Universidad Nacional Pedro Henríquez Ureña

Facultad De Humanidades Y Educación

ESCUELA DE PSICOLOGÍA

"Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

SUSTENTANTE:

Sacha Mariela Santos Molina 10-1029

ASESORADA POR:

MA. Ana Gisela Ramos B.

Trabajo presentado como requisito para la obtención del título de grado en

Licenciada en Psicología Industrial

Santo Domingo,

República Dominicana,

Septiembre 2014

“Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana”.

Índice de contenido

Índice de tablas

Índice de gráficos en anexos

Agradecimientos

En primer lugar, debo dar gracias a Dios por todas las bendiciones que me regala cada día y permitirme ver llegar el momento de poner fin a mi carrera universitaria logrando todas las expectativas esperadas.

A la Universidad Nacional Pedro Henríquez Ureña (UNPHU), porque en cuatro años de carrera no puedo decir nada que no sea positivo de ella. Agradecer tanto a Adrian De Oleo, actual Directora de la Escuela de Psicología como a Evelyn Rivera, ex directora, porque siempre en cada solicitud tanto de mi Escuela como de los demás Departamentos se me dio el soporte y las atenciones requeridas. A todos los maestros que conocí, quienes siempre me estimulaban para dar lo mejor de mí, y a exigirme más porque decían que tenían que explotar todo mi potencial.

Agradezco a mis jurados, porque también estuvieron conmigo siempre a la disposición en estos cuatro años, y ahora les ha tocado aportar sugerencias en lo que es mi Trabajo de Grado, todas recibidas de manera muy conforme porque son excelentes profesionales.

También necesito poner en alto las personas que me ayudaron a recopilar las informaciones necesarias para aplicar mi encuesta de tesis en cada una de las empresas de las telecomunicaciones que solicité, porque sé que el tema es complejo y aun así me dieron la confianza y la oportunidad permitiéndome conocer sobre su empresa para futuros aportes en el sector de las telecomunicaciones. Katherine y Eridalia, gracias por siempre estar ahí apoyándome y acompañándome en todo, hasta en las noches largas de estudio.

Dedicatorias

Dedico este material a mis padres por educarme en valores e inculcarme en todo el transcurrir de mi vida los mejores principios morales y éticos. Papi y mami, son mi norte a seguir, no puedo hablar por separado de ustedes porque los dos son mi vida y les agradezco todo lo que soy hoy. Este logro es más de ustedes que mío. No existen palabras que definan lo que son para mí, ni para agradecerles porque no me da lo que me queda de vida para hacerlo.

A mis hermanos, abuela y tíos, esperando siempre conservemos esa unidad familiar.

Gisela Ramos, nunca me imaginé que la asignación de un asesor que escuchara mis inquietudes y propósitos iba a ser algo tan cómodo, no tengo como agradecerte tus extendidas discusiones y cuantiosos aportes en todo este transcurso. Desde la primera asignatura que recibí contigo me di cuenta que eras la docente idónea para acompañarme en esta fase. Percibía que nos íbamos a entender muy bien porque siempre te comportaste conmigo muy despreocupada por cómo respondería a las asignaciones, ya que siempre has confiado de mis capacidades.

Yanilsa, te dedico este material por permitirme contar con todo tu apoyo siempre. Has sido quien deduce todas mis inquietudes ya que aparte de mi profesora, somos colegas y estamos en el mismo sector de las telecomunicaciones, por eso antes de que yo dijera las cosas ya estabas aportándome sugerencias por toda la experiencia que tienes en el área de Gestión Humana.

Tía y Juan Elías. Porque desde que se pensó la idea de que yo estudiara en Santo Domingo, me adoptaron como su hija sin pensarlo y no hubo un día que no estuvieran conmigo dándome su apoyo, a veces hasta dejando a un lado sus necesidades personales para ayudarme incondicionalmente. Que la vida les pague lo desprendidos que son para ayudar a las personas que quieren, personas así hay muy pocas en este mundo.

A ti Sergio, porque espero poder verte crecer y estar a tu lado en cada paso que des, que seas siempre una persona de bien. Ojalá acontecimientos como este te estimulen a dar siempre lo mejor de ti, porque para ti solo quiero éxitos en esta vida.

Finalmente pero no menos especial, dedico este material a Elvira Hernández, porque eres un estímulo para seguir luchando cuando a veces creemos que no se puede seguir. Madrina, toda la motivación y el apoyo que he necesitado para seguir adelante me lo has dado siempre. Eres un ejemplo a seguir, gracias por tanto, por tu cariño y consentirme como si hubiese salido de tus entrañas desde que sabías que iba a nacer.

Resumen analítico sistémico

Resumen analítico sistémico

Título: "Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

Autor (a): Sacha Mariela Santos Molina

Resumen: Se diseñó una encuesta aplicada a una muestra de 37 empleados de los Departamentos de Gestión Humana, Seguridad Informática, Tecnología, Ventas y Control de Fraudes de las principales empresas del sector de las telecomunicaciones, para identificar las debilidades existentes dentro de las Políticas y Procedimientos de los Departamentos de Gestión Humana de dichas empresas, evitando espionaje industrial. Los resultados arrojados cumplen con los objetivos esperados, porque se han identificado ciertas recomendaciones para el perfeccionamiento de los procedimientos actuales, partiendo de los procesos que se cumplen en la actualidad en dichos departamentos y los que necesitarían ser reforzados buscando lograr una mejor acción de personal.

Descripción: El material contiene 6 capítulos, 108 páginas, 12 tablas y gráficos de los resultados del instrumento aplicado, y 6 gráficos en anexos.

Palabras claves: Espionaje industrial, seguridad informática, información, confidencialidad, eficiencia, robo de información.

Introducción

Introducción

En los últimos años la nueva tendencia en las organizaciones ha sido la de sistematizar los procedimientos simplificando las tareas, pero intentando ser cada vez más productivos. Es por esto que tanto las sociedades desarrolladas como las que se encuentran en vías de desarrollo, experimentan cambios en el manejo de las técnicas de gestión, debido a la aparición y desarrollo de nuevas tecnologías y los modernos estilos de liderazgo que permiten el desarrollo de los procesos de manera más eficiente. Todos estos cambios han ocasionado que la gestión del talento humano haya evolucionado con pasos agigantados en los últimos 40 años.

A pesar de que es infalible que toda empresa de telecomunicaciones otorgue un alto nivel de confiabilidad a sus empleados al momento de encomendarles funciones en su área de trabajo, lamentablemente, también es imprescindible que exista una iniciativa por parte de las empresas para lograr mayores avances y actualizaciones en lo que se refiere a las técnicas de gestión de los departamentos de Gestión Humana, buscando evitar casos de espionaje industrial y robo de información confidencial, hazañas que se han convertido en epidemia en los últimos tiempos, ya que las empresas de las telecomunicaciones de la República Dominicana compiten constantemente por posicionarse en la primera posición en dicho sector.

Por lo tanto, el propósito de esta investigación se basa en identificar el posible impacto que puede ocasionar la intervención que la Gestión de los Recursos Humanos con fines de aportar en evitar casos de espionaje industrial.

Para proponer recomendaciones acertadas ante esta problemática, se pretende profundizar en el tema exponiendo conocimientos básicos sobre el concepto de espionaje industrial y robo de información, se determinarán cuáles tipos de espionaje existen, detectar cuales mecanismos pueden ser necesarios para mantener la honestidad de los empleados, identificar las metodologías idóneas de evaluación de personal que existen en las empresas de las telecomunicaciones que miden la satisfacción del empleado basándose en su desempeño laboral.

De igual manera serán analizados los procedimientos que debe realizar un Departamento de Gestión Humana para el cumplimiento de los Deberes y Derechos de los empleados, y así valorar posibles consecuencias que se aplicarían en el Departamento de Gestión Humana ante casos de espionaje industrial. Serán presentadas informaciones de empresas famosas que han sido víctimas de espionaje industrial.

Este estudio investigativo arrojará posibles recomendaciones y aportes acertados que pueden ser identificados si la Gestión de los Recursos Humanos de las empresas de las telecomunicaciones en la República Dominicana se traza nuevos retos, aportando considerablemente desde el mejoramiento de los procedimientos en sus subsistemas, a reducir o eliminar por completo el interés de los empleados en realizar actos de espionaje industrial, hecho que se manifiesta como una conducta antisocial y que rompe con el compromiso que dichos empleados tienen para la empresa en que trabajan.

Serán enumeradas las grandes consecuencias que puede tener una empresa que es víctima de un delito por espionaje informático y robo de información, resaltando la importancia que tiene que en todo lugar de trabajo exista un clima laboral agradable y unas condiciones óptimas de trabajo, lo que permite que se produzcan menores riesgos de que un empleado se sienta disgustado con la organización y le sea desleal revelando datos confidenciales que pongan en riesgo la productividad colectiva.

CAPÍTULO I:

Planteamiento del problema

CAPÍTULO I: Planteamiento del Problema

Identificación del problema

En el sector de las telecomunicaciones del país, se pueden observar persistentes enfrentamientos legales entre las empresas que lo componen. Existe la probabilidad de que estas situaciones surjan por el interés de ellas en obtener la posición principal en el mercado, acaparando un mayor porcentaje de usuarios. La competencia desleal constante que surge en pleno siglo XXI en la República Dominicana, puede ser el motivo principal de casos de espionaje industrial en las empresas de las telecomunicaciones.

El desarrollo de la tecnología y las telecomunicaciones en la República Dominicana, ha incrementado considerablemente en los últimos años el interés de invertir en dicho sector, pero es necesario que cada empresa adopte las medidas necesarias para evitar el escape de información confidencial que pueda ser de utilidad para la competencia, ya que esto puede tener implicaciones legales y económicas graves.

De aumentar la frecuencia de esta problemática y no tomar las medidas regulatorias necesarias, cualquier empresa del sector en estudio en la República Dominicana, puede ser víctima de casos de espionaje industrial, por lo que es necesario que cada una de ellas identifique las debilidades en gestión que puedan tener dentro de las áreas más vulnerables para evitar situaciones que pongan en riesgo las posición en la que se destacan en el mercado nacional. Como una estrategia para precisar la problemática en estudio, se esgrimen las interrogantes que se detallan en el siguiente subtema:

Preguntas de investigación

1. ¿Cómo los Departamentos de Gestión Humana de las empresas de telecomunicaciones pueden identificar las debilidades que existen para evitar el escape de información?
2. ¿Cuáles medidas pueden ser tomadas en cuenta a fin de lograr mejoras dentro de los subsistemas de Gestión Humana para evitar que empleados desleales ingresen en la organización?
3. ¿Cuáles mecanismos pueden ser implementados para evaluar la honestidad de los empleados?
4. ¿Cómo se evalúa la satisfacción del empleado en las empresas de telecomunicaciones basándose en su desempeño laboral?
5. ¿Cuáles procedimientos realizan los Departamentos de Gestión Humana para el cumplimiento de los Deberes y Derechos de los empleados?
6. ¿Cuáles son los sistemas de consecuencias que aplican los Departamentos de Gestión Humana ante casos de espionaje industrial?
7. ¿Cómo es posible determinar la relevancia que puede tener la relación entre los Departamentos de Seguridad Informática y Gestión Humana, para participar en conjunto en la toma de decisiones y elaboración de procedimientos que eviten casos de espionaje industrial?

Características del estudio

La cualidad principal que distingue esta investigación y la diferencia de las demás investigaciones realizadas en base al Espionaje Industrial, es que la presente se sustenta de informaciones (tanto de fuentes primarias como secundarias), necesarias para sistematizar los resultados que se obtienen mediante el instrumento aplicado, y que sean estos resultados que arrojen los posibles desafíos a tomar en cuenta para mejoras en la Gestión del Talento Humano de las empresas que componen el sector de las telecomunicaciones de la República Dominicana.

Se propicia conseguir la obtención de los resultados de manera objetiva al:

- Verificar los datos obtenidos evitando sesgos en la investigación.
- Planificando previamente la organización del estudio.
- Estableciendo sinergias para cumplir con los objetivos planteados.
- Identificando las técnicas idóneas de recolección de la información.
- Ejecutando el análisis de los datos del informe final.

Justificación

El presente trabajo de investigación tiene como finalidad principal identificar los aportes más relevantes que pueden reforzar las empresas de las telecomunicaciones desde su Departamento de Gestión Humana para evitar el escape de información confidencial. El espionaje industrial puede provocar que cualquier empresa se favorezca de las fortalezas que tienen las diferentes compañías que componen el sector, al filtrar las informaciones que son de su interés para implementarlas de manera interna.

Se pretende identificar en la investigación la importancia de la autoevaluación constante de los Departamentos de Gestión Humana para verificar la eficiencia con la que se realizan todos los procesos que conciernen al manejo de personal, en busca de una mejor gestión. Serán planteadas las debilidades descubiertas desde el Departamento de Gestión Humana para analizar los subsistemas que pueden ser reforzados, y así evitar casos de espionaje industrial.

Los beneficiarios directos serán la totalidad de las empresas que componen el sector de las telecomunicaciones y los usuarios que reciben dicho servicio.

El estudio ofrece a la Universidad Nacional Pedro Henríquez Ureña un nuevo enfoque en la investigación acerca de la relación entre las TIC y Gestión Humana dando oportunidad a que las conclusiones y recomendaciones obtenidas sean un punto de partida a nuevas investigaciones en el área de seguridad empresarial.

De manera personal la investigación permite un amplio crecimiento profesional, ya que será posible conocer los mecanismos infalibles hasta el momento, que deben implementarse en cualquier empresa para la que se labore, con el fin de evitar el escape de información confidencial, y así el espionaje industrial.

CAPÍTULO II:

Marco conceptual

CAPÍTULO II: Marco conceptual

Conceptos

Para los fines del presente estudio se asumen los contenidos semánticos que se exponen en esta sección:

- **Espionaje industrial.** Se define como la actividad dedicada a obtener información fraudulenta en diversos campos, ya sea espionaje científico o industrial. (Diccionario Real Lengua Española. Año 2001).

  En términos de definición, ¨espionaje¨, es la acción de ¨espiar¨ significa acechar, vigilar cautelosa o disimuladamente lo que alguien hace o dice, ¨lo cual implica entonces, que el ¨espía¨ es el encargado de realizar esta acción.

- **Principio de subsidiariedad.** Describe un principio político y de ética social referente a establecer límites de competencia en las relaciones entre la persona humana y las sociedades de las que forma.

- **Contramedidas electrónicas.** Son acciones planificadas e implementadas con el objeto de proteger informaciones sensibles propias y neutralizar, detectar, localizar o perturbar las acciones de espionaje electrónico que se ejerzan sobre el objetivo.
- **Telecomunicaciones.** Es la transmisión y recepción de señales por medio de cualquier medio electromagnético. (Instituto Dominicano de las Telecomunicaciones. Mayo, 1998. Ley General de las Telecomunicaciones).
- **Competencia efectiva:** Es aquella que tiene lugar entre dos o más personas, físicas o jurídicas, a fin de servir una porción determinada del mercado mediante el mejoramiento de la oferta en calidad y precio, en beneficio del cliente o usuario.

- **Competencia leal.** Es aquella que se desarrolla sin incurrir en prácticas que actual o potencialmente distorsionen o restrinjan. Esas prácticas pueden ser predatorias o restrictivas de la competencia, o bien, desleales.
- **Competencia sostenible.** Es aquella que por sus características puede perdurar en el tiempo, pues se basa en condiciones propias de la prestación.
- **Posición dominante.** Es aquella condición en la que se encuentra una prestadora de telecomunicaciones que posee facilidades únicas o cuya duplicación sea antieconómica; o la condición en la que se encuentran ciertas prestadoras de servicios que tengan una situación monopólica en el mercado de un determinado servicio o producto de telecomunicaciones, suficientemente importante como para permitirles imponer su voluntad por falta de alternativa dentro del mercado de dicho producto o servicio, o cuando, sin ser la única prestadora de dicho servicio o producto, los mismos no son susceptibles de prestarse en un ambiente de competencia efectiva.
- **Prácticas desleales.** Es toda acción deliberada tendiente a perjudicar o eliminar a los competidores y/o confundir al usuario y/o procurarse una ventaja ilícita, tales como:

a) Publicidad engañosa o falsa destinada a impedir o limitar la libre competencia.

b) Promoción de productos y servicios en base a declaraciones falsas, concernientes a desventajas o riesgos de otros productos o servicios de los competidores; y

c) El soborno industrial, la violación de secretos industriales, la obtención de información sensible por medios no legítimos y la simulación de productos.

- **Autoevaluación**: Es la herramienta más práctica con que cuenta una dependencia o entidad para conocer los avances y las desviaciones de sus objetivos, planes y programas, sobre todo de la operatividad de aquellas acciones que se emprenden con la finalidad de mejorar la funcionalidad de los sistemas y procesos que regulan el quehacer de la propia entidad.

Corresponde a la revisión detallada y periódica del propio responsable de las acciones emprendidas para mejorar el funcionamiento de determinada área, unidad, órgano, sistema o procedimiento, a fin de medir el grado de eficiencia, eficacia y congruencia en su operación. (definición.org/autoevaluación, S/F, P).

- **Información**. Es un activo, que tal como otros es importante en una empresa o negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente. (ISO 17799, 2005).
- **Seguridad lógica**. Es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permita acceder a ellos a las personas autorizadas para hacerlo. (Borghello & Fabián, 2001).
- **Gestión de seguridad**. Es la coordinación e implementación de metodologías, políticas, técnicas, estrategias y procedimientos orientados a proteger un sistema informático, procurando preservar la integridad, disponibilidad y confidencialidad de la información procesada en un sistema de computadoras.
- **Activos de tecnología de información**. Son las infraestructuras físicas y lógicas, recursos humanos, servicios, documentación, datos y aplicaciones que forman parte del sistema tecnológico de una empresa o institución.
- **Modelo de autoevaluación de control interno**. Métodos o guías que permiten realizar evaluaciones propias sobre los controles y mecanismos de seguridad interna.
- **Seguridad de los activos de tecnología de información**. Hace referencia a asegurar tanto la información, aplicaciones y equipos informáticos dentro de la empresa.
- **Controles internos**. Mecanismos preventivos implementados de manera interna para proteger procesos y equipos.

Los objetivos que se plantean para el control interno son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Transmitir la información de forma que sea recibida solo por el destinatario al cual ha sido enviada y no a otro.
5. Recibir la información como ha sido transmitida.

- **Tics**: Se refiere a la abreviatura del término tecnologías de la información y comunicación.

CAPÍTULO III:

Marco teórico

CAPÍTULO III: Marco Teórico

Antecedentes

En el año 2002, el Instituto de Información Científica y Tecnología (INFO), en La Habana Cuba, publicó un documento que definía los conceptos de Inteligencia Competitiva y Operaciones de Contrainteligencia organizacional. La primera consiste en el servicio que prestan algunas empresas para legal y éticamente buscar información a partir de necesidades de otras organizaciones.

Según el INFO, (2000). La contrainteligencia emocional en cambio es una función gerencial que se expresa en un conjunto de actividades dirigidas y coordinadas, que tienen como propósitos detectar, identificar, disuadir, contrarrestar, neutralizar o revertir los esfuerzos de obtención de información de la Inteligencia Competitiva y del Espionaje Industrial y Económico hostiles a la organización.

La conclusión de la publicación del material resume que toda empresa debe asumir la necesidad de contar con un sistema de contrainteligencia organizacional ya que es un requisito fundamental para sobrevivir como organización en el entorno competitivo actual, y así cuidando las informaciones valiosas, percatándose tanto de la seguridad física, técnica, operacional, industrial, informática y económica financiera, como también la protección de personas que portan información y conocimientos sensibles de la organización.

Otra investigación, realizada en noviembre del año 2007 en la ciudad de México, con fines de obtener el título en la maestría de Ciencias y Administración de Negocios, presenta una propuesta de seguridad de la información, del caso Systematics de México, S.A., intentando evitar la inseguridad que existe en las propiedades básicas de la información (salvaguardar datos) para evitar robo de información en las terminales de punto final. Los resultados que arrojó el instrumento, donde se pretendían identificar los riesgos en los que se puede situar la empresa en este aspecto, dicen que los encuestados carecen de elementos necesarios respecto a cultura informática que les permita resguardar la información de la empresa.

La propuesta analizada de dicha investigación explica los siguientes elementos necesarios para solucionar la problemática:

1. Usar antivirus y actualizarlos.
2. No abrir correos de fuentes no conocidas.
3. Usar contraseñas difíciles de adivinar.
4. Usar firewalls para proteger la información de intrusos.
5. No compartir los accesos con desconocidos.
6. Desconectarse del internet cuando no lo utilice.
7. Respaldar los datos de la computadora.
8. Bajar regularmente actualizaciones o parches de seguridad.
9. Evaluar la seguridad de la computadora periódicamente.
10. Los empleados deben saber si su computadora resulta afectada o ha sido vulnerada.
11. Configurar de manera segura la instalación del sistema operativo.
12. Habilitar la opción para ver la extensión verdadera de los archivos.
13. Configuración segura de la instalación de Office.
14. Políticas de seguridad para minimizar riesgos en internet.

Contexto de las telecomunicaciones a nivel global.

De acuerdo con el Periódico El Deber. (Junio del 2013), fueron publicadas informaciones sobre Edward Snowden, quien divulgó la existencia de dos programas de espionaje secreto de la NSA (Agencia de Seguridad Nacional), que permiten consultar a diario registros de millones de llamadas telefónicas en EEUU y extraer información de servidores de gigantes de internet para espiar a sospechosos de terrorismo.

La ley SOX. (Sarbanes-Oxley), de EE.UU, nombrada así en referencia de sus creadores, obliga a las empresas públicas nacionales de dicho país, o extranjeras inscritas en la Securities and Exchange Comission al llevar un control y almacenamiento informático estricto de su actividad. La ley nace producto de grandes escándalos financieros ocurridos en compañías norteamericanas como Eron y Worldcom, durante el año 2002, en los cuales se comprobó qué información financiera fue falsificada. Esta ha tenido un alto impacto a nivel mundial en empresas que tranzan sus valores en la bolsa de EE.UU. (Burgos & Campos, S/F).

Contempla una revisión más rigurosa de los datos que una empresa declara en sus estados financieros-contables que utiliza para sus controles internos, y no solamente abarca fraudes por falsedad en dichas declaraciones, sino también por inferencia. Las multas por proveer información falsa o incorrecta son muy severas y pueden llegar al extremo de encarcelar a los ejecutivos de la empresa, o que ésta sea retirada de la Bolsa de Valores en que cotiza.

Una noticia publicada por el Periódico Listín Diario expresa la disculpa del Director de la CIA por espiar en el Senado de los EE.UU en el mes de agosto del 2014. Algunos empleados manifestaron se había violado el acuerdo hecho en el 2009 entre el Comité de Inteligencia del Senado y la CIA que habla sobre el acceso a la red de ordenadores conocida como RDINet, la cual está reservada únicamente para que el Comité de Inteligencia del Senado pudiesen revisar documentos de la CIA como parte de su pesquisa sobre la tortura por parte de la agencia de espionaje e inteligencia.

Ramírez, Egil Emilio y Aguilera, Ana Rosa para el año 2009, investigan acerca de los delitos informáticos y su tratamiento internacional, obteniendo las siguientes informaciones:

- En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE), que está compuesta por 34 estados (Alemania, Australia, Austria, Bélgica, Canadá, Chile, Corea, Dinamarca, España, Estados Unidos, Eslovenia, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Israel, Italia, Japón, Luxemburgo, México, Noruega, Nueva Zelanda, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Suecia, Suiza y Turquía), y se considera como una organización de cooperación internacional, inició un estudio sobre la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

- En 1986, la (OCDE*)* publica un informe titulado Delitos de Informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.
- Para el 1992, la OCDE elabora un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.
- En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el Principio de Subsidiariedad.
- Hay otros Convenios realizados por la Organización Mundial de la Propiedad Intelectual (OMPI). En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como:

- Aplicaciones en la Administración de las Tecnologías Informáticas / cibernéticas.
- Blanqueo de capitales, contrabando y narcotráfico.
- Hacia una policía Europea en la Persecución del Delito Cibernético.
- Internet: a la búsqueda de un entorno seguro.
- Marco legal y Deontológico de la Informática.

Liliana (2012), en su investigación publicada sobre el tratamiento internacional de los delitos informáticos, explica que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial.

De ello surge la necesidad de adoptar medidas legislativas. En los Estados Industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años. Los Estados miembros de la Unión Europea acordaron castigar con penas de uno a tres años de prisión a los responsables de delitos informáticos.

Cuando quede comprobado que los ataques cibernéticos están relacionados con el crimen organizado, la pena ascenderá hasta los cinco años. Esta decisión se convierte en un gran avance dentro de la armonización de las legislaciones europeas para luchar contra los delitos informáticos.

Estos delitos se han convertido en un quebradero de cabeza para los cuerpos de policía de los Estados miembros y, sobre todo, para los perjudicados por estos crímenes. El principio de territorialidad del derecho provoca que sea muy complicado perseguir a delincuentes informáticos que actúan desde otros países. Con este intento de unificar la legislación, las autoridades europeas podrán perseguir con una mayor efectividad a delincuentes que hasta ahora, podían cometer sus delitos con casi total impunidad. Además, el acuerdo del Consejo de Ministros de Justicia de los Quince Estados Europeos establece otro aspecto importante, como es la definición de los delitos que se consideran informáticos.

Según Liliana en su investigación ya citada, los Estados miembros distinguen tres tipos de ataques cibernéticos:

- El acceso ilegal a sistemas informáticos.
- La ocupación de sistemas a través de ejemplos como el envío de mensajes que ocupan un espacio considerable.
- La difusión de virus informáticos.

Finalmente, se expresa la intención de que la Unión Europea es doble: por un lado se trata de definir al delito; por otro pretende unificar las penas, ya que el lugar de la comisión del delito es fundamental para saber el derecho aplicable, se trata además de una medida muy sensata que evita la desprotección absoluta que presentan hoy en día las empresas del Viejo Continente. Los Quince Estados Europeos disponen ahora de un plazo de más de dos años para la adaptación de esta medida a sus textos legislativos.

A medida de conclusión, la investigación explica que pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países.

A diferencia de las investigaciones que han sido encontradas con respecto a lo que concierne al estudio del espionaje industrial, la presente investigación pretende ofrecer posibles aportes desde los Departamentos de Gestión Humana de las empresas de las telecomunicaciones de la República Dominicana, identificando las necesidades que deben mejorarse en dichos Departamentos para evitar ser víctima de espionaje industrial.

Contexto de las telecomunicaciones en la República Dominicana

En la República Dominicana, para el 27 de mayo del 1998, surge la Ley General de las Telecomunicaciones No. 153-98, la cual constituye uno de los instrumentos jurídicos más importantes en el ámbito del derecho de la competencia y regulación de los mercados, de manera particular de las telecomunicaciones. El surgimiento de dicha ley es coherente con el Art.- 147 de la Constitución Dominicana, sobre la finalidad de los servicios públicos. Esta expresa que estos servicios están destinados a satisfacer las necesidades de interés colectivo. Serán declarados por ley. (Instituto Dominicano de las Telecomunicaciones.1998. Ley General de las Telecomunicaciones).

En Consecuencia:

1) El Estado garantiza el acceso a servicios públicos de calidad, directamente o por delegación, mediante concesión, autorización, asociación en participación, transferencia de la propiedad accionaria u otra modalidad contractual, de conformidad con esta Constitución y la ley;
2) Los servicios públicos prestados por el Estado o por los particulares, en las modalidades legales o contractuales, deben responder a los principios de universalidad, accesibilidad, eficiencia, transparencia, responsabilidad, continuidad, calidad, razonabilidad y equidad tarifaria;
3) La regulación de los servicios públicos es facultad exclusiva del Estado. La ley podrá establecer que la regulación de estos servicios y de otras actividades económicas se encuentre a cargo de organismos creados para tales fines.

Según el Ex Presidente del Consejo Directivo del INDOTEL Orlando Jorge Mera, el desarrollo de las telecomunicaciones en la República Dominicana necesitaba de la existencia del marco legal propicio para incentivar la competencia en uno de los sectores más pujantes de la economía dominicana. En efecto, dicha ley estableció el organismo regulador de las telecomunicaciones bajo el fundamento de que el mismo debe ser guardián del dominio público del Estado dominicano, propietario del espectro radioeléctrico; promotor del Fondo de Desarrollo de las Telecomunicaciones; y defensor de los derechos y deberes de los usuarios de los servicios públicos de telecomunicaciones.

Existe en el país la ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, aprobada por el Consejo Directivo del Instituto Dominicano de las Telecomunicaciones (INDOTEL), gracias a la resolución no. 086-11. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o orales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos. (Ley No. 53-07 Sobre Crímenes y Delitos de Alta Tecnología).

En otro orden, según la Oficina Nacional de la Propiedad Industrial (ONAPI), en el año 2000, la República Dominicana adecua su legislación de Propiedad Intelectual al Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC). Como consecuencia de lo anterior, el 8 de mayo del año 2000.

Se crea la Ley 20-00 sobre Propiedad Industrial, derogando la Ley 4994 sobre Patentes de Invención del año 1911, y la 1450 sobre Marcas de Fábricas del año 1993, la cual establece la Oficina Nacional de la Propiedad Industrial *(*ONAPI*)* como organismo rector, responsable de otorgar los derechos exclusivos sobre las distintas modalidades de Propiedad Industrial.

Según las publicaciones de OPTIC (Oficina Presidencial de Tecnologías de la Información y Comunicación), en el año 2004 se identificó la necesidad de contar con un organismo de alto nivel gubernamental, debido a la prioridad y el firme propósito del Gobierno Dominicano en articular iniciativas sectoriales en el sentido de masificar en el país el uso de las tecnologías de la información y comunicación (TIC), buscando modernizar al Estado, aumentar la competitividad del sector productivo y socializar el acceso a la información.

Siendo de interés muy particular el fomentar, desarrollar y diseñar proyectos, políticas y estrategias que tiendan a democratizar el uso, acceso y aplicación de las tecnologías de la información y comunicación (TIC) y reducir la marcada brecha digital, que consiste en la diferencia de acceso al conocimiento, a la información y a las tecnologías de la información y comunicación (TIC) entre personas con mayores oportunidades y aquellas que están desprovistas de medios y recursos para subsistir.

A raíz de esto, se proyectó la creación de un organismo encargado de coordinar las iniciativas y proyectos de desarrollo, amparado en las tecnologías de información y comunicación (TIC) de manera armónica y articulada acorde a los planes generales y estratégicos trazados por el Poder Ejecutivo, de crear el ambiente necesario para la competitividad, eficientizar y transparentar el desempeño de la Administración Pública, así como de invertir en las áreas que propicien la participación de toda la ciudadanía.

Sumado al interés como país de cumplir con los acuerdos suscritos con las Naciones Unidas para alcanzar los Objetivos del Milenio y erradicar la pobreza, y dar cumplimiento a acuerdos tales como la Declaración de Bávaro, la Declaración de Principios y el Plan de Acción de la Cumbre Mundial para la Sociedad de la Información en su primera fase, en Ginebra, diciembre 2003, y en su segunda fase el Compromiso y Programa de Acción celebrado en Túnez, noviembre 2005.

Precisamente estas necesidades motivaron que el día 3 de Septiembre de 2004, mediante Decreto No. 1090-04, fuera creada la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), con dependencia directa del Poder Ejecutivo, autonomía financiera, estructural y funcional.

En el mismo orden este decreto adhiere a la OPTIC, las funciones del instituto Audiovisual de Informática (IADI), en la actualidad denominado Centro de Estudios de Tecnologías de la Información y Comunicación (CETIC) y de la Comisión Nacional de Informática (CNI), con la finalidad de integrar bajo un mismo seno las iniciativas de Tecnologías de la Información y Comunicación (TIC) y Gobierno Electrónico.

Además, mediante Decreto No. 212-05, se crea la Comisión Nacional de la Sociedad de la Información y Conocimiento (CNSIC), con la responsabilidad de elaborar, desarrollar y evaluar la Estrategia Nacional de la Sociedad de la Información, la formulación de políticas derivadas de dicha estrategia y la definición de iniciativas, programas y proyectos para su realización.

Otros Decretos han sido emitidos, No. 228-07 y No. 229-07, con miras a institucionalizar el desarrollo e implementación de la Agenda Nacional de Gobierno Electrónico. Estos Decretos establecen el Centro de Contacto Gubernamental y el instructivo de aplicación de Gobierno Electrónico respectivamente.

El Periódico Hoy, en la República Dominicana para julio del 2013, cita que en la República Dominicana más del 58% de los entrevistados en la encuesta realizada para Pulso Dominicano opinaron que el Gobierno debe siempre respetar la privacidad de las personas, al 36.6% le parece aceptable solo en los casos en que la Seguridad Nacional dependa de ello y el 5.2% considera que el Estado siempre tiene derecho a vigilar las comunicaciones de los ciudadanos. Independientemente de la opinión de la gente, esa es una misión constitucional del Estado (ver gráfico 1.1 en anexos).

Concordante con estos puntos de vista, una mayoría de casi tres a dos considera incorrecto que el Gobierno acceda a secretos de los ciudadanos. “Es incorrecto”, escogió el 56.8%; “es correcto, pero solo en casos extremos”, respondió el 36.8%”; “es correcto”, respondió el 10.4%.(ver gráfico 1.2 en anexos).

Al pedir la opinión de los entrevistados sobre una persona que revela secretos de su Gobierno, la opinión pública se muestra dividida. “No es un traidor si actúa para defender los derechos de los ciudadanos”, según el 46.1 por ciento; “es un traidor”, respondió el 44.6 por ciento; el porcentaje restante (9.2 por ciento) estuvo dividido en posiciones minoritarias. (ver gráfico 1.3 en anexos).

La Constitución de la República Dominicana, expresa en el **Art.- 70** el término Habeas Data. Este indica que toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística.

De acuerdo con las legislaciones existentes en la República Dominicana El Código de Trabajo de la también señala ciertos artículos que sustentan y relacionan legalmente en el país el tema a investigar, dentro de los que se destacan:

Art. 44. Considera como obligación de los trabajadores:

> 6º. Observar buena conducta y una estricta disciplina durante las horas de trabajo.
>
> 7º. Guardar rigurosamente los secretos técnicos, comerciales o de fabricación de los productos a cuya elaboración concurran directa o indirectamente, o de los cuales tengan conocimiento por razón de trabajo que ejecuten, así como de los asuntos administrativos reservados cuya divulgación pueda causar perjuicio al empleador, tanto mientras dure el contrato de trabajo como después de su terminación.

Muestra en el **Art. 45.-** Está prohibido a los trabajadores:

> 4º. Usar útiles y herramientas suministradas por el empleador en trabajo distinto de aquel que esté destinado, o usar los útiles y herramientas del empleador sin su autorización.
>
> 5º. Extraer de la fábrica, taller o establecimiento útiles de trabajo, materia prima o elaborada sin permiso del empleador.

Según el Capítulo V, acerca de la terminación del despido del trabajador, se presenta en el **Art. 88:** que el empleador puede dar por terminado el contrato de trabajo despidiendo al trabajador por cualquiera de las causas siguientes:

1º. Haber inducido a error al empleador pretendiendo tener condiciones o conocimientos indispensables que no posee, o presentándole referencias o certificados personales cuya falsedad se comprueba luego.

3º. Incurrir durante sus labores en falta de probidad o de honradez, en actos o intentos de violencias, injurias o malos tratamientos contra el empleador o los parientes de éste bajo su dependencia.

7º. Ocasionar perjuicios graves sin intención, pero con negligencia o imprudencia de tal naturaleza que sean la causa del perjuicio.

8º. Cometer actos deshonestos en el taller, establecimiento o lugar de trabajo.

9º. Revelar los secretos de fabricación o dar a conocer asuntos de carácter reservado en perjuicio de la empresa.

10º. Comprometer, por imprudencia o descuido inexcusable, la seguridad del taller, oficina u otro centro de la empresa o de personas que allí se encuentren.

En caso de incumplimiento a estas disposiciones, el Código de Trabajo Dominicano contempla, que:

Art. 424.- El Departamento de Trabajo investigará las denuncias de irregularidades en la ejecución de los contratos, convenios, leyes y reglamentos de trabajo que le sean sometidas por los empleadores y por los trabajadores perjudicados. La investigación se hará dentro de un plazo de tres días después de la presentación de la denuncia.

El Código de Trabajo Dominicano vigente, consagra el procedimiento ante los tribunales de trabajo en los Conflictos Jurídicos, procedimientos de juicio, producción y discusión de las pruebas (que constan de pruebas escritas, testimonios, inspecciones, informes periciales, confesiones y del juramento).

El impacto de las telecomunicaciones en la economía nacional.

El sector de las telecomunicaciones es, dentro de los servicios, uno de los de mayor contribución al Producto Interno Bruto (PIB) de la nación. En el año 2013 tuvo un crecimiento de 4.5%, según las cifras preliminares del Banco Central de la República Dominicana.

Esta contribución al PIB está relacionada con las grandes inversiones que realizan las concesionarias de servicios de telecomunicaciones, motivadas principalmente, por la ampliación de su nivel de cobertura y la renovación tecnológica de sus redes para mejorar la calidad del servicio brindado y ampliar su oferta de productos.

Finalmente, el INDOTEL afirma según las publicaciones del Banco Mundial, que la experiencia internacional ha mostrado que un incremento en la penetración de la telefonía móvil del 10% conlleva a un crecimiento del Producto Interno Bruto de un 0.50%; y que un incremento del 10% en el servicio de banda ancha representa un aumento de 1.3% en el PIB, lo cual se traduce en una mejor calidad de vida de la población. El reto, entonces, es propiciar que el uso al Internet se traduzca en un incremento de la productividad de los individuos y las empresas, para que de ese modo, aporte al crecimiento de la economía.

Tipos de Espionaje Industrial

- **Espionaje electrónico:** Marco Francisco y Escamilla, David. (2008). Explican que este tipo de espionaje se realiza mediante equipos llamados en inteligencia medidas electrónicas, dispositivos con capacidad para captar informaciones de audibles, visuales o ambas para monitorearlas o grabarlas y enviarlas por un determinado canal discretamente hacia otro punto.

- **Robo interno**: Según Francisco Marco en el libro ¨***El Control en la Empresa***¨**,** el robo interno constituye un 50% de los tipos de robos existentes. El empresario gasta una cantidad económica ingente para paliar el hurto externo mediante cámaras de video y personal de seguridad (correspondiente al 30% de la perdida de información), y realiza auditorías internas y externas para paliar el 20% que corresponde a los errores administrativos (ver gráfico 1.5 en anexos).

  Sin embargo, dicho empresario evita gastar en evitar el hurto interno. Evitándose en gran parte con un buen pre laboral e investigación previa sobre la empresa que se subcontrata.

  Francisco Marco cita, que los empleados que hurtan son:

  a. Un 40% los contratados, y un 10% los subcontratados.
  b. Los no identificados e involucrados en la empresa.
  c. Los que temen ser destituidos o sustituidos.
  d. Los endeudados.
  e. Los que tienen antecedentes de haber realizado lo mismo.
  f. Los descontentos con su trabajo.
  g. Los mal remunerados.

- **Errores administrativos**
- **Hurtos externos: personas externas.**

Experiencias de empresas víctimas de espionaje industrial

Marco Francisco y Escamilla, David. (2008), además muestran las siguientes empresas victimas de espionaje industrial:

1. **Vidal Sasoon y su Wash and Go: la imitación de productos.**

A mediados de los 80, Procter & Gamble lanza al mercado junto a Richardson-Vicks, el primer champú dos en uno, o champú más acondicionador, Wash and Go de Vidal Sasoon. Por ello se juzgó que debía considerarse competencia desleal la imitación de prestaciones de un tercero cuando resultara idónea para generar la asociación por parte de los consumidores.

2. **Juan López** prestaba sus servicios en Aseguradora España, S.A. como jefe superior, director de sucursal, por quejas continuas de que el Sr. López no atendía su puesto de trabajo, se le contrató una agencia de detectives y a través del informe se comprobó que atendía una correduría de seguros de su mujer e hijos.

En 1989, la empresa industrial de Alta Tecnología Martínez, (IATMSA), contrata a una persona como Director Comercial, la empresa luego de un tiempo ve como la competencia gana siempre los concursos en los que se enfrentan y capta a los clientes que IATMSA pierde.

En 1996 la persona renuncia y con él se marchan dos Directores Técnicos, dos comerciales y una secretaria. La persona crea su empresa Industrial de alta tecnología López, S.A. (IATLSA). A partir de ahí se desencadena una batalla y Martínez tiene un descenso en 1997 de un 30% para recuperarlo en 1998, cuando López cierra su empresa por una nefasta Gestión Financiera.

Martínez se entera de que López ya lo había hecho antes y que en la empresa de la competencia que le ganaba en todos los concursos, estaba el cuñado de López.

3. **Banco de Fomento contra Bandesco:**

Fomento formuló demanda de juicio declarativo contra Bandesco al considerar que tres ex empleados del banco actor, haciendo uso del listado de sus clientes de su antigua empresa obtenían la captación de su pasivo para Bandesco.

4. **Coca Cola y Pepsi**: En 2006, Pepsi pudo desmantelar una trama integrada por tres individuos que intentaban vender documentos confidenciales y una muestra de un producto secreto desarrollado por su eterna rival Coca-Cola. Los implicados eran la asistente administrativa de un alto ejecutivo de la marca y otros dos individuos.

5. **Compañía aérea Boeing:** En el 2000 el Departamento de Justicia y el Pentágono investigaron a Boeing por una presunta irregularidad que sirvió para ganar un contrato de 2,000 millones de dólares para fabricar cohetes lanzadores de satélites militares, ya que Kenneth Branch fue contratado en 1997, y era miembro antes de la empresa rival de Boeing (Lockheed Martin).

6. **Súper López:** en 1993 Súper López fue contratado por Volkswagen tras una prestigiosa trayectoria en General Motors, abandonándola junto con seis ejecutivos más. General Motors acusa ante un juzgado de Detroit a Volkswagen y a Super López de Espionaje Industrial y de llevarse de forma masiva y sistemática a directivos de General Motors.
7. **Toyota contra Hyundai:** Un Ingeniero en Toyota fue contratado por Hyundai, proyectaba informaciones y exposiciones informativas en las que figuraba el logo de su anterior empleo. Unos subordinados denunciaron el caso de forma anónima a la Toyota. El empleado fue despedido y los documentos fueron devueltos a la Toyota**.**

8. **Hacking:** en el 2006 una veintena de ejecutivos y directivos de compañías claves de Israel fueron detenidos y acusados de espionaje industrial mediante el uso de software espía introducido en los ordenadores de sus competidores; ejemplos de esto han sido: directivos del canal de televisión por satélite YES, por haber espiado el canal HOT, compañías de teléfono Pelephone y Cellcom por haber espiado a Partner, Mayer encargada de exportar a Israel vehículos Volvo y Honda por espiar a Champion Motors, exportadores de Audi y Volkswagen.
9. **Caso HP**: En 2006, la empresa veía como luego de las reuniones del consejo, se filtraban secretos a la prensa. Luego de haber contratado la presidenta una agencia de detectives Security Solutions para detectar el origen de la filtración, se detectó que uno de los consejeros otorgaba información valiosa a la prensa.
10. **Alhambra contra Heineken España.** En julio del 2001, se hizo una querella de Alhambra contra Heineken y un detective privado por allanamiento de sede industrial, descubrimiento y revelación de secretos.
11. **Kodak:** Harold Worden fue declarado culpable en 1997 de robar información secreta sobre un modelo de máquina fotográfica (el 401). Cuando se retiró se llevó documentos. Ofertó la información a AGFA y Konica.
12. **Gillette:** Steven Davis fue condenado en Tennessee el 3 de octubre de 1997 por cinco cargos de fraude y espionaje industrial al facilitar a terceros los prototipos de las nuevas máquinas de afeitar de Gillette (a Lambert, Bic y American Safety Razor Co).
13. **Avery Dennison:** (de los mayores fabricantes estadounidenses de productos adhesivos) Pin Yen Yang y su hija fueron arrestados el 5 de septiembre de 1997 en Cleveland, acusados de fraude de correos, lavado de capitales, espionaje industrial y receptación al conocerse mediante una investigación previa, que estaban pagando a un empleado de Avery por secretos industriales.

Los casos expuestos constituyen argumentos justificativos de que el espionaje es una realidad y desafío para toda empresa. Por lo expuesto se justifica adoptar políticas y recursos para resguardar sus activos tangibles e intangibles.

Seguridad Informática

Es la condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos establecidos para el correcto manejo y control de la información, en todo su ciclo de vida, así como para prevenir y detectar posibles comprometimientos de la misma que puedan afectar a su confidencialidad integridad o disponibilidad. Por manejo de la información se entenderá el almacenamiento, custodia, elaboración o proceso.

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**. Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad**. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

  ¿Qué debemos proteger?:

  1. Información almacenada en computadoras.
  2. Transmitida en medios electrónicos.
  3. Impresa o escrita en papel.
  4. Enviada por fax.
  5. Almacenada en notebooks.
  6. Hablada en conversaciones.

Muchos de los activos de tecnología de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse de gestiones y procedimientos adecuados. La identificación de los controles requiere una planificación cuidadosa y una atención al detalle.

El marco integrado de control interno del ¨Informe COSO¨, (1992*),* consta de cinco componentes interrelacionados, derivados del estilo de la dirección e integrados al proceso de gestión:

1. Ambiente de control.
2. Evaluación de riesgos.
3. Actividades de control.
4. Información y Comunicación.
5. Supervisión.

Beneficios del control interno

- Ayudar a los directivos al logro razonable de las metas y objetivos institucionales.
- Integrar e involucrar al personal con los objetivos de control.
- Ayudar al personal a medir su desempeño y por ende, a mejorarlo.
- Contribuir a evitar el fraude.
- Facilitar a los directivos la información de cómo se han aplicado los recursos y cómo se han alcanzado los objetivos.
- Apoyar el cambio en la cultura hacia el servicio, y facilitar la introducción de un sistema de administración de calidad.

Norma ISO- 17799.

Es un estándar para la administración de la seguridad de la información, e implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la ***International Organization for Standarization (ISO)*** en diciembre del 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajan las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

La norma ISO / IEC 17799 es redactada y publicada en dos partes:

1) **ISO / IEC 17799 Parte I:** Es una guía de recomendaciones de buenas prácticas para le gestión de la seguridad de la información. Contiene consejos y recomendaciones que permite garantizar la seguridad de la información de la organización, además cubre otras áreas y funciones que puedan afectar dicha información.
2) **BS 17799 Parte II:** Contiene la guía relativa para la implementación de un sistema de gestión de la seguridad de la información que propone recomendaciones con el fin de establecer un marco para la gestión de la información denominada ***Information Security Management System (ISMS).***

El objetivo de la norma, es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

ISO Serie 27000.

A semejanza de otras normas ISO, la 27000 es una serie de estándares que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información, (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoría y certificación de SGSI (ISO 27006), una guía de auditoría de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 270011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de ciber-seguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034),
y una guía de seguridad de la información en el sector sanitario (ISO 27799). (Burgos & Campos, S/F).

Norma ISO 27001.

Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

Es una norma redactada por los mejores especialistas del mundo en el campo de la seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. Se basa en los siguientes controles:

- **Política de seguridad.** Es necesario reflejar las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte.
- **Organización de la seguridad.** Permite establecer la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuestas a incidentes. Esta parte detalla cómo se debe administrar la seguridad de la información dentro de la compañía, como también mantener la seguridad de las instalaciones de procesamiento de información y los activos informáticos accedidos por terceros (proveedores, clientes, etc).
- **Control y clasificación de los recursos informáticos.** Detalla los elementos de la compañía (servidores, PCs, medios magnéticos, información impresa, documentos, etc), que deben ser considerados para establecer un mecanismo de seguridad, manteniendo una protección adecuada, garantizando que reciban un nivel adecuado de protección.

En ese sentido, los activos deben clasificarse en: confidenciales, privados, de uso interno y uso público. Para cada clasificación se deben implantar los mecanismos adecuados de seguridad de acuerdo a su importancia.

- **Seguridad del personal.** Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan.

También determina cómo incide el papel que desempeñan los empleados como corresponsables de la seguridad de la información. Se busca minimizar los riesgos ocasionados por el personal, tales como hurto y manipulación de la información, fraudes y mal uso de la plataforma tecnológica.

Tiene como propósito crear conciencia en los usuarios sobre los riesgos que pueden amenazar la información, para lo cual considera mecanismos y medios para información y capacitar periódicamente a todos los usuarios (personal interno de la compañía y personal que brinde servicios) de todas las políticas, y establecer mecanismos de prevención, identificación, notificación y corrección de posibles incidentes de seguridad.

- **Seguridad física y ambiental.** Responde a la necesidad de proteger las áreas, los equipos y los controles. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la compañía, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputos, PC de usuarios críticos, equipos de los proveedores de servicios, etc), y áreas en las cuales se recibe o se almacena información (magnética o impresa), sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc).

Esto permite minimizar los riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.

- **Manejo de las comunicaciones y operaciones.** Define las políticas y procedimientos para asegurar la correcta operación de las instalaciones de procesamiento (servidores y equipos de comunicación). Los objetivos de esta sección se pueden enumerar como sigue:
    - Asegurar la protección y el funcionamiento correcto de las instalaciones de procesamiento de información.
    - Minimizar la integridad del software y la información.
    - Conservar la integridad y disponibilidad del procesamiento y transmisión de la información.

    - Garantizar la protección de la información en las redes y de la infraestructura de soporte.
    - Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- **Control de acceso.** Establecer la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, internet, comunicaciones, conexiones remotas, etc) que requiere cada empleado de la compañía y el personal externo que brinda servicios, en concordancia con sus responsabilidades.
- **Desarrollo y mantenimiento de los sistemas.**
- **Manejo de la continuidad del negocio.**
- **Cumplimiento**. Verifica si el cumplimiento de la norma 27001 concuerda con las leyes, reglamentos, obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contratos de servicios, etc.

Requiere una revisión a las políticas de seguridad, al cumplimiento y las consideraciones técnicas; busca garantizar que las políticas de seguridad sean acorde a la infraestructura tecnológica de la compañía.

Son publicadas ciertas recomendaciones para organizar el Departamento de Gestión Humana, donde Sulbarán, Eliezer (2011), dice que asimismo, hay que acompañar al personal de servicio con agentes de seguridad para que los supervisen en cuanto a las labores que desempeñan.

Resguardo de la información digital

La información digital siempre tiene que estar a buen resguardo. De acuerdo con Eleazar Sulbarán, la empresa debe disponer de un Departamento de Informática para que no existan fugas de información y que esto fomente la competencia desleal.

Existen formas con la finalidad de impedir esta clase de cosas. Una de ellas cita Sulbarán, es haciendo una campaña interna de carácter informativo para que los usuarios de cada computadora coloquen claves de acceso al sistema operativo, con la finalidad de asegurarlas ante la posibilidad de que algún agente externo pueda sustraer alguna clase de información. Además de la protección técnica de aquellos datos guardados en una computadora es necesario desarrollar un programa de capacitación en cuestiones de seguridad para los empleados.

Según Keith Blogg, en su publicación acerca del Espionaje Corporativo, todas estas son buenas pautas a seguir por todo tipo de compañía, sea pequeña o mediana, ya que son las personas menos pensadas las que puedan estar recolectando información sobre las actividades y los planes de su compañía más allá de límites insospechados.

Cecilia Moya brinda al público lector una publicación sobre cómo prevenir el espionaje industrial, dice que la mayoría de comunicaciones se realizan hoy en día de forma informática por lo que es necesario, casi imprescindible, disponer de programas específicos de protección (antispyware, antivirus, firewall) actualizados de forma constante.

También recomienda:

- El cambio de contraseñas y un protocolo de permisos de acceso a los diferentes niveles de información evitan en muchas ocasiones males mayores.
- La solución del reciclaje de papel.

- Realizar auditorías de seguridad de manera constante.
- Prohibición del uso de memorias USB.

La información adopta diversas formas, puede estar impresa, o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación, por lo tanto, debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

Cómo proteger la información personal en los negocios

Marco Francisco, y Escamilla David, (2008). Expresan en su libro sobre el control en la empresa, que los empleadores y managers deben tomar una serie de precauciones y medidas para asegurarse de que en sus oficinas todo procede tal y como ellos mismos han estipulado en sus estatutos internos, esto puede realizarse mediante:

- **La investigación previa de los empleados:** saber identificar currículos falsos, especialmente aquellos que provienen de empresas de trabajo temporal (ETT).

Un estudio de la ***Society for Human Resource Management*** determina que en EE.UU. el 53% de los currículos falseaba la temporalidad de los trabajos previos, el 51% el último salario y en el 45% no se incluían antecedentes penales.

En España la agencia de detectives española, Método 3, demuestra en el libro El Control en la Empresa (ver gráfico 1.4), que:

1. El 82% de currículos tiene algún dato falso.
2. En el 62% se miente sobre el salario anterior.
3. En el 54% no se indica un trabajo, por lo que se altera la temporalidad de los trabajos anteriores y posteriores.
4. En el 11% hay antecedentes penales o policiales.
5. En el 17% hay un historial empresarial propio negativo.
6. En el 4% el aspirante está en busca y captura.
7. El 1.1% trabaja para la competencia y es un topo.

La página web de la empresa ***Delta detectives*** **y** ***Securitas***, muestra las soluciones que estos proporcionan para controlar y detectar estás fugas tan perniciosas para las empresas. Aplicando el análisis de fuga de capital (AFC) se determinan los puntos vulnerables de la empresa y los procesos de investigación que se realizarán, tales como infiltración en grupos de empleados sospechosos, vigilancias especiales, seguimiento a ejecutivos de alta jerarquía, depuraciones laborales, auditorías encubiertas, control de rutas, chequeos de ventas, entre otros.

- **Mantener el control de los visitantes en la empresa**

Sulbarán, Eleazar. (2011), explica en su publicación, que los visitantes no solo pueden ser personas esperadas, invitadas o deseadas en la empresa. Pero es probable que aquellas compañías que provean algún servicio, sean utilizadas por otras corporaciones para infiltrar a la empresa electrónica o físicamente.

Estos pueden ser herreros, fontaneros, carpinteros, electricistas que a modo de estar realizando un trabajo dentro de la empresa, según Sulbarán, se puede colocar algún dispositivo electrónico para captar audio o video, de tal forma que puedan obtener información. También pueden sustraer documentos importantes. Todo esto lo hacen mientras nadie los esté observando.

Finalmente, Sulbarán concluye que para evitar estas situaciones, hay que realizar a todas las personas que ingresan a las instalaciones de la empresa un registro físico de todas sus pertenencias, como una manera de cerciorarse que entren con lo que realmente necesiten para trabajar.

Rueda, Fernando (2011). Muestra que las negociaciones empresariales cuando el malo es descubierto, se solucionan en el 80% de las negociaciones de una manera más o menos amistosa: cita “Por eso muy pocos casos llegan a los tribunales, dando la sensación de que el problema no existe, porque las empresas son negocios y todo se traduce en dinero”.

Una vez confirmada la traición, normalmente se convoca por sorpresa a una reunión al empleado. Sin la presencia de abogados, se le explica por parte de los directivos de la empresa, acompañados de los investigadores, que ha estado robando información y quieren que se vaya inmediatamente. Si el empleado lo niega, lo que suele ser habitual, se le muestra en una televisión y con una casete las pruebas que le incriminan. El empleado, ante la constatación de su delito, prefiere renunciar al dinero que le correspondería por el despido y evitar ir a la cárcel.

CAPÍTULO IV:

Delimitación de la investigación

CAPÍTULO IV: Delimitación de la investigación

Propósito del estudio

Se pretenden identificar durante el periodo de mayo-septiembre del 2014, los cambios que deben generarse desde los Departamentos de Gestión Humana para evitar casos de espionaje industrial, realizando un análisis de la problemática actual en el sector de las telecomunicaciones de la República Dominicana, y obteniendo resultados para ulteriores sugerencias mediante el estudio de la presente investigación y anteriores relacionadas al tema.

Objetivos

Objetivo General: Identificar desafíos de los departamentos de Gestión Humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial, en la R.D.

Objetivos Específicos

1. Indicar las debilidades que pueden tener los Departamentos de Gestión Humana de las empresas de telecomunicaciones para evitar casos de espionaje industrial.
2. Determinar las medidas a ser tomadas en cuenta con fin de lograr mejoras dentro de los subsistemas de Gestión Humana para evitar que empleados desleales ingresen en la organización.
3. Detectar los mecanismos necesarios para evaluar la honestidad de los empleados.
4. Identificar las metodologías de evaluación de personal existentes en las empresas que midan la satisfacción del empleado basándose en su desempeño laboral.
5. Analizar cuáles son los procedimientos eficaces que pueden realizar los Departamentos de Gestión Humana para el cumplimiento de los Deberes y Derechos de los empleados.
6. Valorar posibles sistemas de consecuencias que se aplicarían en los Departamentos de Gestión Humana ante casos de espionaje industrial.
7. Determinar la relevancia del trabajo coordinado entre Seguridad Informática y Gestión Humana, para participar en conjunto en la toma de decisiones y elaboración de procedimientos que eviten casos de espionaje industrial.

CAPÍTULO V:

Métodos y materiales

CAPÍTULO V: Métodos y materiales

Tipo de investigación

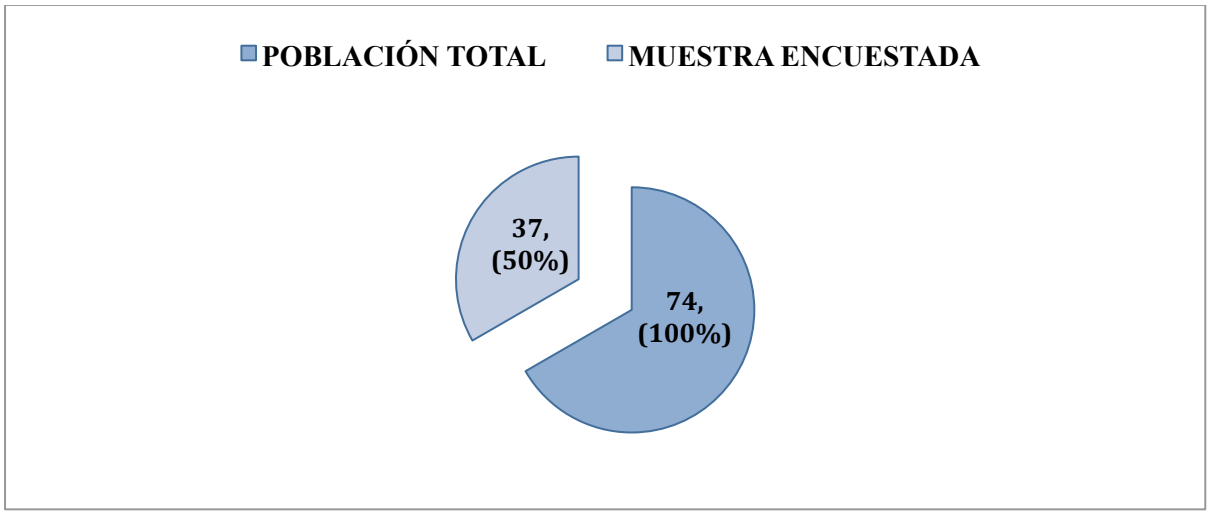
El tipo de investigación es de carácter evaluativa, descriptiva-bibliográfica, y confirmatoria; por validación empírica. Según Hurtado de Barrera, Jacqueline (2002). La investigación evaluativa conforme a la ob cit, es aquella que: ¨tiene el objetivo de evaluar los resultados de uno o más programas los cuales han sido, o estén siendo aplicados dentro de un contexto determinado.

También es un estudio empírico, en tanto implica una investigación de campo: a partir del universo fue precisada una muestra por el personal de Gestión Humana, Tecnología, Ventas y Control de Fraudes de la población total que son las empresas de telecomunicaciones existentes en Santo Domingo, D.N. Será factible realizar esta investigación en un periodo de mayo-septiembre del año en curso.

Población y muestra

Se estableció como universo a los empleados del Departamento de Gestión Humana, el Departamento de Tecnología y los Departamentos de Ventas y Control de Fraudes de las principales empresas del sector de las telecomunicaciones, que son Orange, Viva, Claro y Tricom, incluyendo a BT Latam Dominicana, una empresa revendedora de los servicios de estas cuatro a grandes cadenas de empresas. Estas ofrecen servicios del espectro radioeléctrico en la República Dominicana. (Específicamente las empresas prestadoras de líneas telefónicas).

POBLACIÓN DEPARTAMENTOS VINCULADOS PARA EL ESTUDIO				
UNIVERSO	**GESTIÓN HUMANA**	**TECNOLOGÍA**	**CONTROL DE FRAUDES**	**VENTAS**
ORANGE DOMINICANA	17	11		
TRILOGY DOMINICANA	9			
TRICOM S.A	7			
BT LATAM DOMINICANA				9
INDOTEL	15			
CLARO DOMINICANA			6	
TOTAL UNIVERSO O POBLACIÓN	74			



La muestra poblacional encuestada se compone de la siguiente manera:

- Empleados de Gestión Humana, y de Redes e Informática de Orange Dominicana. Orange es considerada una de las principales empresas de líneas telefónicas en la República Dominicana, con trece años en el país.
- Empleados Gestión Humana de Viva. Empresa de líneas telefónicas que ha consolidado rápidamente su red de telefonía GSM y mejorado su red CDMA en el país.
- Empleados Gestión Humana TRICOM. Dicha empresa es una de las principales empresas de las telecomunicaciones que ofrece en el país servicios de líneas telefónicas, cable e internet banda ancha.
- Empleados Gestión Humana del Instituto Dominicano de las Telecomunicaciones (INDOTEL), como empresa reguladora de los servicios de las telecomunicaciones.
- Empleados Soporte Técnico y Ventas de BT LATAM Dominicana. Empresa transnacional revendedora de los servicios de telecomunicaciones en el país, se encuentra registrada en la República Dominicana y ofrece servicios de telecomunicaciones globales y soporte técnico a cadenas de empresas grandes en el país tales como Occidental Hotels, Frito Lay, Cervecería Nacional Dominicana, AES Dominicana, Krafts Foods, entre otros.

Métodos e instrumentos empleados

Luego del diseño de la encuesta a aplicar, se han insertado las preguntas en una cuenta de usuario de la plataforma online (www.surveymonkey.com), que crea encuestas en línea y recopila las respuestas necesarias para analizar los resultados obtenidos.

Descripción de los instrumentos

El cuestionario de tesis aplicada a la muestra poblacional consta de 10 preguntas, de las cuales siete preguntas corresponden a la escala de Likert por selección múltiple, dos preguntas dan apertura al encuestado a definir las estrategias utilizadas dentro de la empresa, y la última pregunta solicita al encuestado identificar en orden de relevancia y según su parecer, cuales actividades deben ser reforzadas desde los Departamentos de Gestión Humana para mejoras futuras en los procesos de manejo del personal de trabajo.

Procesamiento de los datos

La recopilación de los resultados de la investigación se obtiene desde la cuenta creada en la plataforma online de www.surveymonkey.com enviando desde allí un correo electrónico a la población objetivo, con el link que contienen las preguntas de investigación. Luego de que el encuestado responde, se generan las tabulaciones y gráficos que son almacenadas en la cuenta.

CAPÍTULO VI:

Validación empírica

CAPÍTULO VI: Validación Empírica

Rendimiento de la muestra:

MUESTRA ENCUESTADA DE LOS DEPARTAMENTOS VINCULADOS PARA EL ESTUDIO					
UNIVERSO	**GESTIÓN HUMANA**	**TECNOLOGÍA**	**CONTROL DE FRAUDES**	**VENTAS**	**SOPORTE TÉCNICO**
ORANGE DOMINICANA	4	2			
TRILOGY DOMINICANA	6				
TRICOM S.A	5				
BT LATAM DOMINICANA				4	2
INDOTEL	13				
CLARO DOMINICANA			1		
TOTAL MUESTRA:	37				

Análisis de resultados

Tabla 1

1. En las empresas de las telecomunicaciones, el Departamento de Seguridad Informática y el Departamento de Gestión humana, deben participar en conjunto en la toma de decisiones y elaboración de procedimientos que eviten casos de espionaje industrial.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	24	64.87
DE ACUERDO	10	27.03
NI DE ACUERDO NI EN DESACUERDO	1	2.70
EN DESACUERDO	1	2.70
TOTALMENTE EN DESACUERDO	1	2.70
TOTAL:	**37**	**100**
Fuente: Pregunta No.1 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

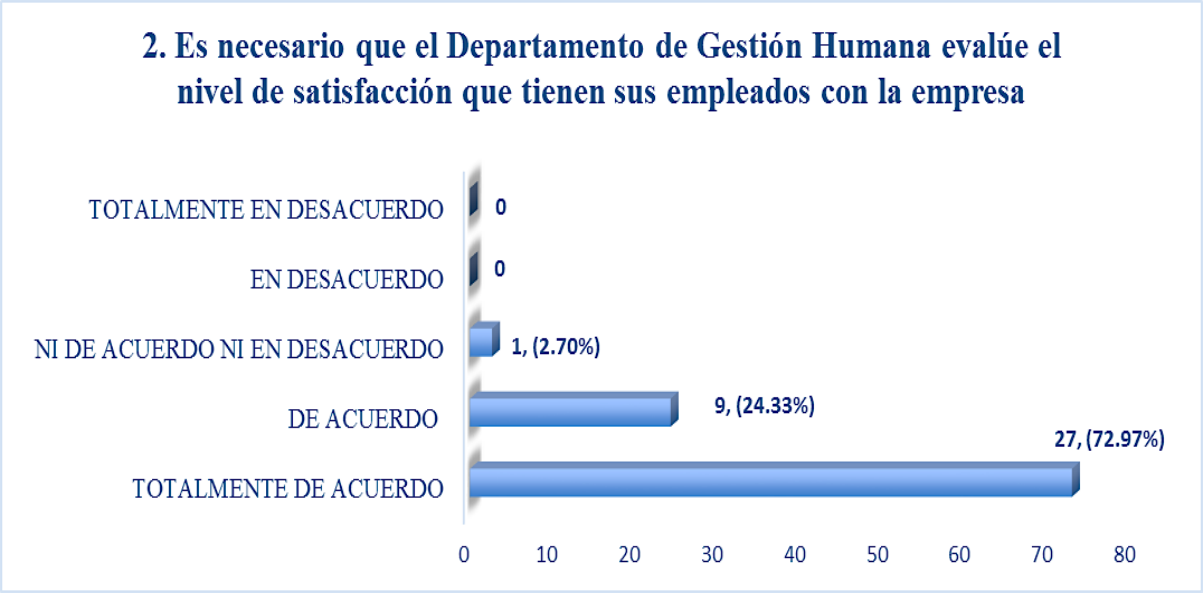
En las empresas de telecomunicaciones el 64.8% considera estar totalmente de acuerdo en que el departamento de seguridad informática y el de gestión humana, deben participar en conjunto en la toma de decisiones y elaboración de procedimiento que eviten casos de espionaje industrial, mientras que el 27.03% está de acuerdo, el 2.70% ni de acuerdo ni en desacuerdo, 2.70% manifiesta estar en desacuerdo y ese mismo porcentaje está totalmente en desacuerdo.

Fuente: Tabla no. 1

Tabla 2

2. Es necesario que el Departamento de Gestión Humana evalúe el nivel de satisfacción que tienen sus empleados con la empresa.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	27	72.97
DE ACUERDO	9	24.33
NI DE ACUERDO NI EN DESACUERDO	1	2.7
EN DESACUERDO	0	0
TOTALMENTE EN DESACUERDO	0	0
TOTAL:	**37**	**100**
Fuente: Pregunta No.2 Fuente: Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

El 72.97% de los encuestados está totalmente de acuerdo que es necesario que el Departamento de Gestión Humana evalúe el nivel de satisfacción que tienen sus empleados con la empresa, el 24.33% está de acuerdo y el 2.7% manifiesta estar ni de acuerdo ni en desacuerdo.

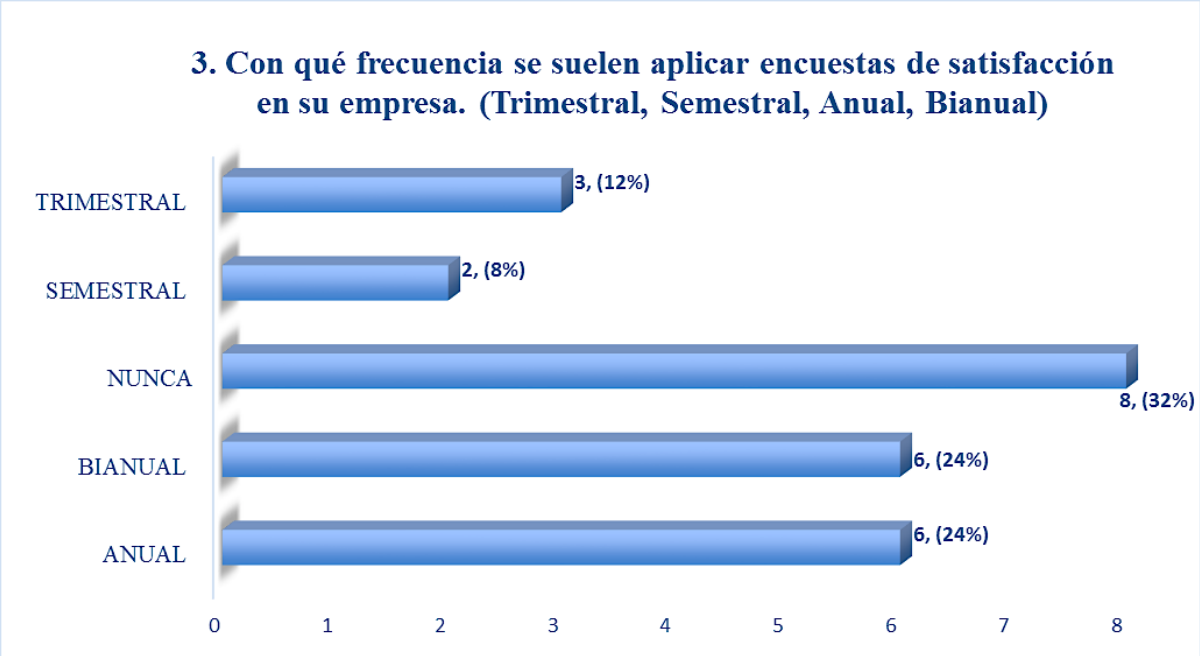


Fuente: Tabla no. 2

Tabla 3

3. Con qué frecuencia se suelen aplicar encuestas de satisfacción en su empresa (Trimestral, Semestral, Anual, Bianual)		
RESPUESTAS:	**FRECUENCIA**	**%**
ANUAL	6	24
BIANUAL	6	24
NUNCA	8	32
SEMESTRAL	2	8
TRIMESTRAL	3	12
TOTAL:	**25**	**100**
Fuente: Pregunta No.3 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

Se identificó la frecuencia en que se suele aplicar encuestas de satisfacción en la empresa; donde el 24% de los encuestados indican que se realizan anual y de igual porcentaje señalan que bianual, se encontró que el 32% subraya que nunca se realiza la encuesta, tanto que el 12% dicen que de forma trimestral, sin embargo el 8% mide la satisfacción en forma semestral. Doce encuestados omitieron las respuestas a la pregunta comentada.

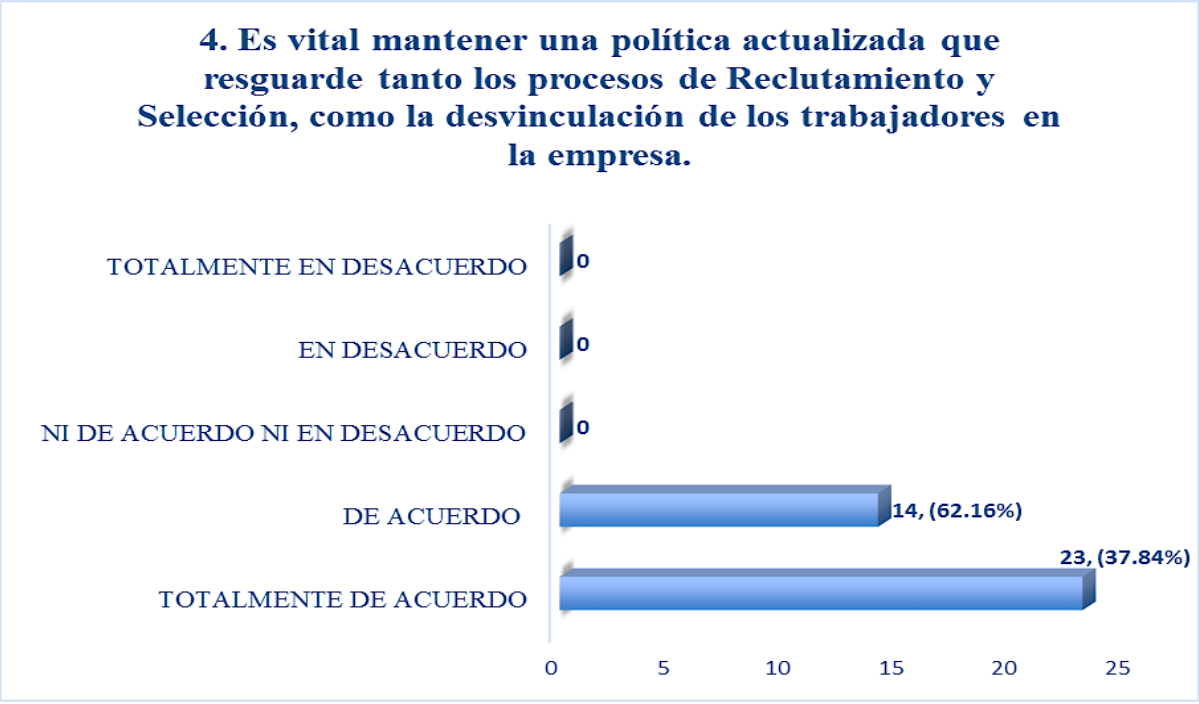


Fuente: Tabla no. 3

Tabla 4

4. Es vital mantener una política actualizada que resguarde tanto los procesos de Reclutamiento y Selección, como la desvinculación de los trabajadores en la empresa.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	23	62.16
DE ACUERDO	14	37.84
NI DE ACUERDO NI EN DESACUERDO	0	0
EN DESACUERDO	0	0
TOTALMENTE EN DESACUERDO	0	0
TOTAL:	**37**	**100**
Fuente: Pregunta No.4 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

Opinan estar totalmente de acuerdo el 62.16% de los encuestados en que es vital mantener una política actualizada que resguarde tanto los procesos de reclutamiento y selección, como la desvinculación de los trabajadores en la empresa, mientras que el 37.84% están de acuerdo.



Fuente: Tabla no. 4

Tabla 5

5. Existen en la empresa políticas y procedimientos claros en el marco de la confidencialidad de la información clasificada.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	16	43.24
DE ACUERDO	17	45.95
NI DE ACUERDO NI EN DESACUERDO	0	0
EN DESACUERDO	4	10.81
TOTALMENTE EN DESACUERDO	0	0
TOTAL:	**37**	**100**
Fuente: Pregunta No.5 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

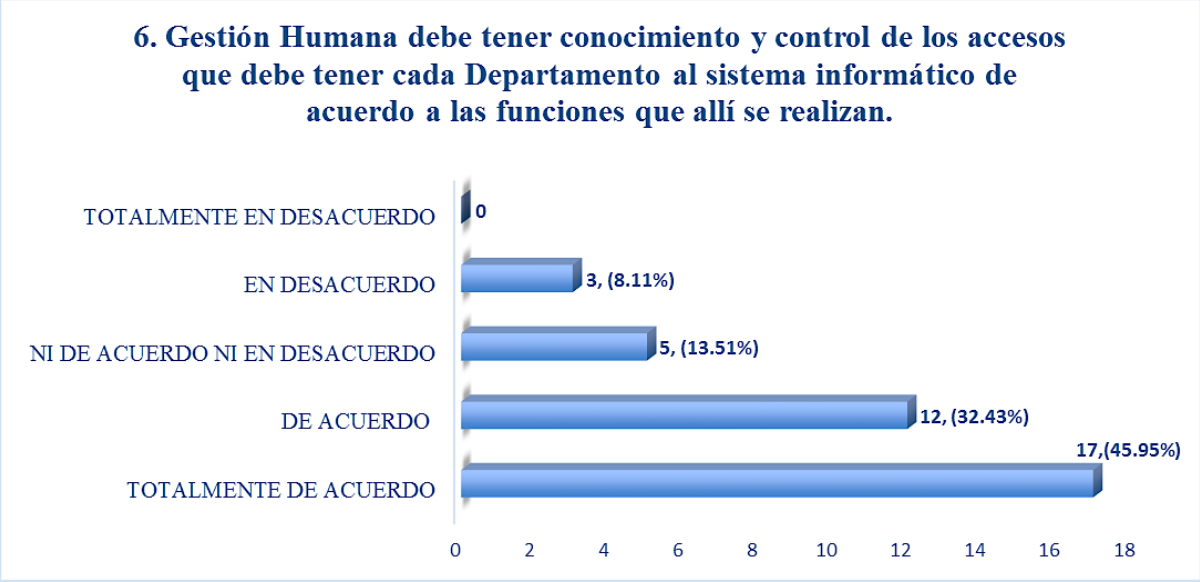
El 43.24% de los encuestados está totalmente de acuerdo en que existen en la empresa políticas y procedimientos claros en el marco de la confidencialidad de la información clasificada, de igual porcentaje 45.95% está de acuerdo en esta afirmación, sin embargo en desacuerdo se encuentra el 10.81%.

Fuente: Tabla no. 5

Tabla 6

6. Gestión Humana debe tener conocimiento y control de los accesos que debe tener cada Departamento al sistema informático de acuerdo a las funciones que allí se realizan.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	17	45.95
DE ACUERDO	12	32.43
NI DE ACUERDO NI EN DESACUERDO	5	13.51
EN DESACUERDO	3	8.11
TOTALMENTE EN DESACUERDO	0	0
TOTAL:	**37**	**100**
Fuente: Pregunta No.6 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

De las respuestas presentadas, totalmente de acuerdo es el 45.95% en que Gestión Humana debe tener conocimiento y control de los accesos que debe tener cada departamento al sistema informático de acuerdo a las funciones que allí se realizan, el 32.43% está de acuerdo a este tema, tanto el 13.51% ni de acuerdo ni en desacuerdo. En un porcentaje menor de 8.11% están en desacuerdo.

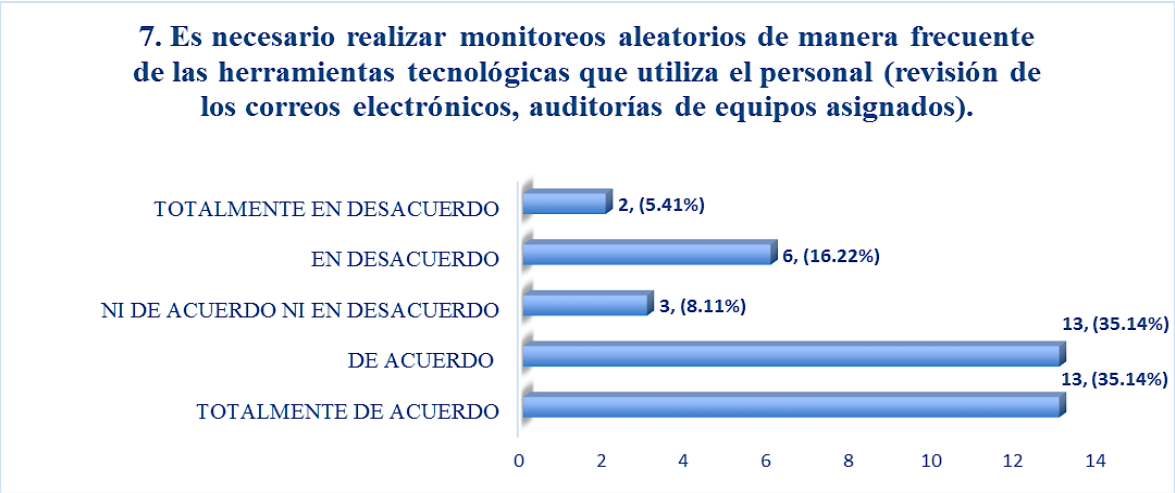


Fuente: Tabla no. 6

Tabla 7

7. Es necesario realizar monitoreos aleatorios de manera frecuente de las herramientas tecnológicas que utiliza el personal (revisión de los correos electrónicos, auditorías de equipos asignados).		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	13	35.14
DE ACUERDO	13	35.14
NI DE ACUERDO NI EN DESACUERDO	3	8.11
EN DESACUERDO	6	16.22
TOTALMENTE EN DESACUERDO	2	5.41
TOTAL:	**37**	**100**
Fuente: Pregunta No.7 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

Se presenta la afirmación de que es necesario realizar monitoreo aleatorios de manera frecuente de las herramientas tecnológicas que utiliza el personal, lo cual para un porcentaje de 35.14% en las respuestas están totalmente de acuerdo y de igual porcentaje 35.14% están de acuerdo, mientras que el 16.22% manifiesta estar en desacuerdo y el 8.11% ni de acuerdo ni en desacuerdo, sin embargo el 5.41% totalmente en desacuerdo de esta afirmación planteada.

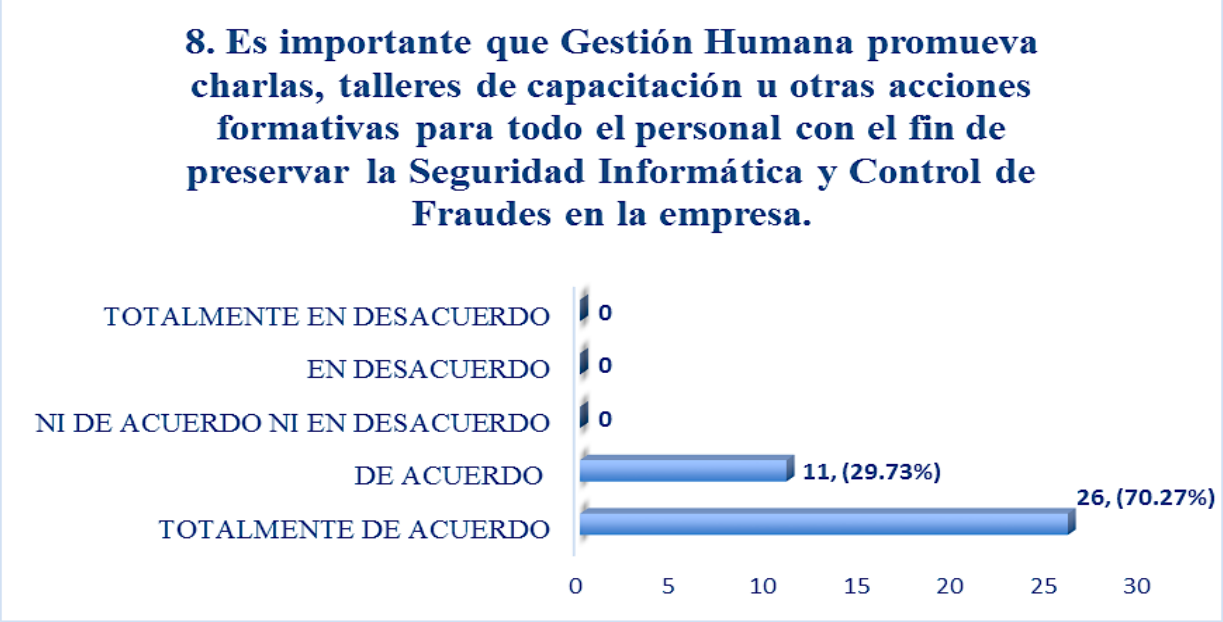


Fuente: Tabla no. 7

Tabla 8

8. Es importante que Gestión Humana promueva charlas, talleres de capacitación u otras acciones formativas para todo el personal con el fin de preservar la Seguridad Informática y Control de Fraudes en la empresa.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
TOTALMENTE DE ACUERDO	26	70.27
DE ACUERDO	11	29.73
NI DE ACUERDO NI EN DESACUERDO	0	0
EN DESACUERDO	0	0
TOTALMENTE EN DESACUERDO	0	0
TOTAL:	**37**	**100**
Fuente: Pregunta No.8 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

El mayor porcentaje de los encuestados el 70% considera es importante que Gestión Humana promueva acciones formativas para todo el personal con el fin de preservar la seguridad industrial, mientras que el 29.73% de los mismos señala estar de acuerdo en este planteamiento.

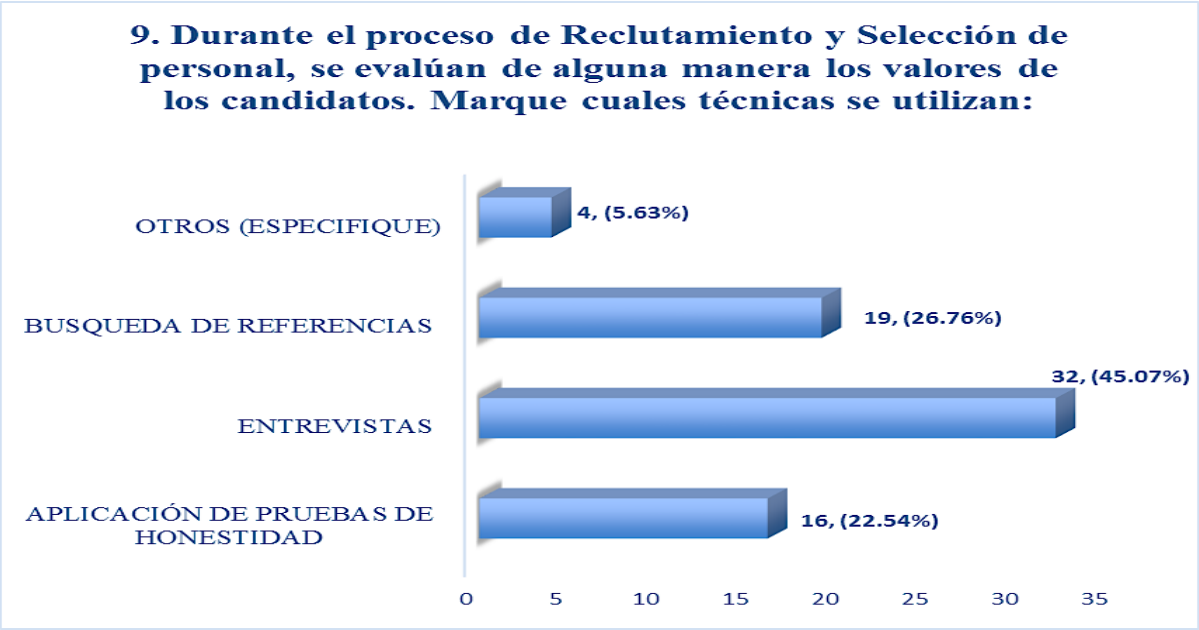


Fuente: Tabla no. 8

Tabla 9

9. Durante el proceso de Reclutamiento y Selección de personal, se evalúan de alguna manera los valores de los candidatos. Marque cuales técnicas se utilizan:		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
APLICACIÓN DE PRUEBAS DE HONESTIDAD	16	22.54
ENTREVISTAS	32	45.07
BUSQUEDA DE REFERENCIAS	19	26.76
OTROS (ESPECIFIQUE)	4	5.63
NINGUNO	0	0
TOTAL:	**71**	**100**
Fuente: Pregunta No.9 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

El 22.54% de los evaluados, durante el proceso de reclutamiento y selección de personal señala que se evalúa mediante la aplicación de pruebas de honestidad, el 45.07% utiliza la técnica de entrevista, el 26.76% tienen en cuenta la búsqueda de referencias, mientras que el 5.63% menciona otras técnicas. La frecuencia en esta pregunta fue de 71 debido a que cada entrevistado tenía la posibilidad de llenar varias opciones.



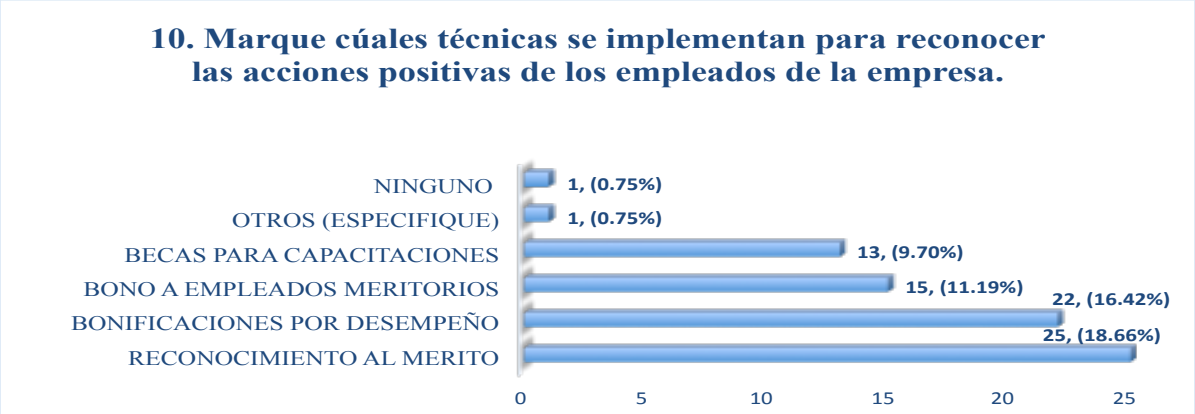
Fuente: Tabla no. 9

Tabla 10

10. Marque cuales técnicas se implementan para reconocer las acciones positivas de los empleados de la empresa.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
RECONOCIMIENTO AL MERITO	25	18.66
BONIFICACIONES POR DESEMPEÑO	22	16.42
BONO A EMPLEADOS MERITORIOS	15	11.19
BECAS PARA CAPACITACIONES	13	9.70
OTROS (ESPECIFIQUE)	1	0.75
NINGUNO	1	0.75
TOTAL:	**77**	**57.46**

Fuente: Pregunta No.10 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.

Entre las técnicas que se implementan para reconocer las acciones positivas de los empleados de la empresa, encontramos que un 18.66% practica el reconocimiento al mérito, el 16.42% implementa la bonificación por desempeño, el 11.19% realiza la entrega de bono a los empleados meritorios, la beca para capacitaciones es dada en un 9.70% de las empresas, tanto que el 0.75% otros y de igual porcentaje 0.75% no reconoce a sus empleados. En la presente pregunta hubo una frecuencia de 77, ya que el encuestado tenía la posibilidad de elegir más de una opción.

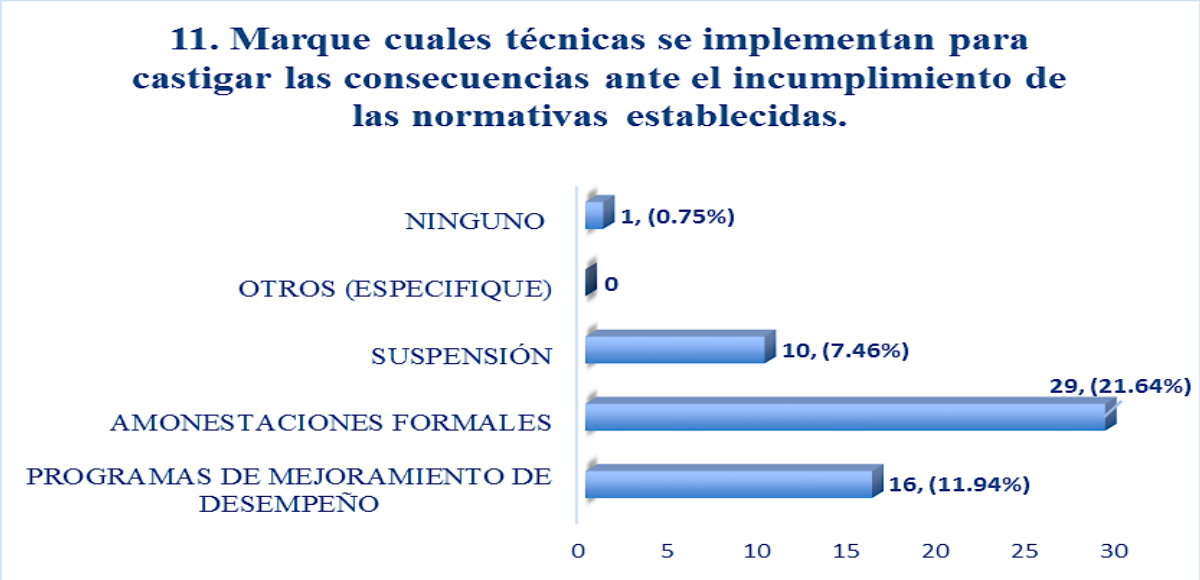


Fuente: Tabla no. 10

Tabla 11

11. Marque cuales técnicas se implementan para castigar las consecuencias ante el incumplimiento de las normativas establecidas.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
PROGRAMAS DE MEJORAMIENTO DE DESEMPEÑO	16	11.94
AMONESTACIONES FORMALES	29	21.64
SUSPENSIÓN	10	7.46
OTROS (ESPECIFIQUE)	0	0.00
NINGUNO	1	0.75
TOTAL:	**56**	**41.79**
Fuente: Pregunta No.11 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

El 21.64% de los encuestados señalan que realizan amonestación formal a sus empleados, mientras que el 11.94% practica los programas de mejoramiento de desempeño como técnica de consecuencia ante el incumplimiento de las normas de la empresa, sin embargo el 7.46% indica que ejerce la suspensión a sus empleados. Se obtuvo una frecuencia de 56, ya que el encuestado tenía la oportunidad de elegir más de una opción.

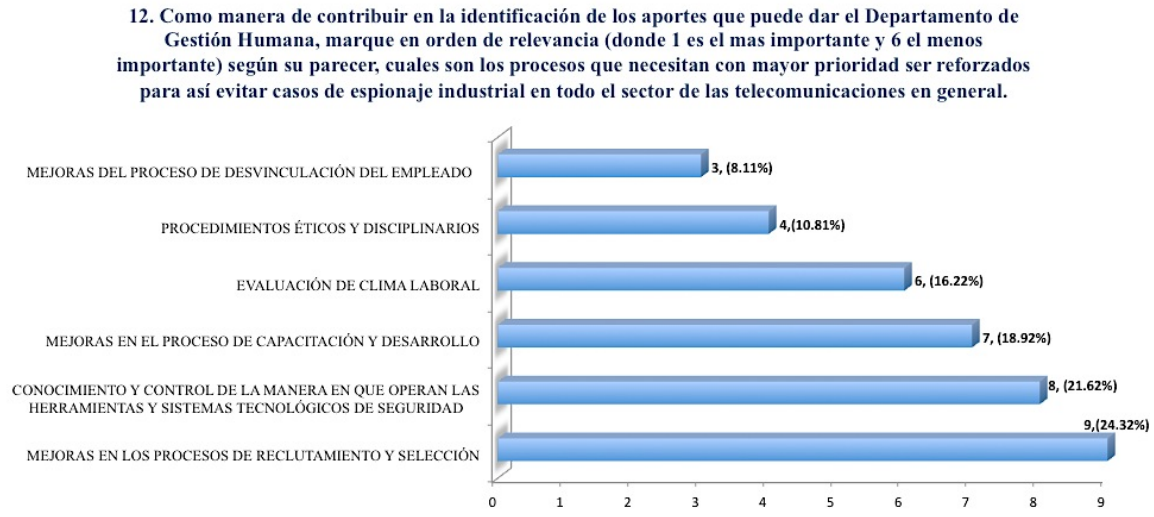


Fuente: Tabla no. 11

Tabla 12

12. Como manera de contribuir en la identificación de los aportes que puede dar el Departamento de Gestión Humana, marque en orden de relevancia (donde 1 es el más importante y 6 el menos importante) según su parecer, cuales son los procesos que necesitan con mayor prioridad ser reforzados para así evitar casos de espionaje industrial en todo el sector de las telecomunicaciones en general.		
OPCIONES DE RESPUESTAS	**FRECUENCIA**	**%**
MEJORAS EN LOS PROCESOS DE RECLUTAMIENTO Y SELECCIÓN	9	24.32
CONOCIMIENTO Y CONTROL DE LA MANERA EN QUE OPERAN LAS HERRAMIENTAS Y SISTEMAS TECNOLÓGICOS DE SEGURIDAD	8	21.62
MEJORAS EN EL PROCESO DE CAPACITACIÓN Y DESARROLLO	7	18.92
EVALUACIÓN DE CLIMA LABORAL	6	16.22
PROCEDIMIENTOS ÉTICOS Y DISCIPLINARIOS	4	10.81
MEJORAS DEL PROCESO DE DESVINCULACIÓN DEL EMPLEADO	3	8.11
TOTAL:	**37**	**100**
Fuente: Pregunta No.12 Encuesta aplicada a empleados de Gestión Humana, Informática, Ventas y Control de Fraudes de las empresas de telecomunicaciones.		

Entre los proceso a priorizar manifestados por los encuestados vemos que el 24.32% indica que las mejoras en los procesos de reclutamiento y selección han de mejorar, en segundo lugar el 21.62% indica que el conocimiento y control de la manera en que operan las herramientas y sistemas tecnológicos de seguridad, en tercer orden el 18.92% sugiere que existan mejoras en el proceso de capacitación y desarrollo, el 16.22% entienden que es importante la evaluación del clima laboral, mientras que el 10.81% sugiere ver los procedimientos éticos y disciplinarios, tanto que el 8.11% plantean realizar mejoras del proceso de desvinculación del empleado.



Fuente: Tabla no. 12

Valor de confiabilidad de la encuesta

En la presente investigación al ser tan reducida y no llegar a 100 personas, se pretendió aplicar la encuesta a toda la población (74 personas), sin embargo solo 37 personas respondieron satisfactoriamente a la encuesta, por lo cual se está valorando en 37 como la muestra poblacional.

A continuación se detalla la formula que nos dará respuesta al grado de confiabilidad de la encuesta aplicada:

$$Z = \sqrt{\frac{e \cdot n}{p \cdot q}}$$

$$Z = \sqrt{\frac{0.05\ (37)}{(0.5)\ (0.5)}}$$

$$Z = \sqrt{7.4}$$

$$Z = 2.75$$

$$\frac{-74}{2.75}$$

71.25%

Donde:

n: Tamaño de la muestra

P= Probabilidad de éxito

Q= Probabilidad de fracaso

e: Error muestral

Se manejaron los siguientes valores universales:

e= 5% = 0.05

n: 37

P= 50% = 0.50

Q= 1-P= 0.50

El porcentaje que respondió implica un (71.25%) de confiabilidad y margen de error del (23.75%). En opinión de Carlos Custodio, experto en estudios estadísticos, el presente estudio con el margen de error señalado es confiable en virtud de que la población encuestada es desde el punto de vista profesional y por su desempeño laboral homogénea; sus valoraciones tienen alto grado de confiabilidad aún cuando solo se haya podido aplicar el instrumento al 50% de la población total. Según estadísticos, las encuestas comerciales siempre arrojan de un 60 a un 80% el valor de confiabilidad, las sociales y políticas de un 80 a un 95%.

Discusión de los resultados

Se ha alcanzado el objetivo principal del estudio, que ha sido identificar los desafíos que tienen los departamentos de Gestión Humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial.

Se aplicó la encuesta a los Departamentos de Gestión Humana del sector de las telecomunicaciones, ya que este es considerado la pieza clave para los procesos de selección y administración de personal. También se encuestó el Departamento de Seguridad Informática, y el de Tecnología, que permiten vigilar los sistemas informáticos utilizados en la empresa y controlar los accesos de personas a las áreas que la componen, al Departamento de Ventas, porque se encarga de gestionar las estrategias de ventas de los productos que promueve la empresa, manejando la publicidad y promoción de estos y el de Control de Fraudes; encargado de la supervisión y buen cumplimiento de los deberes que tienen los usuarios de las informaciones y sistemas en la empresa.

La encuesta ha arrojado los resultados esperados, obteniendo de ella a manera de conclusiones generales que la mayor población ha seleccionado en orden de mayor a menor relevancia, los procesos que entienden deben mejorarse para una mejor gestión del talento humano.

En primer lugar, un porcentaje de un 24.32% afirma que antes que nada se debe trabajar en la propuesta de mejoras en el subsistema de Reclutamiento y Selección.

De estos resultados puede también inferirse que el personal de una empresa tiende a suponer que solo deben cuidarse los procesos de vinculación con la empresa, dejando más a un lado mantener el empleado comprometido con su lugar de trabajo y cuidar los procesos de desvinculación del empleado con la empresa, sea cual fuere la causa de dicha desvinculación.

El 21.62% de la muestra poblacional encuestada, afirma que el Departamento de Gestión Humana debe tener total conocimiento y control de la manera en la que operan las herramientas y sistemas tecnológicos de seguridad. Este criterio procura que todos los empleados de la empresa solo puedan acceder a la información que le compete de acuerdo a sus funciones, siendo el Departamento de Gestión Humana que solicite los accesos necesarios al sistema informático del individuo en caso de ser designado a una función o que este pase por un cambio de posición ya sea en su misma área con diferentes funciones, o en otro Departamento de la empresa.

Un 18.92%, en tercer lugar afirma que deben realizarse mejoras en los procesos de Capacitación y Desarrollo, principalmente incluyendo igualdad de oportunidades para subsidios estudiantiles, becas para capacitaciones y bonificaciones a empleados meritorios. Según los resultados obtenidos se confirma que existe la necesidad de elaborar propuestas que den mayor apertura a los empleados a tener una igualdad de oportunidades para capacitarse o desarrollarse profesionalmente, y que se reconozcan las acciones positivas de dichos empleados, ya que esto les hace sentir que se valora su esfuerzo y los mantiene comprometidos con la empresa.

Otorgando el cuarto lugar al 16.22%, se solicita que se realicen mejoras en la evaluación de clima laboral. Según los resultados, se tuvo la oportunidad de identificar cual es la frecuencia en que se aplican encuestas de satisfacción en la empresa; donde el mayor porcentaje de la muestra encuestada correspondiente al 32%, afirma nunca haber participado de una evaluación de clima laboral en la empresa en el tiempo que tienen trabajando para ella. Es necesario tomar en cuenta el tiempo en que debe aplicarse la evaluación de clima laboral con el fin de cumplir con las políticas que la contemplan.

Las mejoras de los procedimientos éticos y disciplinarios, han obtenido un quinto lugar, dando un resultado del 10.81%, y demostrando que existe la necesidad de realizar mejoras en esta parte. Puede ser necesaria la revisión frecuente de dichos procedimientos para cumplir con una actualización constante de los reglamentos éticos, disciplinarios, normas y políticas de la empresa. Por último pero no menos importante, un 8.11% plantea que se hagan propuestas en el proceso de desvinculación del empleado con la empresa, haciendo que su proceso de salida sea de la manera menos traumática posible.

Cada uno de los Departamentos encuestados se adecua al estudio ya que son primordiales en los procesos vitales de la empresa, tanto en la Gestión del talento humano, los procesos Informáticos y su Seguridad, como de las Ventas Corporativas. Dichos Departamentos en conjunto, han podido arrojar las informaciones necesarias para identificar oportunidades de mejora en los procesos internos de las empresas de las telecomunicaciones. Aunque cada uno por separado se visualice teniendo funciones disímiles, todos se relacionan porque cada Departamento realiza tareas significativas, que en su conjunto consiguen una mejor Gestión de Personal.

Conclusión

Conclusión

Se ha tenido la oportunidad de identificar en el presente estudio, los procedimientos en los Departamentos de Gestión Humana que deben ser reforzados para evitar casos de espionaje industrial en el sector de las telecomunicaciones del país, cumpliendo así con el objetivo general propuesto. Ha sido necesaria la aplicación de una encuesta a la muestra poblacional, para poder obtener un conocimiento básico de los procesos que se realizan en dicho Departamento, y de ahí partir a sugerir las posibles oportunidades de mejoras en el área.

Ha sido planteada la interrogante acerca de que si existe la necesidad de relacionar el Departamento de Gestión Humana con los procesos que maneja el Departamento de Seguridad Informática, ya que es cierto que la protección de las informaciones es responsabilidad del área que las generan, así como las personas que tienen acceso a ella. Sin embargo, las personas que tienen a su cargo procesos de Selección y Administración de Personal, inevitablemente también están ligadas a la protección de la información.

La realización de este trabajo ha permitido alcanzar los objetivos específicos de la siguiente manera:

1. El instrumento utilizado en la investigación ha arrojado informaciones acerca de los procedimientos de Reclutamiento y Selección que actualmente se aplican en las empresas de las telecomunicaciones, ayudando a determinar las medidas que pueden ser tomadas en cuenta con el fin de lograr mejoras en el Departamento de Gestión Humana para evitar que empleados desleales ingresen en la organización. Dando lugar así la respuesta al primer objetivo especifico.

A consideración de los encuestados, la mayor cantidad de empleados afirmó estar de acuerdo con que se requieran ciertas mejoras en el proceso de Reclutamiento y Selección, y en último lugar se destacó que existe la necesidad de aportar mejoras en el proceso de desvinculación del empleado con la empresa. Teniendo en cuenta la profesionalidad y experiencia de cada persona encuestada, el porcentaje más reducido también es merecedor de atención.

2. En relación al segundo objetivo, se ha concluido que han sido detectados ciertos mecanismos que se consideran necesarios para evaluar la honestidad de los empleados en el proceso de Reclutamiento y Selección, así mismo se reconocen de alguna manera otros valores de los candidatos en este proceso. Se afirmó que en primer lugar son aplicadas entrevistas al momento de reclutar personal nuevo para la empresa, en segundo lugar se afirma que se utiliza el mecanismo de búsqueda de referencias, y en tercer lugar han contestado que se aplican pruebas de honestidad.

3. Se han identificado diversas metodologías que evalúan la satisfacción del empleado basándose en su desempeño laboral, cuestionando si son aplicadas en las empresas pruebas de satisfacción de personal, y cada qué tiempo se realizan. Dando así respuesta al tercer objetivo de la investigación, se encontró en su mayor porcentaje, que nunca se han aplicado pruebas de satisfacción, resultado que fue tomado en cuenta para realizar las recomendaciones de lugar.

4. El análisis de los procedimientos correctos que pueden mejorar los Departamentos de Gestión Humana para el cumplimiento de los Deberes y Derechos de los empleados, se ha elaborado mediante la identificación de las técnicas que son aplicadas para otorgar compensaciones en base a evaluaciones positivas de los empleados, como también realizar las amonestaciones de lugar ante el incumplimiento de las normativas establecidas. El mayor porcentaje de los encuestados ha respondido que el reconocimiento al mérito y las bonificaciones por desempeño son las técnicas más utilizadas, alcanzando así el logro del cuarto objetivo.

5. El quinto objetivo de la investigación, ha permitido identificar las valoraciones posibles ante los sistemas de consecuencias que se aplicarían en los Departamentos de Gestión Humana en casos de espionaje industrial. Los resultados arrojados muestran que son aplicadas mayormente amonestaciones formales, y programas de mejoramiento de desempeño.

6. Ha sido detectada la necesidad que puede tener la relación entre los Departamentos de Seguridad Informática y Gestión Humana, para participar en conjunto en la toma de decisiones y elaboración de procedimientos que eviten casos de espionaje industrial. Los resultados del instrumento aplicado confirman la necesidad de esta alianza, cumpliendo así con los resultados esperados en el sexto objetivo de la investigación.

En conclusión, cabe destacar que desde siempre el espionaje ha sido una posibilidad de la cual toda empresa debe cuidarse. En esta investigación, se realizó un aporte que permite mejorar las planificaciones a optimizar en las políticas y procedimientos de los Departamentos de Gestión Humana, para una correcta implementación de estas desde la gestión continua del personal de trabajo.

Recomendaciones

Recomendaciones

Se ha tenido la oportunidad de señalizar posibles aportes que busquen proporcionar mejoras desde los procesos internos de Gestión Humana, dentro de las que se destacan:

1. **Conocimiento del personal de trabajo.** Identificar las personas que se sienten inconformes en la empresa, pudiendo llegar a ser conflictivas debido a este aspecto, ya que un empleado insatisfecho no se considera la persona indicada para tener acceso a informaciones confidenciales. Se ofrece esta recomendación ya que se ha cuestionado con qué frecuencia se aplican pruebas de satisfacción en la empresa, y la mayor cantidad de respuestas arrojó que nunca se han aplicado en el tiempo que tienen trabajando los encuestados para ella, determinándose así que es necesario que sean aplicadas con mayor regularidad. Contradice la idea que a pesar de que las empresas de las telecomunicaciones cuentan con políticas y procedimientos que guían las acciones de personal, no se mide de manera frecuente el compromiso de los empleados con la empresa.
2. **Custodiar los procesos de vinculación y desvinculación en la organización.** Es importante el control de los accesos y registros que realiza la persona en sus primeros o últimos momentos en la empresa. Por lo que se ha indagado si existe la necesidad de elaborar un plan de mejoras en los procesos de vinculación y desvinculación de los empleados, partiendo de las operaciones que los Departamentos de Gestión Humana realizan en la actualidad. Según los resultados recopilados, se ha concluido en que es primordial evaluar los procesos actuales de reclutamiento y selección:
    - Aplicando herramientas que puedan medir la honestidad al momento de evaluar los candidatos para una posición vacante.

- Cumpliendo con la búsqueda de las referencias laborales, confirmando así la validez de los datos del currículum vitae.
- Solicitar al empleado antecedentes penales.
- Diseño de un formulario de autorización de revisión de datos de los candidatos en el proceso de reclutamiento y selección, midiendo en esta parte el cumplimiento ante responsabilidades sociales.

3. En el proceso de desvinculación se pueden implementar nuevas técnicas como el outplacement, conocido como el conjunto de técnicas que se utilizan para reubicar a los trabajadores cuando por una razón u otra hay que prescindir de parte del personal. Esta transicion pretende contenerlos y reorientarlos, facilitandoles una positiva reinserción laboral.

4. Existe la necesidad de inculcar a la cultura empresarial del sector de las telecomunicaciones, que al Departamento de Gestión Humana también concierne tener conocimiento de la manera en que operan las herramientas tecnológicas (hardware, software o la combinación de ambos) que ha desarrollado la empresa para prever la fuga de información en los equipos y la red. Es necesario que se promueva la participación en conjunto del Departamento de Gestión Humana e Informática, para la toma de decisiones y elaboración de procedimientos que eviten casos de espionaje industrial. Se confirma en este punto la necesidad de realizar monitoreos aleatorios a las herramientas tecnológicas que utiliza el personal de trabajo (revisión del buen uso de los correos empresariales, auditorías a los equipos asignados).

5. La necesidad de contar con políticas y procedimientos bien definidos en las empresas de las telecomunicaciones. Es infalible la transmisión a los empleados y comprensión clara de las políticas de seguridad empresarial. Se sugiere:

- Revisar anualmente las políticas y procedimientos de gestión humana en las empresas, procurando mantener actualizadas las acciones de personal en la empresa.
- Que las empresas de las telecomunicaciones revisen anualmente las políticas y procedimientos que complementan el marco de la confidencialidad de la información clasificada, incluyendo dentro de dichas políticas empresariales formularios que contemplen acuerdos de confidencialidad para el manejo de la información delicada por parte de los empleados.
- Igualdad de oportunidades dentro del otorgamiento de becas para capacitación. Se sugiere más apertura a las empresas del sector de las telecomunicaciones para quienes puedan realizar estudios que puedan ser de beneficio tanto para el empleado como para las empresas.
- Cumplimiento de los procedimientos fieles a la leyes del Código de Trabajo Dominicano, de las técnicas aplicadas en caso de incumplimiento de las normativas establecidas en las empresas de las telecomunicaciones, ya que los resultados han arrojado que solo un mínimo porcentaje de la muestra poblacional encuestada afirma que son aplicadas suspensiones o procedimientos legales en caso de que el empleado viole sus deberes como parte de la empresa.

6. Implementar estrategias de concienciación. Dar a conocer al personal de trabajo la responsabilidad que se tiene ante el manejo de información clasificada, pudiendo utilizar dentro de los Departamentos sensibles trituradoras, y mostrar las consecuencias que puede traer la fuga de información. Es necesario aplicar dentro de la empresas, una capacitación permanente a los empleados que trabajan para ella de la siguiente manera:

- Incluyendo dentro de las políticas y procedimientos de capacitación la necesidad de contar en las empresas de las telecomunicaciones con charlas, talleres, conferencias u otras acciones formativas que en el año promuevan la Seguridad Industrial.

La prevención de fuga de información es una problemática que debe concernir no solo a las empresas de las telecomunicaciones, sino también:

- Es necesario que el Congreso Nacional y el Poder Ejecutivo sigan legislando para responder a los desafíos para una necesaria transparencia, competencia leal y la garantía de los derechos de cada cliente o usuario de las telecomunicaciones.

- Las universidades deben hacer mejoras en los contenidos curriculares en carreras relacionadas con las telecomunicaciones, y la informática, así como crear nuevas carreras, como expertos en derecho informático.

- Finalmente, se requiere de igual manera fortalecer los acuerdos con la comunidad internacional para perseguir el delito de las telecomunicaciones desde donde pueda ocasionarse.

Limitaciones de la investigación

Limitaciones de la investigación

Dentro de los límites de la investigación se encuentra la negación al acceso a la información por parte de ciertas empresas de las telecomunicaciones que componen la población de dicho sector, tales como Claro Dominicana y WIND Telecom, quienes de ninguna manera permitieron la aplicación formal de la encuesta a su Departamento de Gestión Humana, ni de manera presencial ni virtual, ni siquiera con un aval de la universidad que solicitase la autorización para aplicar la encuesta, ya que justificaban que su Departamento de Ética le impedía que terceros accedieran a sus informaciones sobre sus políticas y procedimientos empresariales. Claro Dominicana no vio un formato siquiera de la encuesta donde ellos mismos confirmaran que no existían preguntas comprometedoras.

Cabe destacar la reciente compra de Orange Dominicana por parte de Tricom, S.A. donde ya se encuentran de manera estructural fusionados, pero dicha fusión aún no tiene validez operativa ya que el Instituto Dominicano de las Telecomunicaciones (INDOTEL), hasta la fecha no ha aprobado legalmente su unificación. Es por esto que fue un poco más complicado realizar la solicitud de aplicación de la encuesta de tesis, ya que algunos empleados no sabían cual era la mecánica para manejarse a causa de esa situación. Se aplicó la encuesta por separado al personal de Orange, y Tricom, S.A. aunque ya estén en el mismo edificio.

Sugerencias de ulteriores investigaciones

Sugerencias de ulteriores investigaciones

Debido a la magnitud de las inquietudes que existen con respecto al tema investigado, y la escasa iniciativa de estudiar al respecto por la delicadeza con que es tratado el espionaje industrial, se han sugerido diversos estudios que pueden servir de aporte para ulteriores investigaciones, dentro de las que se destacan:

- Implementación de la encriptación de los correos empresariales y mantenimiento de los canales de información para conseguir una sólida seguridad informática de las empresas.
- Análisis de la viabilidad de contratación de empresas externas dedicadas a la protección de datos corporativos.
- Disertación de las legislaciones existentes en torno al espionaje industrial en Latinoamérica.

La realización de dichos estudios podrían servir de base para abrir paso a nuevas interrogantes del espionaje industrial y las consecuencias que produce a las empresas víctimas.

Referencias bibliográficas

Referencias bibliográficas

Bibliografía

Diccionario de la Real Academia Española. (2001). Diccionario de la Lengua Española. (21ra Ed.). Madrid, España: Espasa- Calpe.

Marco, Francisco y Escamilla, David. (2008). El control en la empresa. Granica: España. 270 páginas.

Ley General de las Telecomunicaciones No.153-98. INDOTEL

Cabrera Mejía, Lucymarie. (2000). Derecho a la privacidad en la interceptación de líneas telefónicas. Tesis Lic. En Derecho.

Comisión Europea. Europa: Preguntas y respuestas, el por qué y el cómo de la competencia en el sector de las telecomunicaciones.

Ballesteros Moffa, Luis Ángel. (2005). La Privacidad Electrónica. Valencia: Tirant lo Blanch. Monografía.

Torres, Enilda. (2001). La guerra del espionaje. Vol. 40. Págs. 1194.

Peña, Pascual. (sept. 2007). Intimidad, espionaje y secreto. Gaceta Judicial año 11, No. 250. Pág. 46-49.

Arbaje Berges, Joan Carolina. (2007). Análisis jurídico de la interconexión de redes de telecomunicaciones en la República Dominicana. Tesis licenciatura en derecho.

Blake, Roy. (2004). Sistemas electrónicos de comunicaciones. 2da. Ed. México: D.F. Thomson. 985 Páginas.

Akalin, Ogus. (1979). Leyes de radiodifusión: materiales sobre política y sociedad en la republica federal de Alemania.

Código de Trabajo de la República Dominicana, 2013.

Constitución de la República Dominicana, 1994.

Constitución de la República Dominicana, 2010.

Despradel, Fernando. (2001). Inteligencia envenenada (novela). Págs. 173.

Navarro, Emilio del Peso. (2003). Manual de Outsorcing Informático: Análisis y contratación. Madrid: Ediciones Díaz de Santos. Págs. 85-87.

Aznar, Hugo, Villanueva, Ernesto. (2000). Deontología y autorregulación informativa: ensayos desde una perspectiva comparada. México: Fundación Manuel Buendía: Universidad Iberoamericana. Págs. 89-90.

Parsons, June Jamrich y Oja, Dan. (2008). Conceptos de Computación: nuevas perspectivas. México: CengageLearning. Págs. 18-24.

Gutiérrez Francés, María Luz. (1991). Fraude informático y estafa. Madrid: Artegraf. Págs. 642.

Users staff. (2011). Hacking desde cero. Buenos Aires: Fox Andina. Págs. 174.

Bremmer, Ian. (Lunes 13 enero, año 2014). El peligroso control de la Información. Periódico El País. Fuente recuperada el 10 de julio del 2014.

Tamayo, A. (2001). Auditoría de sistemas, una visión práctica. Colombia: Universidad Nacional de Colombia.

Sánchez, M.E. (2013). Las tecnologías de la información y comunicación (TIC), como un componente clave en las entidades públicas para la implementación de los sistemas de gestión de control interno. Bogotá, Colombia: Universidad Militar Nueva Granada.

Ruíz, G.F. (1999). Planificación y gestión de sistema de información. Escuela superior de información de ciudad real. Universidad Castilla- La Mancha.

Hernández S, R.; Fernández C., C.; Baptista L., P. (2003). Metodología de la investigación. México, Distrito Federal: Mc Graw Hill.

Diccionario enciclopédico. (2003). Edición Larousse.

Diccionario enciclopédico El Pequeño Larousse Ilustrado. (2007). Madrid, España: Larousse.

Aguilera, P. (2010). Seguridad informática. Madrid, España: Editorial Editex, S.A.

Bernuy, J.J. (2008). Implementación de seguridad de la información mediante ISO-17799. Tesis de grado de ingeniería electrónica. Universidad Nacional Autónoma de México: Distrito Federal, México.

Soler Pujals, Pere. (2001). Investigación de mercados. Universidad Autónoma de Barcelona; Departamento de Comunicación Audiovisual y de Publicidad. Página 11.

Web grafía

Hernández, Fernando Bugarini. (noviembre 2007, México). Una propuesta de seguridad en la información: caso Systematics: México. Recuperado el 10 de marzo del 2014. En: http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/498/1/TESIS%20PROPUESTA%20SEGURIDAD.pdf

Investigación empresarial. Recuperado el 15 de marzo del 2014. En: http://www.deltadetectivesrd.com/servicios-de-investigacion/empresariales/

Blog, Keith. Espionaje Corporativo. Recuperado el 16 de marzo del 2014. En: http://www.forodeseguridad.com/artic/segcorp/7208.htm

Espionaje electrónico. Recuperado el 25 de marzo del 2014. En http://www.rnds.com.ar/articulos/025/RNDS_104W.pdf

Cohen, Tom. (junio, 2013). El espionaje evitó "decenas" de ataques, según la inteligencia de EE.UU. Recuperado el 28 de marzo del 2014. en: http://cnnespanol.cnn.com/2013/06/12/el-espionaje-evito-decenas-de-ataques-segun-la-inteligencia-de-ee-uu/

Marza, Juan Cruz. (octubre, año 2013). Consejos para la prevención del espionaje industrial en tu empresa. Recuperado el 28 de marzo del 2014. En: https://www.google.com/search?client=safari&rls=en&q=como+rrhh+puede+combatir+el+espionaje+industrial&ie=UTF-8&oe=UTF-8

Cdconsultores. (enero, año 2013.) Prevenir la fuga de información también involucra a las áreas de Recursos Humanos. Recuperado el 30 de marzo del 2014. En: http://blog.cdconsultores.com.mx/2013/01/31/prevenir-la-fuga-de-informacion-tambien-involucra-a-las-areas-de-recursos-humanos/

(10 junio, 2013). Edward Snowden, genio informático que desnuda el espionaje en E.E.U.U. Recuperado el 18 de abril del 2014. En: http://www.eldeber.com.bo/edward-snowden-el-genio-que-39desnudo-39-la-inteligencia-de-eeuu/130610161211

De Paula, Iván. (agosto, año 2006). INDOTEL cancela funcionario por espionaje. Recuperado el 20 de abril del año 2014. En: http://btdom.wordpress.com/2006/08/21/indotel-cancela-funcionario-por-espionaje/

(julio, año 2013). Diez tips para asegurar sus datos. Sección de Tecnología; Periódico Listín Diario. Recuperado el 21 de abril del año 2014. En: http://listindiario.com.do/tecnologia/2013/7/15/284596/Diez-tips-para-asegurar-sus-datos

Bermúdez Vega, Humberto Andrés. (Año 2002, La Habana). La contrainteligencia en las organizaciones. Recuperado el 20 de mayo del 2014. En: http://www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH0126.dir/doc.pdf

Moya, Cecilia (12 marzo, año 2014). Como prevenir el espionaje industrial. Recuperado el día 28 de mayo del 2014. En: http://agente0014.blogspot.com/2014/03/005.html

Sulbarán, Eleazar. (agosto, año 2011). ¿Cómo detectar el espionaje industrial? Dos claves profesionales. Recuperado el 30 de mayo del año 2014. En http://eleazar.over-blog.es/article-como-detectar-espionaje-industrial--claves-profesionales-85923760.html

(21 agosto, 2006). INDOTEL cancela funcionario por espionaje. Recuperado el 03 de julio del 2014. En: http://btdom.wordpress.com/2006/08/21/indotel-cancela-funcionario-por-espionaje/

(4 julio, 2013). Alemania recomienda renunciar a los servidores de EE.UU. para evitar el espionaje. Recuperado el 05 de julio del 2013. En: http://actualidad.rt.com/actualidad/view/99155-alemania-renunciar-google-facebook-eeuu

García Noguera, Noelia. (15 julio, 2002). Delitos Informáticos en el Código Penal Español. Recuperado el 05 de julio del 2014. En: http://www.portaley.com/delitos-informaticos/espionaje.shtml

Cohen, Tom. (junio, 2013). El espionaje evitó "decenas" de ataques, según la inteligencia de EE.UU. recuperado el 05 de julio del 2014. En: http://cnnespanol.cnn.com/2013/06/12/el-espionaje-evito-decenas-de-ataques-segun-la-inteligencia-de-ee-uu/

Aehightech, (7 noviembre, 2012).Contraespionaje, Barridos Electrónicos, Equipos Espías, Protección, Espionaje, Búsqueda. Recuperado el 05 de julio del 2014. En: http://espionajemexico.blogspot.com/2012/11/5-simples-reglas-para-evitar-el.html

(31 Diciembre, 1969). Escándalo por espionaje industrial en RENAULT. Recuperado el 08 de julio del 2014. En: http://www.elheraldo.co/internacional/escandalo-por-espionaje-industrial-en-renault

Báez, Julio. (25 agosto, 2010). Green Love, la solución del reciclaje de papel en RD. Recuperado el 08 de julio del 2014. En: http://www.laalertaverde.com/2010/08/green-love-la-solucion-al-reciclaje-de.html

Normas y Políticas de seguridad de la información. Código de buenas prácticas para la gestión de la seguridad de la información (basado en la norma técnica NTP-ISO/IEC17799:2000. Recuperado el 10 de julio del 2014. En: https://www.crq.gov.co/Documentos/NORMAS_SEGUIRIDAD_CRQ.pdf

Reseña Histórica OPTIC. Recopilado el 25 de agosto del 2014. En: http://www.optic.gob.do/index.php?option=com_zoo&view=item&Itemid=117

Ramírez Egil, Aguilera Ana Rosa. (Mayo, 2009). Los delitos informáticos. Tratamiento internacional. Recopilado el 28 de agosto del 2014. En: http://www.eumed.net/rev/cccss/04/rbar2.htm

Periódico Listín Diario. (01 agosto 2014). CIA se disculpa por espiar ante el Senado EE.UU. Sección Las Mundiales. Recuperado el 28 de agosto del 2014. En: http://www.listin.com.do/las-mundiales/2014/7/31/331945/CIA-se-disculpa-por-espiar-en-el-Senado-EU

Touriño, Alejandro. (13 enero, 2011). ¿Puede mi ¨jefe¨ espiar mi correo electrónico?. Recuperado el 01 de septiembre del 2014. En: http://blogs.lainformacion.com/legal-e-digital/2011/01/13/

Hurtado de Barrera, Jacqueline. (2002). El proyecto de investigación holística. Colección Holos: Bogotá. 135 páginas.

Ley 53-07 Sobre crímenes y delitos de alta tecnología. Recuperado el 05 de septiembre del 2014. En: http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

Carmona, M.A, Camacho, G.B., Vásquez, V.L.; Rivas, M.A. (2008). Guía para la integración de sistemas de gestión sobre la base de los procesos. Instituto Andaluz de Tecnología. Recuperado el 28 de julio del 2014. En: http://excelencia.iat.es/files/2012/08/Guia_integraci%C3%B3n.pdf

Chiriboga, M.G. (2008). Diseño de pruebas de cumplimiento para el control interno, basadas en la ley Sarbenex-Oxley. Universidad Tecnológica Equinoccial. Quito, Ecuador. Recuperado el 18 de agosto del 2014. En: http:/repositorio.ute.edu.ec/bitstream/123456789/9936/1/35581_1.pdf

Lago, H. (2010). Mejores prácticas en gestión de servicios de TI. Recuperado el 20 de julio, 2014. En: http://www.slideshare.net/Nbarros/presentacin-5532544

Informe COSO (1992). Recuperado el 20 de julio, 2014. En: http://www.coso.org/

Heras, I., Bernardo, M.; Casadesús, M. (2007). La integración de los sistemas de gestión basados en estándares internacionales: resultado de un estudio empírico. Revista de dirección y administración de empresas. Número 14. Recuperado el 20 de julio, 2014. En: http://ehu.es/ojs/index.php/rdae/article/view/11435/10551

Burgos, S.J.; Campos, G.P. (S/F). Modelo para la seguridad de la información en TIC. Chile: Universidad Bio-Bio. Recuperado el 25 de julio del 2014. En: http://ceur-ws.org/Vol-488/paper13.pdf

Cano, F. (2012). Gestión de activos de TI. Recuperado el 28 de julio del 2014. En: http://www.seinhe.com/blog/64-gestion-de-activos-de-ti

Control interno en tecnología de la información. (n.f.). Recuperado el 20 de julio, 2014. En: http:/www.buenastareas.com/ensayos/Control-Interno-En-Tecnolog%C3%Ada-De-Informaci%C3%B3nll/3675747.html

Borghello, C.F. (2001). Seguridad información: su implicancias e implementación. Tesis de grado para optar por licenciatura en sistemas. Recuperado el 25 de julio del 2014. En: http://www.segu-info.com.ar/tesis/

Álvarez, F.M.; y García, P.A. (2007). Implementación de un sistema de seguridad de la información basado en la norma 27001 para la intranet de la corporación metropolitana de salud. Escuela politécnica nacional. Recuperado el 22 de julio del 2014. En: http://bibdigital.epn.edu.ec/bitstream/15000/565/1/CD-1077.pdf

ANEXOS

ENCUESTA TRABAJO DE GRADO

"Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

DATOS GENERALES

SEXO: **F** ☐ **M** ☐ **EMPRESA:**_____

INSTRUCCIONES GENERALES

Esta encuesta es realizada con la finalidad de obtener mediante una investigación cualitativa, informaciones que permitan identificar los aportes que pueda realizar la Gestión de los Recursos Humanos en las empresas de las telecomunicaciones de la República Dominicana, para reducir o evitar el espionaje industrial y robo de informaciones confidenciales.

Espionaje industrial es la práctica y conjunto de técnicas asociadas a la obtención encubierta de datos o información confidencial.

Los resultados serán manejados de una forma completamente anónima y confidencial. Agradeceremos sus respuestas con la mayor transparencia, veracidad y objetividad posible, para así poder tener un acercamiento a desarrollar sistemas de mejoras en el departamento de Gestión Humana.

ENCUESTA TRABAJO DE GRADO

"Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

ENCUESTA

1. En las empresas de las telecomunicaciones, el Departamento de Seguridad Informática y el Departamento de Gestión humana, deben participar en conjunto en la toma de decisiones y elaboración de procedimientos que eviten casos de espionaje industrial.

TOTALMENTE DE ACUERDO ☐
DE ACUERDO ☐
NI DE ACUERDO NI EN DESACUERDO ☐
EN DESACUERDO ☐
TOTALMENTE EN DESACUERDO ☐

2. Es necesario que el Departamento de Gestión Humana evalúe el nivel de satisfacción que tienen sus empleados con la empresa.

TOTALMENTE DE ACUERDO ☐
DE ACUERDO ☐
NI DE ACUERDO NI EN DESACUERDO ☐
EN DESACUERDO ☐
TOTALMENTE EN DESACUERDO ☐

3. Complete con qué frecuencia se suelen aplicar encuestas de satisfacción en su empresa (Trimestral, Semestral, Anual, Bianual).

Trimestral ☐
Semestral ☐
Anual ☐
Bianual ☐
Nunca ☐

"Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

4. Es vital mantener una política actualizada que resguarde tanto los procesos de Reclutamiento y Selección, como la desvinculación de los trabajadores en la empresa.

TOTALMENTE DE ACUERDO ..... ☐
DE ACUERDO ..... ☐
NI DE ACUERDO NI EN DESACUERDO ..... ☐
EN DESACUERDO ..... ☐
TOTALMENTE EN DESACUERDO ..... ☐

5. Existen en la empresa políticas y procedimientos claros en el marco de la confidencialidad de la información clasificada.

TOTALMENTE DE ACUERDO ..... ☐
DE ACUERDO ..... ☐
NI DE ACUERDO NI EN DESACUERDO ..... ☐
EN DESACUERDO ..... ☐
TOTALMENTE EN DESACUERDO ..... ☐

6. Gestión Humana debe tener conocimiento y control de los accesos que tiene que tener cada Departamento al sistema informático de acuerdo a las funciones que allí se realizan.

TOTALMENTE DE ACUERDO ..... ☐
DE ACUERDO ..... ☐
NI DE ACUERDO NI EN DESACUERDO ..... ☐
EN DESACUERDO ..... ☐
TOTALMENTE EN DESACUERDO ..... ☐

"Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

7. Es necesario realizar monitoreos aleatorios de manera frecuente de las herramientas tecnológicas que utiliza el personal (revisión de los correos electrónicos, auditorías de equipos asignados).

TOTALMENTE DE ACUERDO ☐
DE ACUERDO ☐
NI DE ACUERDO NI EN DESACUERDO ☐
EN DESACUERDO ☐
TOTALMENTE EN DESACUERDO ☐

8. Es importante que Gestión Humana promueva charlas, talleres de capacitación u otras acciones formativas para todo el personal con el fin de preservar la Seguridad Informática y Control de Fraudes en la empresa.

TOTALMENTE DE ACUERDO ☐
DE ACUERDO ☐
NI DE ACUERDO NI EN DESACUERDO ☐
EN DESACUERDO ☐
TOTALMENTE EN DESACUERDO ☐

9. Durante el proceso de Reclutamiento y Selección de personal, se evalúan de alguna manera los valores de los candidatos. Marque cuales técnicas se utilizan:

APLICACIÓN DE PRUEBAS DE HONESTIDAD ☐
ENTREVISTAS ☐
BÚSQUEDA DE REFERENCIAS ☐
OTROS, ESPECIFIQUE ☐
NINGUNO ☐

10. Marque cuales técnicas se implementan para reconocer las acciones positivas de los empleados de la empresa.

RECONOCIMIENTO AL MERITO ..... ☐
BONIFICACIONES POR DESEMPEÑO ..... ☐
BONO A EMPLEADOS MERITORIOS ..... ☐
BECAS PARA CAPACITACIONES ..... ☐
OTROS (ESPECIFIQUE) ..... ☐
NINGUNO ..... ☐

11. Marque cuales técnicas se implementan para castigar las consecuencias ante el incumplimiento de las normativas establecidas.

PROGRAMAS DE MEJORAMIENTO DE DESEMPEÑO ..... ☐
AMONESTACIONES FORMALES ..... ☐
SUSPENSIÓN ..... ☐
OTROS (ESPECIFIQUE) ..... ☐
NINGUNO ..... ☐

"Desafíos de los departamentos de gestión humana en el sector de las telecomunicaciones para evitar casos de espionaje industrial. Período mayo-septiembre del 2014. Santo Domingo, D.N. República Dominicana".

12. Como manera de contribuir en la identificación de los aportes que puede dar el Departamento de Gestión Humana, marque en orden de relevancia (donde 1 es el mas importante y 6 el menos importante) según su parecer, cuales son los procesos que necesitan con mayor prioridad ser reforzados para así evitar casos de espionaje industrial en todo el sector de las telecomunicaciones en general.

MEJORAS EN LOS PROCESOS DE RECLUTAMIENTO Y SELECCIÓN ..... ☐

MEJORAS DEL PROCESO DE DESVINCULACIÓN DEL EMPLEADO ..... ☐

MEJORAS EN EL PROCESO DE CAPACITACIÓN Y DESARROLLO..... ☐

CONOCIMIENTO Y CONTROL DE LA
MANERA EN QUE OPERAN LAS HERRAMIENTAS
Y SISTEMAS TECNOLÓGICOS DE SEGURIDAD ..... ☐

PROCEDIMIENTOS ÉTICOS Y DISCIPLINARIOS ..... ☐

EVALUACIÓN DE CLIMA LABORAL ..... ☐

Concesionarias Servicio de Telefonía

No.	Concesionarias del servicio de "Telefonía"	Provincia	Teléfonos
1	Advanced Voip Telecom, S.A.	Santo Domingo	829-236-3330 / 809-549-6810
2	Cap Cana Tel, S.A.	Santo Domingo	809-469-7065 ext. 7972 y 3298 / 809-472-2525 Fax. 809-375-5509 / 809-682-0508
3	Colortel, S.A.	Santo Domingo	829-229-9000 / Fax 829-229-9001
4	Compañía Dominicana de Teléfonos, C. por A. (Claro-Codetel)	Santo Domingo	809-220-2957 / Cel 809-519-2403 / Fax 809-567-2840
5	DR Pronto Telecommunications Corp., S.A. (Prontotel)	La Romana	809-441-7056 / Cel. 809-813-1967 / Fax 809-686-5413
6	Estrela Telecom, S.A.	Santo Domingo	829-471-7600
7	Mundo 1 Telecom, S.R.L.	Santiago	809-724-5676
8	Onemax, S.A.	Santo Domingo	809-530-6242, Fax 809-530-1252
9	Orange Dominicana, S.A.	Santo Domingo	809-859-1621 / 809-859-1085 / Fax 809-859-1078
10	Ozymandias Company, S.A.	Santo Domingo	829-946-5533 / 809-449-7000
11	Skymax Dominicana, S.A.	Santiago	809-724-1166 / Fax 809-587-3239
12	Sociedad Nacional de Telecomunicaciones (Sonatel)	Santo Domingo	Cel. 809-519-0770 (Juan Ant. Simo) / Ofic.809-621-8599 / Fax 809-565-4654
13	Tekcom Dominicana, S.A.	Santo Domingo	809-979-6400 / 829-589-0665
14	Tricom, S.A.	Santo Domingo	809-476-4120 / 809-633-8594 / Fax 809-476-4412
15	Trilogy Dominicana, S.A. (Viva)	Santo Domingo	809-503-9412 / 809-503-1000 / 809-503-1075
16	Turitel, S.A.	Santo Domingo Este	809-482-0874 / 809-596-1000 ext. 302 Fax 809-687-2621
17	Viark-Tek Network Communication, S.A.	Santo Domingo	809-565-9655 / 809-333-3311
18	Wind Telecom, S.A.	Santo Domingo	829-946-3037 / Ofi. 829-946-3111 / 3037 / 3003 / 829-946-3038

Ultima Actualización: 30 de Noviembre de 2012
Compilado por: José Rafael Matías, Encargado de Recaudaciones
Nota: Este listado solo incluye empresas autorizadas "operando"

Gráfico 1.0

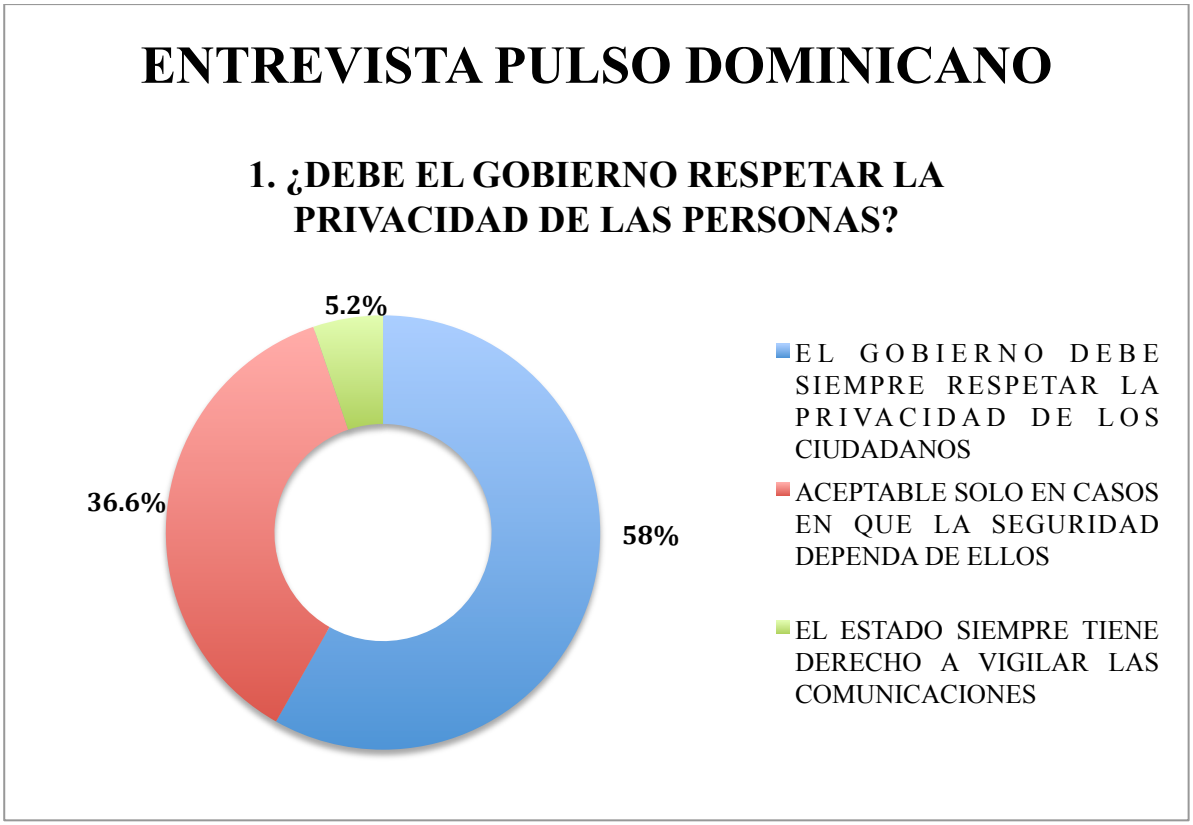


Gráfico 1.1

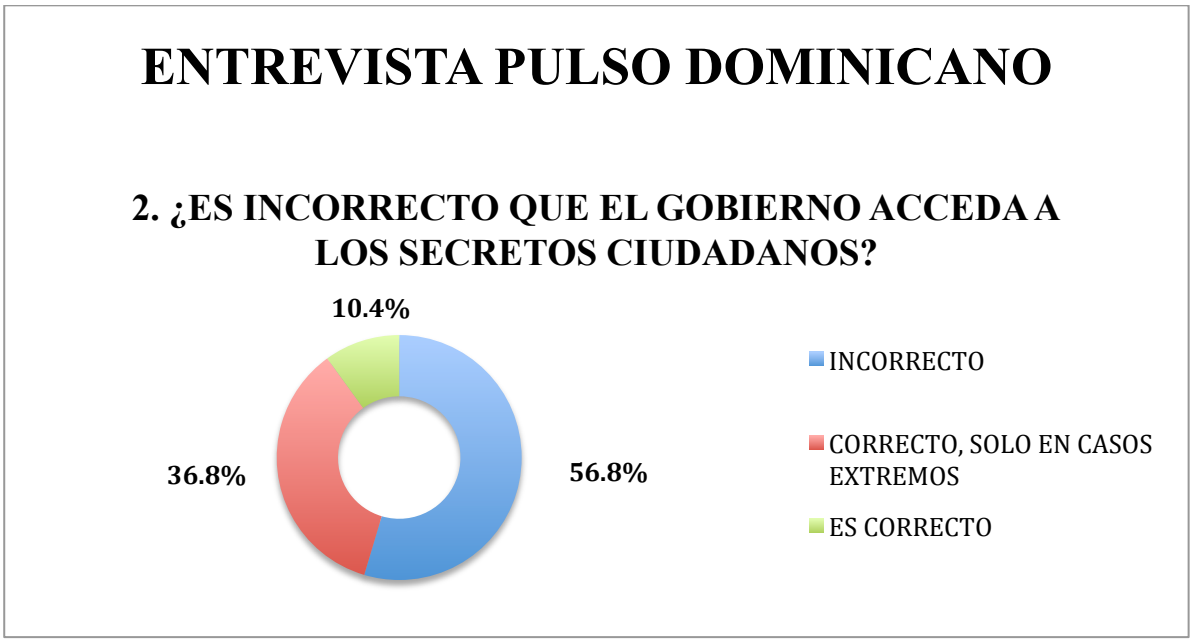


Gráfico 1.2

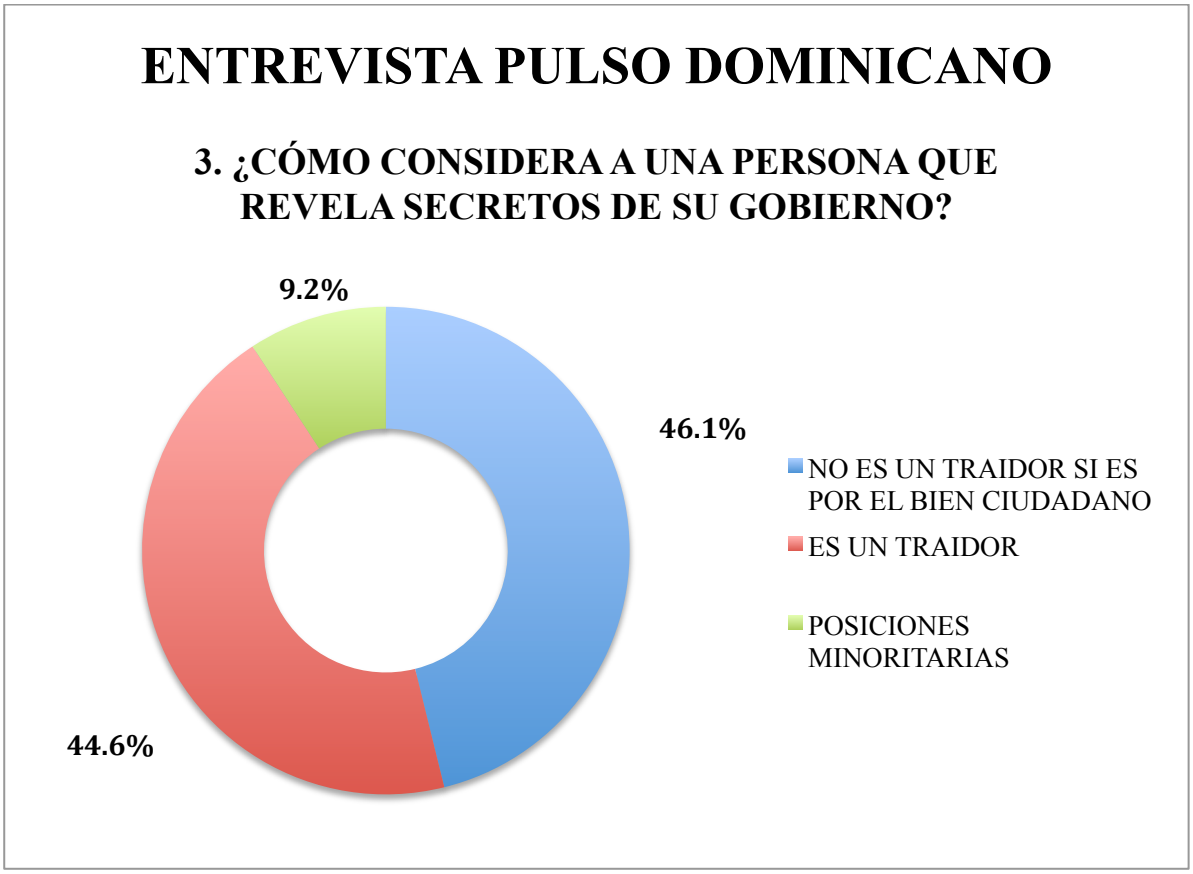


Gráfico 1.3

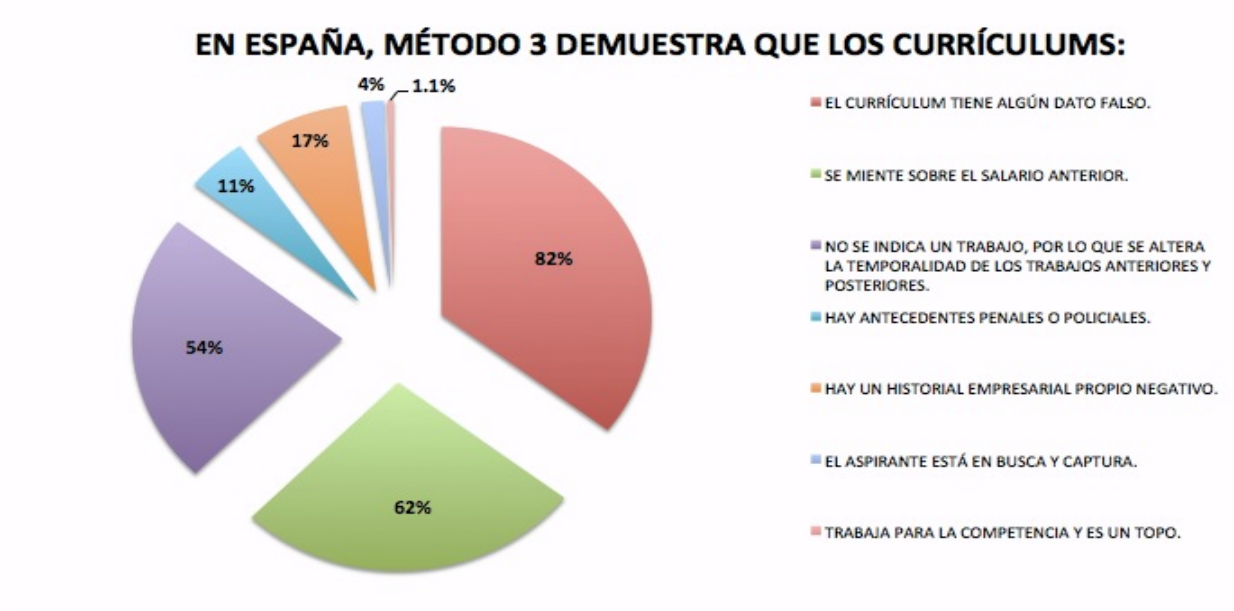


Gráfico 1.4

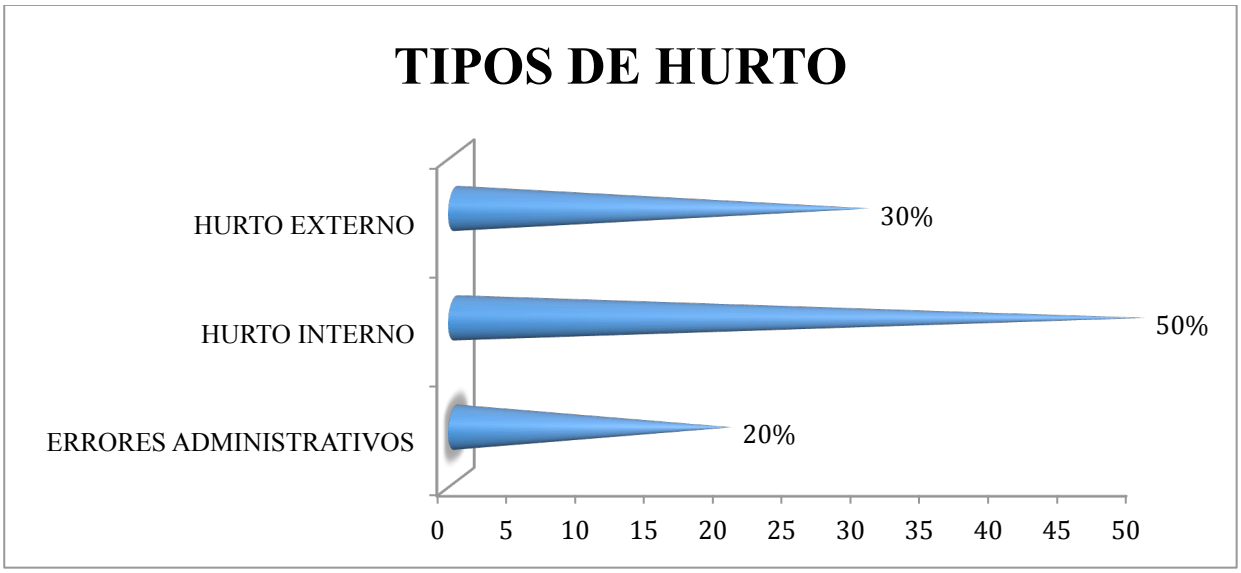


Gráfico 1.5

EVALUACIÓN

Sustentante:

_____
Sacha Mariela Santos Molina

Asesor (a):

_____
Ana Gisela Ramos B.

Jurados:

_____ _____
Lelia de la Cruz Yanilsa Benítez

_____
Alexandra Elizo

_____
Licda. Adrian Teonilda De Oleo
Directora Escuela Psicología

Calificación: _____

Fecha: ____/____/_____