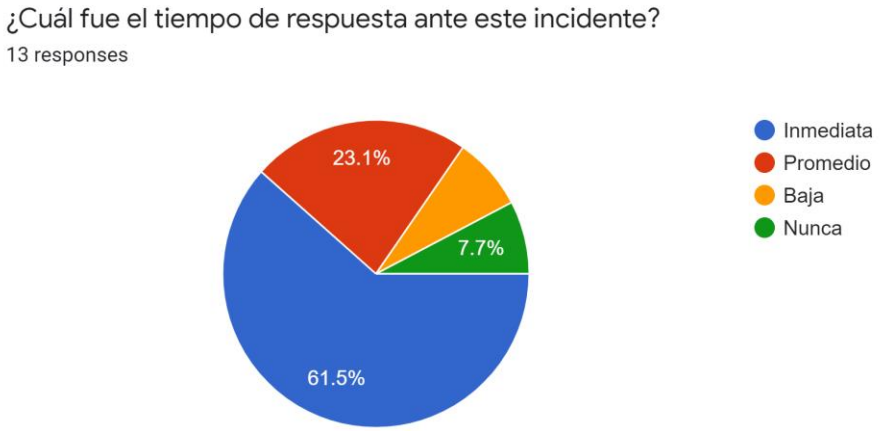



El Phishing es uno de los ataques más comunes y el cual su origen surge en los correos electrónicos, es el ataque de mayor contingencia en nuestra investigación con un 57.10%, por consiguiente, es el ataque con un enfoque mayor en cuanto a la representación de daños causados. Como bien se mencionaba anteriormente, la empresa de seguridad digital Fortinet había reportado que durante el año 2019 fue uno de los ataques con más incrementos en comparación a los Gusanos (Troyanos) de los cuales el 14.30% representa esta investigación, este peligro de origen digital a través de las redes digitales y correos electrónicos, así como, los Spywares con un 7.10%, una herramienta dedicada al robo y recolección de datos personales. Por consiguiente, se encuentra el Malware con un 21.40% representando por 2 de los individuos encuestados, Adware el cual es un tipo de

virus que descarga publicidad maligna al navegar en línea representada por un 7.10%.

Finalmente, otra porción del 7.10% está dirigido hacia los ataques DDoS, el cual es un tipo de peligro dedicado a la inhabilidad de servidores o infraestructura. Cabe destacar que el 7.10% restante está representado por ataques no ocurridos.

**Gráfico e1:** Tiempo de Respuesta




El tiempo de respuesta ante los distintos tipos de peligros es de nivel diversificado, para el 7.70% de las personas preguntadas el tiempo de respuesta ha sido baja mientras que el otro 7.70% ha sido nunca, dando apertura a la propagación a los ataques sufridos por la organización. Este gráfico es ideal para nuestras recomendaciones en el siguiente capítulo consiguiente a los resultados obtenidos.

**Gráfico e2:** Disponibilidad Protocolos de Seguridad


A pesar de las cantidades de tiempo de respuestas promedios, es de importancia destacar las cantidades personas que no cuentan con un protocolo de seguridad para evitar la propagación de los ataques sufridos por los individuos.

**Gráfico e3:** Disposición para Implementar un Sistema de Estrategias

De acuerdo con nuestra indagación, el 73.70% de las personas encuestadas sí está dispuesto a implementar un sistema de estrategias lo que facilita el apoyo de las recomendaciones dictadas posteriormente en la investigación realizada. En tal sentido, es positivo mencionar que esta parte ayudará a disminuir la agresión de los ciberataques de manera discreta y que se busca agotar los métodos para evitar tales peligros.

Esta institución tiene como propósito permanecer en vanguardia al digitalizar gran parte de sus procesos administrativos y educativos, en donde podemos mencionar las gestiones realizadas por el departamento de Recursos Humanos y la exposición a la que se enfrenta la empresa ante individuos dedicados al cibercrimen. Es por lo mencionado anteriormente que se tomó la decisión de ser elegida foco de estudio.

En la investigación realizada, se determinó que en los últimos dos años la universidad no ha sido víctima de ningún evento de seguridad electrónica en los sistemas educativos y financieros. Sin embargo, los usuarios finales se ven diariamente expuestos a peligros digitales que el departamento de Tecnología se encarga de mitigar. El peligro más frecuente al que se ha enfrentado la universidad es el SPAM o correo no deseado, ya que diariamente reciben cientos de correos de este tipo dirigidos a los usuarios; los mismos son bloqueados a tiempo o reportados por los mismos receptores.

Con respecto a la variedad de sistemas utilizados para la prevención de fraudes y ciberataques, no fue posible detallar los programas en específico que utilizan. No obstante, se pudo resaltar el uso de la suite de Microsoft Office 365 ATP para el caso de SPAM al ser el peligro con mayor recurrencia al que se ven expuestos. Gracias al filtrado de los correos electrónicos, a pesar de ser el más común los casos son mínimos y suelen ocurrir por errores humanos ante el uso de la tecnología.

# Conclusiones

La evolución sin final de las tecnologías, medios digitales, así como, sus usos, impactan directamente sobre el deber de desarrollar soluciones de ciberseguridad que se adapten a cada necesidad de las entidades empresariales, también, como lo es la Gestión Humana. En el informe elaborado la ciberseguridad fue un tópico clave y en la exploración realizada se amplió detalladamente dentro de los resultados acerca de todas las incidencias relacionadas a los peligros digitales, y de los cuales se puntualizan estos tópicos en el capítulo 3 del presente trabajo. De lo planteado en la herramienta de estudio se recolectaron unas series de muestras que sirvió para dar soporte a las conclusiones y recomendaciones a aplicar en el informe realizado.

Los correos electrónicos como herramientas de trabajo, a pesar de ser útiles y comunes en las instituciones, es el medio con un foco más orientado a recibir diferentes tipos de ataques digitales, originando niveles que pueden afectar de manera tanto insignificante como masiva, asimismo, a niveles colaterales. Actualmente unas de las herramientas que han ayudado a mediar la atención hacia este foco han sido las de comunicación instantánea Zoom y Microsoft Teams; ambas redes digitales han desviado la carga de trabajo y han utilizado la encriptación de documentos sensibles. Sin embargo, la utilización de redes sociales para la continuación de las labores ha dado a exponer múltiples maneras

de adecuar al sujeto a atacar para llevar a fines dichos delitos mediante spam u otras técnicas.

El conocimiento sobre el fenómeno que son los ataques cibernéticos amplifica las probabilidades de identificación de los diversos entes como los previamente mencionados, por ende, el incremento de conciencia existente agudiza la manera en que los individuos pueden manejar las diversas situaciones en las que se encuentren.

Sin embargo, no obstante, al conocimiento de los delitos digitales, la exposición a las que se han encontrado los sujetos ha dejado secuelas y de las cuales el tiempo de respuesta son escasas dejando una abertura a la continuidad de los delitos que circulan en la organización objeto y así afectar los protocolos establecidos; originando ineficiencias.

En otro escenario, la introducción a nuevos mecanismos de combate contra los ciberataques en las entidades de la República Dominicana provee a todos los recursos humanos nuevas metodologías de atenuación que sirven como alternativa para la generación de incremento en la protección de sus capitales, por tal, la protección y encriptación de datos manejados por cada personal.

Con la proposición de tales mecanismos es posible recrear escenas que ayudan a la toma de decisiones, asimismo, la validez de los distintos niveles de

ciberseguridad; como eficientizar los procesos al instante de operar. Es cierto que, al implementar una propuesta señalada previamente, le agrega plusvalía a los recursos digitales que posee la entidad y la realización de nuevos procesos.

# Recomendaciones

1. Capacitación y Concientización de Seguridad Cibernética: Los usuarios son parte importante del ambiente y pueden llegar a ser el eslabón más débil. No importa que tan elevado son los controles y mecanismos si se produce algún ataque debido a una exposición interna pueden afectar los controles que se tengan preparados.
2. Gestión de Riesgo: No es posible eliminar el riesgo a ataques, pero si es posible mitigar el riesgo. Con esto se puede realizar un levantamiento de la infraestructura y procesos de la organización para determinar el tipo de riesgos que están expuestos y el impacto que estos pueden llegar a tener. Sin antes realizar un análisis de riesgo no es posible levantar controles apropiados que se adecuen con el entorno de una empresa.
3. Fortalecimiento en Mecanismos de Autorización y Autenticación: Es importante contar con controles que utilicen más de un (1) método de autenticación para la validación de credenciales y es importante revisar de manera periódica los niveles de autorización de los usuarios sobre los diferentes niveles de permisos que tienen dentro de una empresa.
4. Sistema de Actualización y Ejecución de Parches: Es importante mantener al día los sistemas que se utilizan y el de los antivirus ya que cuando se lanza un parche o actualización es para corregir fallas conocidas en las

versiones actuales y mantener una versión obsoleta puede llevar a vulnerabilidad de dichos sistemas.

5. Contar con Herramientas Automatizadas de Defensa: Hoy en día los sistemas de ciberdefensa que funcionan con una base de datos de problemas conocidos ya no son suficiente ya que los ataques se vuelven cada vez más sofisticados, es importante contar con mecanismos de defensas que puedan recolectar logs (sucesos) de lo que se acontece en una red y correlacionar los eventos que suceden para tomar acciones más apropiadas.

# Bibliografía


APEC, U. (01 de enero de 2020). *unapec* . **Consultada : 06 de agosto 2020** Obtenido de sobre nosotros : https://unapec.edu.do

ciberseguridad, c. n. (04 de abril de (2020)). **Consultada : 23 de junio 2020** *ciberseguridad en tiempos de covid-19*. Obtenido de cncs.gob.do: https://www.instagram.com/p/CBnazRxDPvi/?igshid=18pwzvgeb2wic

ciberseguridad, c. n. (01 de diciembre de 2019). **Consultada : 22 de junio 2020** *Glosario de terminos de ciberseguridad*. Obtenido de cncs.gob.do: https://cncs.gob.do/wp-content/uploads/2019/12/Glosario-de-Terminos-de-Ciberseguridad.pdf

DICAT. (16 de enero de 2020). **Consultada : 02 de agosto 2020** *departamento de investigacion de crimenes y delitos de alta tecnologia* . Obtenido de delitos electronicos : https://dicat.gob.do/

Digital, U. (02 de diciembre de 2019). **Consultada : 22 de junio 2020** *riesgos digitales como conocerlos y gestionarlos*. Obtenido de www.unir.net: https://www.unir.net/empresa/revista/noticias/riesgos-digitales-como-conocerlos-y-gestionarlos/549204181484/

elDinero. (26 de noviembre de 2019). **Consultada :22 de junio 2020** *elDinero*. Obtenido de www.eldinero: https://www.eldinero.com.do/94321/republica-dominicana-sufrio-mas-de-106-millones-de-intentos-de-ciberataques-entre-abril-y-septiembre-de-2019/

electronicas, A. (20 de marzo de 2020). **Consultada : 2020** *estos son los crimenes tecnologicos mas comunes en RD segun la procuraduria*. Obtenido de audienciaselectronicas.net: http://www.audienciaelectronica.net/2017/11/estos-son-crimenes-tecnologicos-mas-comunes-en-rd-segun-procuraduria/

empresarial, r. (20 de enero de 2020). **Consultada : 10 de julio 2020** *gestion humana*. Obtenido de revistaempresarial.com: https://revistaempresarial.com/gestion-humana/

Gob., D. (01 de enero de 2020). **Consultada : 22 de junio 2020** *dominicana.gob.do*. Obtenido de index.php: http://dominicana.gob.do/index.php/seguridad-y-delito-electronico

L., L. J. (16 de febrero de 2019). **Consultada :30 de junio 2020** *libro blanco de la universidad* . Obtenido de peligros digitales y gestion : https://books.google.com.do/books?id=u_nkCgAAQBAJ&pg=PA266&lpg=PA266&dq=opiniones+de+autores+sobre+los+peligros+digitales+en+gestion+humana&source=bl&ots=Y2Rn3a_FVb&sig=ACfU3U2KKjSSLzoEh_LbhpUX-wGzOZz4cw&hl=es-419&sa=X&ved=2ahUKEwjM29yskqzqAhVqRN8KHbVpANA

ROBBIN, S. (20014). **Consultada : 22 de junio 2020** COMPORTAMIENTO ORGANIZACIONAL. En s. robbin, *comportamiento organizacional* (pág. 670). los angeles, california: PERSON.

# Apéndices

**Anexo No.1 – Anteproyecto**

Introducción

Contexto

Actualmente en la República Dominicana las organizaciones no cuentan con la defensa requerida en cuanto a ciberseguridad se refiere y se ven regularmente expuestas a peligros digitales. Una de las áreas fundamentales dentro de la compañía es la de Gestión Humana, debido a que posee información confidencial y de suma importancia sobre el personal de la empresa; por lo cual es una de las áreas más propensas a ser afectadas por este tipo de peligros.

Es importante destacar que el área de Gestión Humana se encuentra en una constante evolución en cuanto a sus procesos y estructuras. Sin embargo, son muchas las compañías que hoy en día invierten poco en la seguridad digital y como consecuencia, se ven expuestas ante riesgos generados por entidades dedicadas al delito cibernético que pueden causar daños incalculables en caso de que información privilegiada caiga en manos equivocadas.

Según el glosario de términos del Ciber-Observatorio del Centro Nacional de Seguridad de Ciberseguridad de la Rep. Dom. define como Ciberataques o Cibercrimen “Los actos delictuales donde el ciberespacio es el objeto del delito o

su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos". Sin embargo, muchos de estos peligros digitales están dirigidos hacia el robo de informaciones sensibles de las organizaciones más que el daño de estas. (p.2)

Es por tal, que las empresas u organizaciones buscan poder detener estos tipos de peligros o ciberataques, un solo acto delictivo puede causar en cualquier intento, circunstancias desfavorables trayendo consecuencias negativas en cuanto al funcionamiento provocando indisponibilidad. No obstante, no todas las organizaciones actúan antes de que ocurra el acto, más bien, cuando ya ha sido realizado.

## Planteamiento del Problema

Hoy en día cualquier individuo o empresa puede verse afectado ante un ataque cibernético debido al incremento del uso de redes digitales en los últimos tiempos. Según un estudio realizado por Bromium, que muestra cómo los ingresos por delitos digitales han aumentado a 1,5 billones de dólares anuales en ganancias ilícitas. Son muchos los sitios web populares que se enfrentan a ataques de mayor envergadura y de alta tecnología todos los días, siendo víctimas de la creciente tendencia ciberataque.

Enfocándonos en la República Dominicana, con el incremento de los últimos meses del teletrabajo, clases virtuales y el contacto con personas a través de dispositivos electrónicos por motivo del estado de emergencia en el que nos encontramos, las autoridades han detectado un aumento en estafas cibernéticas.

De acuerdo con las estadísticas emitidas por el Centro Nacional de Ciberseguridad, pudieron visualizar un incremento de un 150% en dominios utilizados para generar actividades maliciosas, 140% de phishing o mejor conocido como enlaces maliciosos y un 180% en divulgación de noticias falsas, siendo una gran parte dirigidas a las organizaciones empresariales que se encuentran operando remotamente por lo que se puede especular que una muestra de esta parte fue dirigida a órganos esenciales incluyendo Recursos Humanos.

Por otra parte, según un informe presentado por la Compañía de Ciberseguridad Fortinet, en el año 2019 la Rep. Dom. sufrió más de 106 millones de ciberataques siendo las amenazas principales que fueron dirigidas a la red: descargas no deseadas, criptojacking, explotación de vulnerabilidades, malware y troyanos; quienes se encargan de buscar información y robarlas a usuarios. No obstante, a esto, la prevalencia de estos ataques ya es conocido por los receptores y de los cuales tienen remediación, por lo que esto da a demostrar que aún es necesario el desarrollo de prevenciones ante malwares o ataques.

## Objetivo General

Identificar los peligros digitales y su impacto en el ámbito de gestión humana, en una organización de la República Dominicana para mitigar los riesgos junto a un área especializada de tecnología con parámetros, año 2020.

## Objetivos Específicos

1. Medir el impacto de la tecnología defectuosa en el área de Gestión Humana.
2. Mencionar los peligros digitales a los que se enfrenta el área de Gestión Humana.
3. Determinar los sistemas de prevención utilizados para evitar el fraude digital en el área de gestión humana.
4. Analizar la evolución de los peligros digitales en los últimos cinco años en el área de gestión humana.
5. Explicar las consecuencias a las que se enfrentan los empleados al ser víctimas de los riesgos digitales relacionada con la información que maneja la gestión humana.

## Justificación de la Investigación (Teórica)

El propósito de esta investigación es identificar los distintos niveles de peligro que han atacado a las áreas de gestión humana en las organizaciones empresariales

de la República Dominicana a nivel digital, de igual manera, medir el impacto que causan estos riesgos al ser incorporarse a los sistemas tecnológicos de dicha área. Así también, identificar qué posibles medidas han tomado las áreas u organizaciones para combatir este ente y fomentar una mayor seguridad para las organizaciones. En la actualidad las empresas u organizaciones corren un sin números de riesgos al querer transformarse a la era tecnológica o simplemente migrar informaciones a sistemas digitales. De acuerdo con UniRsevista (2019), intentar aplicar un proceso de transformación en las empresas requiere un cambio de mentalidad antes de ir a la acción, esto exige analizar el estado del cual se parte. Ser digital en una empresa implica conocer los riesgos, amenazas y posibles sanciones que pueden ocurrir al desarrollar la actividad.

Dado a todo esto, es por tal razón que el fin de esta investigación es poder identificar estos tipos de riesgos o peligros para poder medir la gravedad del impacto que esta causa en las áreas de Gestión Humana de una organización.

Justificación de la Investigación (Metodológica)

Para lograr los objetivos definidos para esta investigación, se recurrirá a implementar técnicas científicas que ayudarán al desarrollo de la investigación, tales como: la técnica estadística, la técnica descriptiva y la técnica deductiva. Estas técnicas servirán de soporte para obtener el resultado de dicha investigación.

## Justificación de la Investigación (Práctica)

Esta investigación se realiza porque existe la necesidad de medir el grado e identificar los peligros a los cuales las áreas de gestión humana están expuestas. Con el uso del resultado validado de la indagación realizada, la organización podrá establecer parámetros que permitirán minimizar la extracción de informaciones y otros tipos de peligros comunes.

## Preguntas de la Investigación

Del propósito de estudio que justifica esta investigación se derivan las siguientes preguntas de investigación:

1. ¿A qué se debe el alto nivel de ataques que causa este peligro en las áreas de Gestión Humana?
2. ¿Cuáles medidas han adoptado las organizaciones para evitar estos tipos de riesgos?
3. ¿Cuáles son los efectos que causaría a las organizaciones el establecer parámetros para frenar este riesgo?

## Tipos de investigación

Luego de analizar los diversos tipos de investigación existentes, hemos decidido implementar los siguientes:

### Histórica

Realizaremos un viaje al pasado, para conocer la evolución que ha tenido el mundo digital dentro el área de Gestión Humana y cuáles son las ventajas y desventajas que vivimos hoy en día gracias a esto.

### Documental

Analizaremos la información disponible relacionada con nuestro objeto de estudio.

### Descriptiva

Procederemos a identificar, analizar y plasmar las características de nuestro caso de estudio.

## Marco de Referencia

### Teórico

Reinmoller y Senoo, citan en el libro blanco de la universidad digital (2010), citan que, para una empresa grande, es esencial un buen manejo de las TIC, no

dejando a un lado la advertencia de los peligros digitales, que se encuentran exclusivamente en el área de gestión humana.

Bulchand y Rodríguez (2004), menciona que la gestión del conocimiento de los peligros digitales es muy limitada, debido a la exclusividad humana en lo que a obtener información a partir de datos personales a los que se refiere.

Los autores Meso y Smith (2000), identificaron tecnologías a las que se denominan tecnologías de conocimiento, y las agruparon según su función en el área de gestión del conocimiento y áreas puntuales de una organización, como es la gestión de personal.

Por otro lado, el autor Gartner, en su encuesta anual Gartner Executive Programs Annual CIO Survey, señala que la mejora en la seguridad de IT Governance ha pasado de la prioridad 10 a la 8, en dos años, es decir, la importancia de este factor ha escalado dos puestos de importancia.

Conceptual

Ciberataque, son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet.

Gestión Humana, se define, como el conjunto de procesos necesarios para dirigir a las personas dentro de una empresa.

Peligros Digitales, también conocido como riesgos digitales, son amenazas operaciones que cubren daños a la propiedad material de una organización.

Ciberseguridad, se le conoce como la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

Sistemas Electrónicos, es un conjunto de circuitos que interactúan entre sí para obtener un resultado.

Espacial

El espacio al que se aplicará la investigación es al área de Gestión Humana de la compañía de seguros BMI en Santo Domingo, República Dominicana.

Temporal

La información extraída y de la cual se utilizará corresponde al período entre el año 2018 y el año 2020, de acuerdo con esto se podrá plasmar la evolución que ha tenido el tema de riesgos digitales en el tiempo indicado.

Metodología de la Investigación

La naturaleza de esta investigación es la descriptiva, ya que se analizaron las causas de los ataques digitales y los peligros que estos riesgos le generan a las Áreas de Gestión Humana en las organizaciones empresariales en la República Dominicana. De igual forma, se identificaron las ventajas que proveen los parámetros establecidos en las organizaciones. El método de investigación utilizado fue el deductivo, debido a que se partió de las informaciones captadas de manera general, para luego determinar por qué las organizaciones son afectadas recurrentemente por entes digitales de naturaleza delictiva.

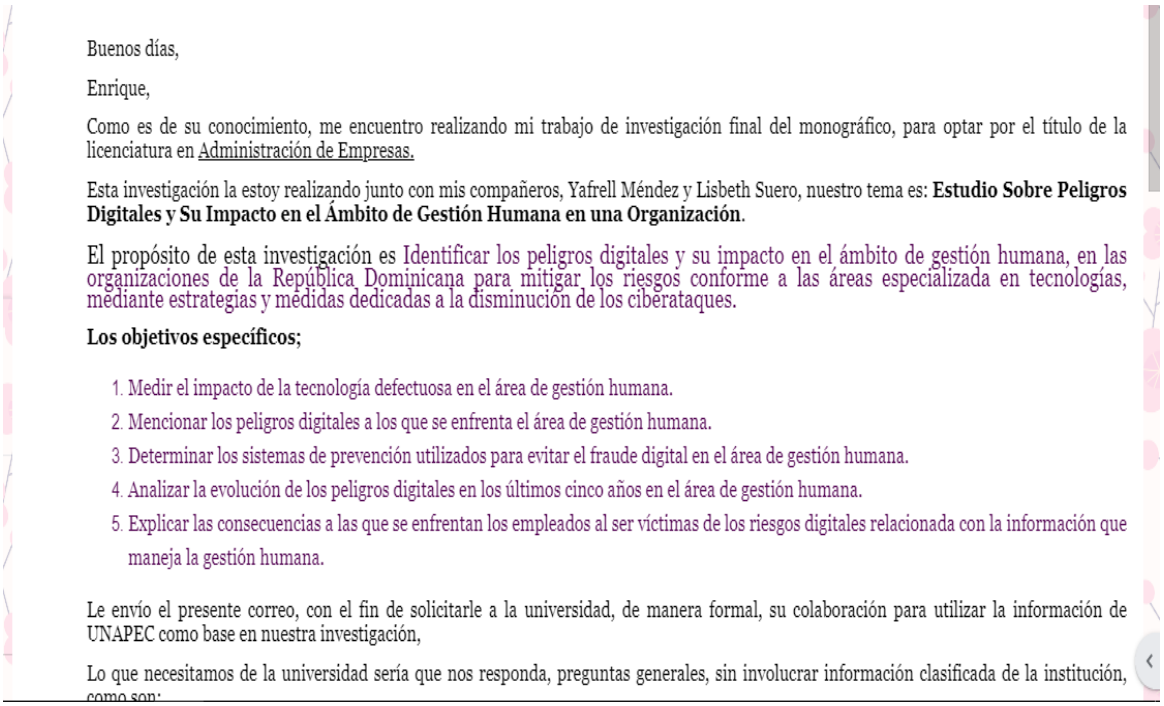
Dentro de las técnicas de investigación que fueron utilizadas, están la documental, debido a que se compilaron informaciones relacionadas a las de los delitos digitales afectadas por las áreas de gestión humana dentro de las organizaciones empresariales, estas informaciones fueron recopiladas de fuentes confiables que ayudaron a la organización y análisis del desarrollo del trabajo.

De igual forma, se utilizó la técnica de investigación documental, indagando cómo ha ido evolucionando los ataques de orígenes virtuales, de tal, manera se recopiló la cantidad de datos necesarios que servirán como soporte para continuar con el desarrollo del trabajo que se estará realizando. También, el rol que han desempeñado los entes empresariales para combatir estos tipos de delitos para mitigar o promover una mejor protección bajo las circunstancias que se han encontrado. Esta técnica permitió establecer una relación en segundo plano con

informaciones claves, sobre los sucesos y funcionamientos de las distintas herramientas utilizadas para realizar los ciberataques.

La investigación documental fue realizada a través de la recopilación de datos de distintas fuentes y mediante una comparación de las distintas formas de riesgos, las cuales son las más usuales en la Rep. Dom., se logró analizar el grado de incidencia e impacto en la Gestión Humana tanta de manera directa como indirecta. Fue así, que se logró recolectar la información necesaria para la obtención del resultado de esta investigación.

**Anexo No. 2 – Solicitud Autorización para Realizar Investigación**



Buenos días,

Enrique,

Como es de su conocimiento, me encuentro realizando mi trabajo de investigación final del monográfico, para optar por el título de la licenciatura en Administración de Empresas.

Esta investigación la estoy realizando junto con mis compañeros, Yafrell Méndez y Lisbeth Suero, nuestro tema es: **Estudio Sobre Peligros Digitales y Su Impacto en el Ámbito de Gestión Humana en una Organización**.

El propósito de esta investigación es Identificar los peligros digitales y su impacto en el ámbito de gestión humana, en las organizaciones de la República Dominicana para mitigar los riesgos conforme a las áreas especializada en tecnologías, mediante estrategias y medidas dedicadas a la disminución de los ciberataques.

**Los objetivos específicos;**

1. Medir el impacto de la tecnología defectuosa en el área de gestión humana.
2. Mencionar los peligros digitales a los que se enfrenta el área de gestión humana.
3. Determinar los sistemas de prevención utilizados para evitar el fraude digital en el área de gestión humana.
4. Analizar la evolución de los peligros digitales en los últimos cinco años en el área de gestión humana.
5. Explicar las consecuencias a las que se enfrentan los empleados al ser víctimas de los riesgos digitales relacionada con la información que maneja la gestión humana.

Le envío el presente correo, con el fin de solicitarle a la universidad, de manera formal, su colaboración para utilizar la información de UNAPEC como base en nuestra investigación,

Lo que necesitamos de la universidad sería que nos responda, preguntas generales, sin involucrar información clasificada de la institución, como son:

...

--
Raquel Rosario

**Enrique Ernesto Eusebio Landestoy** 4 ago. 2020 13:04 (hace 8 días)
para Carmen, Larissa, mí

Buenas tardes,

Respuestas en verde:

1. ¿ha sido víctima UNAPEC de los peligros digitales en los últimos 2 años?

   No, actualmente UNAPEC no ha sido víctima de ningún evento de seguridad en los sistemas académicos y financieros.

   Dicho esto, lo usuarios finales se ven diariamente expuestos a peligros digitales del cual nos encargamos de mitigar.

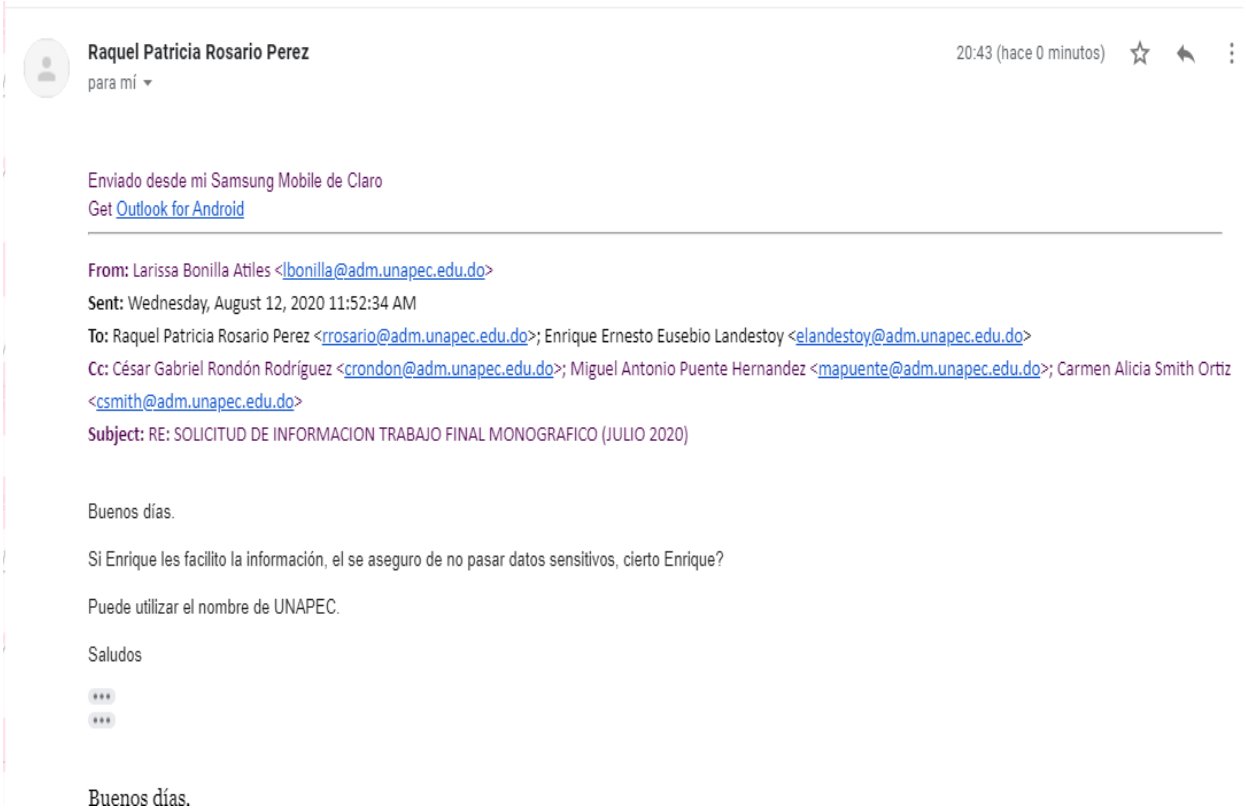
2. ¿Cuáles han sido estos peligros digitales a los que la universidad le ha hecho frente?

   El peligro más frecuente es el SPAM o correo electrónico no decesado, diariamente recibimos cientos de correos de este tipo dirigidos a los usuarios los mismos son bloqueados con éxito o reportados por usuarios.

3. ¿Cuántos casos han tenido en los últimos 2 años?

   Debido al sistema de filtrado de correo electrónico los casos de este tipo son mínimos.

   Luego tenemos otros tipos de controles avanzados que en caso de error humano eliminan la amenaza antes de convertirse en un



**Raquel Patricia Rosario Perez** 20:43 (hace 0 minutos)

para mí

Enviado desde mi Samsung Mobile de Claro
Get Outlook for Android

---

**From:** Larissa Bonilla Atiles <lbonilla@adm.unapec.edu.do>
**Sent:** Wednesday, August 12, 2020 11:52:34 AM
**To:** Raquel Patricia Rosario Perez <rrosario@adm.unapec.edu.do>; Enrique Ernesto Eusebio Landestoy <elandestoy@adm.unapec.edu.do>
**Cc:** César Gabriel Rondón Rodríguez <crondon@adm.unapec.edu.do>; Miguel Antonio Puente Hernandez <mapuente@adm.unapec.edu.do>; Carmen Alicia Smith Ortiz <csmith@adm.unapec.edu.do>
**Subject:** RE: SOLICITUD DE INFORMACION TRABAJO FINAL MONOGRAFICO (JULIO 2020)

Buenos días.

Si Enrique les facilito la información, el se aseguro de no pasar datos sensitivos, cierto Enrique?

Puede utilizar el nombre de UNAPEC.

Saludos

•••
•••

Buenos días.

**Anexo No. 3 – Cuestionario Investigación**

# Evaluación Conocimientos y Exposición ante Ciberataques

Somos un grupo de estudiantes el cual está trabajando para la implementación de estrategias contra los ciberataques.

Esta gestión es para fines de trabajo de grado, por lo que apreciamos mucho que pueda colaborar con sus respuestas.

* Required
1. Edad *

2. Sexo *

*Mark only one oval.*
Mujer Hombre

3. Nivel Académico *

*Mark only one oval.*
Bachiller Universitario Maestría Doctorado Other:

4. ¿Trabaja Actualmente? *

*Mark only one oval.*
Sí No

5. ¿Su labor se relaciona con los recursos humano? *

*Mark only one oval.*
Sí No
Other:

6. ¿Cuál de los siguientes medios de comunicación utiliza para desempeñar su labor? *

*Check all that apply.*
E-mail Instagram Teams Zoom Facebook

Other:

7. ¿Es de uso obligatorio estos medios tecnológicos? *

*Mark only one oval.*
Sí No

8. ¿Conoce lo que es un Ciberataque? *

*Mark only one oval.*
Sí No
Other:

9. ¿Alguna vez ha estado expuesto a peligros digitales (Ciberataques) en su área laboral? *

*Mark only one oval.*
Sí No
Other:

10. ¿A cuáles de estos ciberataques se ha expuesto?

*Check all that apply.*
Spyware Phishing Malware Adware
Gusanos (Troyanos) Other:

11. ¿Cuál fue el tiempo de respuesta ante este incidente?

*Mark only one oval.*
Inmediata Promedio Baja Nunca

12. ¿Cuentan con protocolos de seguridad para evitar los ciberataques? *

*Mark only one oval.*
Sí No
Other:
13. ¿Estaría dispuesto a implementar un sistema de estrategias para disminuir los ciberataques? *

*Mark only one oval.*
Sí No
Tal vez

14. Edad *

15. Sexo *

*Mark only one oval.*
Mujer Hombre

16. Nivel Académico *

*Mark only one oval.*
Bachiller Universitario Maestría Doctorado Other:

17. ¿Trabaja Actualmente? *

*Mark only one oval.*
Sí No

18. ¿Su labor se relaciona con los recursos humano? *

*Mark only one oval.*
Sí No
Other:

19. ¿Cuál de los siguientes medios de comunicación utiliza para desempeñar su labor? *

*Check all that apply.*
E-mail Instagram Teams Zoom Facebook
Other:

20. ¿Es de uso obligatorio estos medios tecnológicos? *

*Mark only one oval.*
Sí No
21. ¿Conoce lo que es un Ciberataque? *

*Mark only one oval.*
Sí No
Other:
22. ¿Alguna vez ha estado expuesto a peligros digitales (Ciberataques) en su área laboral? *

*Mark only one oval.*
Sí No
Other:
23. ¿A cuáles de estos ciberataques se ha expuesto?

*Check all that apply.*
Spyware Phishing Malware Adware
Gusanos (Troyanos) Other:
24. ¿Cuál fue el tiempo de respuesta ante este incidente?

*Mark only one oval.*
Inmediata Promedio Baja Nunca
25. ¿Cuentan con protocolos de seguridad para evitar los ciberataques? *

*Mark only one oval.*
Sí No
Other:
26. ¿Estaría dispuesto a implementar un sistema de estrategias para disminuir los ciberataques? *

*Mark only one oval.*
Sí No

Tal vez