UNIVERSIDAD APEC
UNAPEC

Escuela de Graduados
Maestría en Gerencia y Productividad

ANALISIS DE LOS PROCESOS DE SEGURIDAD EN INFORMATICA EN LA GERENCIA DE TECNOLOGÍA DE LA INFORMACION Y COMUNICACIÓN DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES INDOTEL, EN LA CIUDAD DE SANTO DOMINGO, PERÍODO ENERO-ABRIL 2013

Trabajo de Investigación para optar por el Grado de Magíster en Gerencia y Productividad.

Presentado por:

Maika Sivelth Rodríguez Pérez 2011-2250

Asesor:

Miguel Ángel Díaz Méndez, M.A

Santiago de los Caballeros

República Dominicana

ABRIL, 2013

RESUMEN

El tema de este estudio consiste en el “Análisis de los procesos de seguridad informática en la Gerencia de Tecnología de la Informacion y Comunicación (GTIC), del Instituto Dominicano de las Telecomunicaciones (INDOTEL) en la ciudad de Santo Domingo, República Dominicana, período enero-abril de 2013”. La historia del INDOTEL no fue sino, hasta la promulgación de la Ley General de Telecomunicaciones, No 153.98. A través del auge de las nuevas tecnologías este ha acogido las mismas utilizando plataformas técnologica, siendo cada vez más dependiente de sus recursos informáticos, teniendo esto consigo diversos riesgos, que de ocurrir afectarían los activos de la institución, traduciéndose esto a pérdidas invaluables de información, y esto a su vez, paraliza los procesos administrativos, es por esto que el objetivo general de está invetsigación es: Analizar los procesos de seguridad informática de la GTIC en el INDOTEL, así como también los objetivos específicos son: Identificar las herramientas tecnológicas de la GTIC del INDOTEL, Identificar las políticas de seguridad en informática aplicadas por la GTIC en el INDOTEL e Identificar las amenazas y vulnerabilidades que enfrenta la seguridad informática de la GTIC en el INDOTEL. Concluyéndose que la Gerencia de Tecnología de la Información y Comunicación no cuenta con el hardware necesario para lograr un mejor desempeño en cuanto a la seguridad informática se refiera, de igual forma se observó que las herramientas tecnológicas deben facilitar los procesos de gestión de la seguridad Informatica, así como también, debe existir la documentación necesaria para el control y los registros, que ayuden a realizar la labor diaria y se debe diseñar una política de seguridad.

TABLA DE CONTENIDO Pág.

DEDICATORIAS

Este trabajo va dedicado muy especialmente a:

A Dios, por haberme dado la vida, fortaleza, voluntad, salud y sobre todo por darme la luz en el camino para terminar este proyecto de investigación.

A mi esposo, Daniel Monegro, por darme apoyo, ánimo en los momentos que más lo necesitaba, por estar a mi lado durante esta trayectoria. Te dedico mi esfuerzo porque eres parte de mi inspiración y fuente principal de motivación. Te amo.

A mi familia, en especial a mis padres, hermanos, cuñados y sobrinos por ofrecerme su apoyo cuando elegí comenzar a estudiar de nuevo y entenderme durante este tiempo los quiero, le dedico esta investigación como fruto del sacrificio del tiempo que era para ustedes y lo invertí en la universidad.

Maika

AGRADECIMIENTOS

Les agradezco infinitamente a las siguientes personas:

Al amor de mi vida, mi esposo Daniel Monegro, por siempre estar dispuesto a ayudarme. Gracias por creer en mí, por motivarme, por ser mi inspiración para hacer las cosas excelentes y por enseñarme a distribuir mejor mí tiempo. Gracias por existir, eres y serás mi compañero, amigo, mi apoyo, mi profesor a lo largo de los días de mi vida. Gracias lo logramos juntos amor.

A mi Asesor y Profesor, Miguel Angel Díaz, quien con su paciencia y profesionalismo me guió en todo este trayecto, enriqueciendo mi trabajo de investigación con cada una de las correcciones, con la intención de que el producto final fuera lo mejor posible. Gracias profesor por sus críticas constructivas las cuales me permitieron día a día con cada observación suya mejorar, llegando a ser para mí una experiencia enriquecedora el haber podido conocerlo y contar con usted.

A papi, por ser el mejor papá del mundo, por tener la paciencia de cada mañana llevarme, apoyándome todos los días de mi vida, dándome su voto de confianza en todo lo que hago. Gracias por creer en mí.

A mami, gracias por darme la vida, por estar a mi lado en cada etapa importante de mi vida profesional, por dar su voto de confianza en mí. Eres un ser muy especial te adoro.

A todos aquellos que de una manera u otra aportaron su granito de arena para que esta investigación tuviera éxito.

Maika

INTRODUCCION

El tema de este estudio consiste en el “Análisis de los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo, período Enero-Abril 2013”.

Los antecedentes de este tema se remontan a los inicios de la escritura (con los sumerios, 3000 AC), en la biblia, también autores como Homero, Julio César y Cicerón en obras donde se mencionan rasgos de seguridad tanto en la guerra como el gobierno.

La historia de la seguridad informática comienza con los primeros intentos criptográficos, jugando así los griegos un papel predominante mediante la utilización de la excítala que le permitía cifrar la información por transposición. A principios del siglo XIX nace la informática conjuntamente con el avance tecnológico, en esta época solo se implementaba en organizaciones gubernamentales o para el ejército, ya que los ataques en las guerras y para su comunicación era de suma importancia la información de las grandes naciones, es por ello que estalló todo lo referente a la computación.

Con el paso de los años fue evolucionando, su acceso ya no era tan restringido, tanto la computación y la informática se empezaron a implementar en las grandes organizaciones. Naciendo de esta forma la Seguridad Informática, ya que por medio de las computadoras se manejaba la información de las empresas, representando esto grandes riesgos, por lo que se debió desarrollar técnicas y métodos para la seguridad informática.

Según Rosales (2002), en todo objeto de estudio de la humanidad, se necesita estabilidad y protección de información o bienes, en informática sabemos que la herramienta principal que ayudo a su divagación en el mundo, son las computadoras, cualquiera que sea la categoría.

De esa misma manera surgen las políticas de seguridad informáticas como una herramienta organizacional para concientizar a los colaboradores de la empresa sobre la importancia y sensibilidad de la información y servicios críticos, asegurando de esta forma el buen uso de los recursos informáticos y la información como activos, que se deben cuidar de daños y posibles riesgos.

Asimismo cita Correa López en su estudio Políticas y Estándares de Seguridad Informática, donde expresa que la seguridad es un proceso en el cual se deben evaluar, administrar los riegos apoyados en políticas y estándares que cubran las necesidades del departamento en función.

Desde la creación del INDOTEL mediante la promulgación de la Ley No 153-98 en Mayo de 1998, la información ha sido administrada, con ayuda de la tecnología, haciendo uso de bases de datos de la empresa con la finalidad de que los empleados hagan uso de ellas, haciendo consultas o enriqueciendo la misma. Dicha información dependiendo del departamento es confidencial y crítica “No Vulnerables”, es decir se debe evitar cualquier fuga de información a través de internet.

Hoy en día el INDOTEL es más dependiente de sus recursos informáticos, así como también se tiene presente que enfrenta diversos riesgos, que de ocurrir afectarían los recursos de la organización.

Una vulnerabilidad en la seguridad informática se traduce a pérdidas invaluables de información, y esto a su vez, paraliza los procesos administrativos, es por esto que la Gerencia de Tecnología de la Información y Comunicación juega un papel relevante en la protección de la información de la empresa.

Es por esto, que en esta investigación tiene por objeto analizar las políticas de seguridad, vulnerabilidades, amenazas con la finalidad de conseguir un sistema de información seguro y confiable.

Según Hallberg, la seguridad informática existe solo si se juntan todos los elementos y métodos que la hacen posible ya que cualquier método utilizado por sí solo no puede abarcar todos los puntos vulnerables de los sistemas de información.

Según Chávez Flores.A, es ahí donde entra en juego la seguridad informática, la cual dota a la empresa de las herramientas necesarias para restringir los programas malignos (con un antivirus), que personas foráneas accedan a la red (con un firewall), el acceso de personas a los equipos físicos de la red de la empresa.

Teniendo muy en claro, que no existe una seguridad en términos absolutos. Sólo se pueden reducir las oportunidades de un ataque o reducir los impactos del mismo ya que existen tres elementos en riesgos:

- Los datos (información guardada en las computadoras) estos tienen tres características a proteger: Confidencialidad, Integridad y Disponibilidad.
- Los recursos (el equipamiento en sí mismo).
- La reputación (una de las actividades iniciales es el Análisis de Riesgos, para lo cual, se debe realizar un modelado de amenazas), se trata de una actividad de carácter recurrente. Un riesgo es una combinación de activos, vulnerabilidades y atacantes.

Por todas estas razones previamente mencionadas se requiere responder a la siguiente interrogante:

¿Es posible analizar los procesos de seguridad en informática de la Gerencia de Tecnología de la Informaión y Comunicación (GTIC), del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo?

Las sub preguntas o sub problemas que surgen de la pregunta generadora o problemática anteriormente formulada son las siguientes:

¿Cuáles son las Herramientas tecnológicas de la Gerencia de Tecnología de la Información y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo?

¿Cuál es la política de seguridad de la Gerencia de Tecnología de la Información y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo?

¿Cuáles son las amenazas y vulnerabilidades que enfrenta la seguirdad informática de la Gerencia de Tecnología de la Información y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo?

La justificación principal de esta investigación, es que mediante la realización de este estudio se analizarán los procesos de Seguridad en Informática de la Gerencia de Tecnología de la Información y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, demostrar que la GTIC administra los sistemas de información, los cuales no dejan de ser inherentemente seguros, por lo que se debe velar por la seguridad tanto, lógica, física, recuperación de desastres, educacional y documentación necesaria.

Todo esto con la finalidad de conocer hasta qué punto se tiene control y se protegen los recursos de los equipos de información digital, con el objetivo de que exista confidencialidad (evitar divulgar información privada), mantener la integridad (evitar alterar o destruir información), y asegurar la disponibilidad (garantizar operación continua de los sistemas de la empresa, así como también si se tiene un control y monitoreo de los virus, escaneo de puertos, sabotaje a la red, pornografía, abuso interno, denegación de servicios DNS, intrusión de Red, fraude Financiero, mal uso de redes inalámbricas.

Según Torres Zarrate, L. en un estudio presentado conjuntamente con el servicio secreto de Estados Unidos, dice que el 98 % de los delitos informáticos son causados por agentes externos, motivados por el robo de datos corporativos, el resto del porcentaje es de empleados internos. Según un estudio del CSI/FBI año 2008, nos demuestra que la seguridad informática se convierte en un factor determinante para el éxito o el fracaso por el cual las organizaciones fallan.

Esta investigación dará como resultado un benchmarking para tener una mejor seguridad en informática en la GTIC, así como también recomendaciones para la política de seguridad.

A continuación se planteará el objetivo general y los objetivos específicos en torno al desarrollo de la investigación sobre los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación del INDOTEL, en Santo Domingo, siendo el objetivo general el siguiente:

- Analizar los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo.

Los Objetivos específicos:

- Identificar las herramientas tecnológicas de la Gerencia de Tecnología de la Informaión y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo.

- Definir las políticas de seguridad de la Gerencia de Tecnología de la Informaión y Comunicación (GTIC) del Instituto Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo.

- Identificar las amenazas y vulnerabilidades que enfrenta la Gerencia de Tecnología de la Información y Comunicación (GTIC) del Instituto

Dominicano de las Telecomunicaciones INDOTEL, en la ciudad de Santo Domingo.

La delimitación del estudio ayuda a identificar si el desarrollo de la investigación podrá ser posible, el cual se divide de la siguiente manera:

Tiempo: La investigación se desarrollará durante el período Enero – Abril del año 2013, correspondiente a un cuatrimestre académico de la Universidad APEC.

Personas: El universo de esta investigación está conformado por el personal de la Gerencia de Tecnología de la Información y Comunicación del INDOTEL en Santo Domingo.

Espacio: La investigación se realizará en el Instituto Dominicano de las Telecomunicaciones INDOTEL, ubicado en la Av. Abraham Lincoln #962, Edificio Osiris, Santo Domingo, República Dominicana.

Área: El área del estudio es la Gerencia de Tecnología de la Información y Comunicación, del INDOTEL.

El tipo de estudio elegido es el exploratorio porque del tema de investigación que se ha elegido no hay ningún estudio previo. El propósito general es analizar procesos de seguridad en informática de la Gerencia de Tecnología de Información y Comunicación del Instituto Dominicano de las Telecomunicaciones, en lo adelante INDOTEL, en la ciudad de Santo Domingo, analizándose todos los beneficios para la institución y para los usuarios en general. El método a utilizar es el cualitativo por la vía del razonamiento inductivo, ya que se obtuvieron informaciones generales sobre las herramientas tecnológicas, definir las políticas de seguridad, e identificar las amenazas y vulnerabilidades de la Gerencia de Tecnología de Información y Comunicación del INDOTEL.

Todo esto con la finalidad de llegar a conocer la particularidad del caso es decir, entender todo lo referente a la seguridad informática dentro de la GTIC del INDOTEL. Para lograr los objetivos de la presente investigación y medir las variables de interés, se aplicó un instrumento de recolección de datos. Dicho instrumento de recolección de datos fueron las entrevistas.

Según Palencia M, la entrevista no es más que una técnica utilizada como estrategia para la recolección de la información. Se define como la reunión concertada entre dos o más personas que ocurre al establecer un diálogo, a través del cual se identifica y reconoce de la opinión, postura o conocimiento sobre un cierto fenómeno. Las entrevistas en este caso fueron dirigidas a los actores principales de la Gerencia de Tecnología de la Información y Comunicación, con la finalidad de que aportaran toda la información de lugar.

Las fuentes de información constituyen todos los elementos capaces de suministrar información para ser utilizada en una investigación.

Según Palencia M. se distinguen tres tipos fundamentales de fuentes de información:

• **Fuentes primarias o directas**: son las que corresponde a los datos obtenidos de primera mano, por el propio investigador.

•**Fuentes secundarias o información**: consisten en resúmenes, compilaciones o listados de referencias, preparados en base a fuentes primarias.

•**Fuentes terciaria o de tercera mano**: aquellas que hacen cita de cita. De modo que una fuente primaria es aquella que provee un testimonio o evidencia directa sobre el tema de investigación.

Para la realización de esta investigación se utilizaron dos tipos de fuentes a continuación se presentarán: Fuentes Primaria (entrevistas) **y** Fuentes Secundarias (Revistas, internet, artículo y periódico).

CAPITULO I. MARCO REFERENCIAL (MARCO TEORICO)

1.1 Marco teórico

Según Briones, el marco teórico es el grupo central de conceptos y teorías que se utilizan para formular y desarrollar un argumento o tesis. Así mismo se refiere a las ideas básicas que forman la base para los argumentos con el objetivo de desarrollar una tesis coherente y que sea convincente.

En otras palabras el marco teórico es el campo o área del estudio en el que el investigador definirá todas las variables contenidas en el mismo con el objetivo de que sus lectores se familiaricen y con la connotación específica para que el estudio sea entendido a cabalidad.

A continuación se detallarán las variables que marcan las pautas del desarrollo del presente estudio:

- Herramientas tecnológicas.
- Políticas de seguridad.
- Vulnerabilidades y amenazas.

1.1.1 Herramientas tecnológicas

Son el conjunto de aplicaciones y hardware que facilitan la gestión y el control de todos los elementos informáticos del INDOTEL.

Según la RFC 1244 los recursos que se deben considerar como herramientas tecnológicas al calcular las amenazas a la seguridad en general son: hardware (Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores, terminales, routers), software (programas fuente, programa objeto, programa de diagnóstico, sistemas operativos), datos (durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditorías, bases de datos), personas (usuarios, personas necesarias para operar los

sistemas), documentación (sobre programas, hardware, sistemas, procedimientos, administrativos locales), suministros (papel, formularios, cintas, medios magnéticos). En resumen las herramientas tecnológicas son el conjunto de software y hardware, los cuales permiten que los recursos informáticos sean aplicados eficientemente.

1.1.1.1 Recursos

Según el diccionario de la lengua española un recurso es una fuente o suministro del cual se produce un beneficio. Normalmente, los recursos son material u otros activos que son transformados para producir beneficio y en el proceso pueden ser consumidos o no estar más disponibles.

Sin embargo según Alegsa, M. un recurso es un medio que permite satisfacer necesidades o alcanzar objetivos. Los recursos tecnológicos son medios con los que se vale la tecnología para cumplir su propósito.

Los recursos tecnológicos sirven para optimizar procesos, tiempos, recursos humanos; agilizando el trabajo y tiempos de respuesta que finalmente impactan en la productividad y muchas veces en la preferencia del cliente o consumidor final. Los recursos tecnológicos considerados se clasifican como específicos y transversales. Los recursos específicos incluyen herramientas, equipos, instrumentos, materiales, máquinas, dispositivos y software específicos necesarios para lograr el propósito técnico establecido.

Por su parte, los recursos transversales son de tipo intangible, y pueden ser identificados como capital intelectual (estructural y humano) o de manera más general como información y conocimiento. Mientras que los recursos transversales son necesarios para el desarrollo de los procesos que se aplican sobre un sistema (cadena de valor, unidad estratégica de negocios, empresa) y sus componentes.

1.1.1.2 Software

Según el estándar 729 del IEEE un software es el conjunto de los programas de cómputos, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

> Asimismo cita Avila, K. “El software del sistema se encarga de controlar, integrar y administrar los componentes de hardware de un sistema informático, proporcionando un entorno amigable para que los usuarios puedan ejecutar otras aplicaciones de software”

> Siendo el mismo, no más que un conjunto de programas de software que permiten al usuario interactuar con los dispositivos sin perderse en la complejidad técnica del equipo. Estos programas son la base de la arquitectura del software, incluyendo las partes que regulan las funciones de entrada/salida.

> El software del sistema incluye los sistemas operativos, controladores de dispositivos, servidores, sistemas de ventanas y programas de utilidades. Permitiendo coordinar todos los dispositivos internos o externos de la computadora como impresora, mouse, teclado y monitor.

1.1.1.3 Hardware

Según la Real Academia Española hardware es el conjunto de los componentes que integran la parte material de una computadora, el término, aunque sea lo más común, no solamente se aplica a las computadoras; del mismo modo, también un robot, un teléfono móvil, una cámara fotográfica o un reproductor multimedia.

Es decir el término hardware se refiere a todas las partes tangibles de un sistema informático, es decir sus componentes los cuales son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o

cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado, es todo lo tangible. Un sistema informático se compone de una unidad central de procesamiento (UCP/CPU), encargada de procesar los datos, uno o varios periféricos de entrada, los que permiten el ingreso de la información y uno o varios periféricos de salida, los que posibilitan dar salida (normalmente en forma visual o auditiva) a los datos procesados.

1.1.1.4 Gestión

Según el diccionario de la Lengua Española el término gestión se refiere a una acción o trámite que hay que llevar a cabo para conseguir o resolver una cosa, así como también en otro contexto es el conjunto de operaciones que se realizan para dirigir y administrar un negocio o una empresa.

El concepto de gestión hace referencia a la acción y a la consecuencia de administrar o gestionar algo. Al respecto, hay que decir que gestionar es llevar a cabo diligencias que hacen posible la realización de una operación comercial o de un anhelo cualquiera. Administrar, por otra parte, abarca las ideas de gobernar, disponer dirigir, ordenar u organizar una determinada cosa o situación.

1.1.1.5 Documentación

Según el diccionario de la lengua española Larousse, documentación es la información o conocimiento que se consigue o proporciona sobre algo con un fin determinado.

Otra definición es, que es la ciencia del procesamiento de la información, que proporciona información sobre algo con un fin determinado, de ámbito multidisciplinar o interdisciplinar.

Según Pujol, se puede señalar a la Documentación como una ciencia auxiliar e instrumental. También es una ciencia en si misma y una de las finalidades primordiales de la Documentación es informar.

Asimismo Ros García. J, la considera como una ciencia (documental), a la vez que una disciplina, no sólo una técnica. También pueden considerarse, en sentido general, las ciencias de la documentación y la documentación como sinónimos, si el contexto no perturba la intención del emisor, es decir, si no se distorsiona el mensaje del interlocutor porque no se dé ambigüedad semántica.

1.1.2 Políticas de seguridad

Identificar los elementos y las áreas de normalización con las cuales la Gerencia de Tecnología de la Información y Comunicación deberá adoptar para salvaguardar sus sistemas y la información

Según Dusan Clavijo, las políticas de seguridad son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.

Es por esto, que una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

El objetivo de la Política de Seguridad debe dirigir y dar soporte a la gestión de la seguridad de la información.La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información. Constituyéndose entonces en la base de todo el sistema de seguridad de la información.

Si bien existen algunos modelos o estructuras para su diseño, estás tienen que ser elaboradas de forma personalizada para cada empresa para así recoger las características propias que tiene la organización.

1.1.2.1 Areas de Normalización

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas, Seguridad en: Física, lógica, en redes, en los recursos humanos, en el Outsourcing y planes de Contingencia.

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

1.1.2.2 Elementos que conforman una política de seguridad

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas.
- Objetivos de la política.
- Responsabilidades de cada uno de los servicios y recursos informáticos.
- Definición de violaciones y sanciones.
- Responsabilidades de los usuarios por el acceso a la información.
- Deberán establecer las expectativas de la organización.
- Redacción clara y sencilla de la política de seguridad.
- Actualización periódica de la política de seguridad informática.

1.1.2.3 Procedimientos

Según Biegler J. (1980), los procedimientos representan la empresa de forma ordenada de proceder a realizar los trabajos administrativos para su mejor función en cuanto a las actividades dentro de la organización.

Un procedimiento es un término que hace referencia a la acción que consiste en proceder, que significa actuar de una forma determinada. El concepto, por otra parte, está vinculado a un método o una manera de ejecutar algo.

Un procedimiento, en este sentido, consiste en seguir ciertos pasos predefinidos para desarrollar una labor de manera eficaz. Su objetivo debería ser único y de fácil identificación, aunque es posible que existan diversos procedimientos que persigan el mismo fin, cada uno con estructuras y etapas diferentes, y que ofrezcan más o menos eficiencia.

1.1.3 Amenazas y Vulnerabilidades

Determinar todos los problemas y riesgos que afecten la seguridad de la información del INDOTEL, pero antes vamos a definir por separado amenaza y luego vulnerabilidad, cada uno con sus respectivos indicadores.

1.1.3.1 Amenaza

Según la Organización Internacional por la Normalización (ISO) define riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños”

A raíz de esta definición podemos concluir que cualquier problema que afecte al total funcionamiento de la empresa es considerado un riesgo o amenaza para la entidad.

Los problemas de seguridad se multiplican con gran facilidad, por lo que las empresas deben perfeccionar los sistemas y los procesos para evitar amenazas o

abordarlas cuando se produzcan. Para garantizar que la información de nuestra organización posea las características de seguridad ya mencionadas como son la confidencialidad, integridad y disponibilidad se debe poner en práctica un plan de seguridad informática.

Según Dussan Clavijo (2006), con los beneficios que nos brindan las nuevas posibilidades de conectividad, emergen también una serie de de nuevos riesgos. Muchas empresas son amezadas en su activo la información, trayendo las vulnerabilidades en los sistemas de información graves problemas y pérdidas cuantiosas.

Existen diversos tipos de amenazas a la seguridad informática, ya que ninguna empresa se encuentra excenta de las vulnerabilidades a las que se encuentra expuesta. Una amenaza siempre latente es el personal de la organización que por diversas razones pueden representar un peligro ya sea por los errores que pueda cometer sin intención como aquellos que son hechos con el objetivo de dañar a la organización.

1.1.3.1.1 Tipos de Amenazas

Amenazas Humanas

Las amenazas humanas son acciones provocadas por el hombre y pueden ser de dos tipos maliciosas y no maliciosas. Ver anexo 1.

Las maliciosas: son las amenazas que se llevan a efecto con el propósito de causar daño a la organización, estas pueden ser externas e internas. Externas: Las amenazas externas que pueden afectar al desarrollo y buen funcionamiento de las actividades de las empresas son frecuentemente originadas por el acceso a internet, ya que en esta red existen una serie de peligros como son los virus, hackers, entre otros que infiltrándose en la red interna de la organización provocando daños como mal funcionamiento de los sistemas y pérdida de información. Internas: Las amenazas internas más frecuentes son las originadas

por los propios funcionarios y ex - funcionarios de la organización motivados por un factor determinado, este abarca desde robo de información, espionaje, sabotaje hasta provocar incendios.

No maliciosas**:** Este tipo de amenazas son producidas en la mayoría de los casos por errores ocasionados por empleados que no cuentan con el conocimiento o adecuada capacitación en el manejo de equipos y sistemas.

Desastres Naturales

Son eventos originados por la naturaleza son las menos frecuentes en las organizaciones pero aún así no podemos dejar de considerarlas. Los desastres naturales contenplados son:

- Sismos
- Tsunamis
- Inundaciones

1.1.3.1.2 Categorización

Según Alvarez Marañon. G, (2007), las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

Clasificando la misma en cuatro categorías generales de amenazas o ataques: Interrupción (Este es un ataque contra la disponibilidad de información), Intercepción (Este es un ataque contra la confidencialidad), Modificación (Manipulación de la información. Es un ataque en contra de la integridad), Fabricación (Este es un ataque contra la autenticidad). Asímismo señala que estos ataques se pueden clasificar de forma útil en términos de ataques pasivos y

ataques activos. Ataques Pasivos: En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Estos ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante. El objetivo general es la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Ataques activos: Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.

- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.

- Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

1.1.3.2 Vulnerabilidades

Según Hernandez Pinto, M. en su tesis Auditor en Control de Gestión, sostiene que las vulnerabilidades suceden cuando existen grandes cantidades de datos que están almacenados electrónicamente. Estas vulnerabilidades se pueden originar por factores técnicos, institucionales, ambientales y en conjunto por malas decisiones administrativas.

Los sistemas computarizados son especialmente vulnerables a tales desafíos por las siguientes razones: complejidad en los sistemas de información, registros propios del computador, procedimientos computarizados, por cambios, el desarrollo y operación de los sistemas, sistemas automatizados, acceso a los sistemas, procesamiento de datos.

A través de los avances en las telecomunicaciones, las vulnerabilidades a la seguridad de los sistemas han aumentado, ya que los fraudes no se limitan a un solo lugar sino que puede ocurrir en cualquier punto de acceso a la red, lo que crea nuevas áreas y oportunidades para penetración y manipulación de los sistemas

1.1.3.2.1 Riesgos

Según la Organización Internacional por la Normalización (ISO), define los riesgos como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y como la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños.

Luego de esta definición se puede concluir que cualquier problema que afecte al total funcionamiento es considerado un riesgo o amenaza, siendo los peligros más frecuentes de los que deben protegerse las empresas:

- Hackers: Son piratas informáticos que acceden a la información que existe y se transmite por internet, haciendo mal uso de la información.
- Cracker: Son personas que rompen la seguridad de un sistema, accediendo con malas intenciones a la información.
- Virus: Son programas diseñados para modificar o destruir datos, pueden ser ingresados al sistema por un dispositivo externo o través de la red (e-mails).
- Gusanos: Son virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM.
- Caballos de Troya: Son virus que entra al ordenador, parece ser una cosa o programa inofensivo cuando en realidad se está expandiéndo y haciendo otra cosa, es crítico cuando lo instala un programador de la propia empresa.
- Spam: También llamado correo no deseado.
- Mantenimiento de Equipos: Es la ejecución de medidas que ayuden a prolongar la vida útil del equipo y hacer que permanezca libre de reparaciones. Existen dos tipos de mantenimiento:
  - Mantenimiento Preventivo: Se refiere a la revisión del equipo antes de que se presenten las fallas.
  - Mantenimiento Correctivo: Consiste en la reparación del computador después de alguna falla o mala manipulación del equipo.

Se deben tomar las siguientes consideraciones para el mantenimiento de los equipos: Período de mantenimiento adecuado y los registros de mantenimiento.

1.1.3.2.3 Factores

Según el diccionario de la Lengua Española los factores son los elementos o circunstancias que contribuye, junto con otras cosas, a producir un resultado.

Los factores que originan las vulnerabilidades en la seguridad informática son: Técnicos, Institucionales, ambientales y por malas decisiones administrativas. Ver anexo 2.

CAPITULO II. MARCO CONTEXTUAL

2.1 Aspectos Generales

2.1.1 Instituto Dominicano de las Telecomunicaciones INDOTEL

La historia del INDOTEL tuvo su origen a partir del 1995 con un proceso de concertación y colaboración entre el sector público y el privado, luego de este proceso el entonces Excelentísimo Señor Presidente de la República, Dr. Leonel Fernández Reyna promulga el 17 de mayo de 1998, la Ley General de Telecomunicaciones, No. 153-98, marcando un hito en la historia de las telecomunicaciones de la República Dominicana. Esta normativa sustituyó la anterior Ley de Telecomunicaciones No. 118, la cual databa del 1ro de febrero de 1966.

Los motivos que impulsaron la elaboración y aprobación de esta nueva Ley obedecieron a dos razones esenciales: primero, la necesidad de que la República Dominicana contara con un marco legal en consonancia con los acuerdos, convenios y tratados comerciales suscritos y ratificados por el país; y segundo, la imperiosa necesidad de disponer de una pieza legislativa que propiciara la promoción del servicio, el fomento de la libre y leal competencia en la oferta y el mejoramiento continuo, en precio y calidad de los servicios de telecomunicaciones que reciben los consumidores y usuarios dominicanos.

La Ley No. 153-98 estableció por vez primera, para la República Dominicana, reglas claras para el acceso y suministro de los servicios de telecomunicaciones, facilitando la presencia de una variada gama de aplicaciones y modalidades de servicios en la oferta, que dinamizan no sólo el mercado, sino también el desarrollo tecnológico.

Los objetivos de interés público y social contemplados en el artículo 2, de la Ley 153-98, son la base para la interpretación de las disposiciones contempladas en la misma ley y responden a:

a) Reafirmar el principio del servicio universal a través de:

i. La garantía, en áreas rurales y urbanas de bajos ingresos, de la posibilidad de acceso a un servicio mínimo y eficaz de telefonía, a precios asequibles, mediante el libre funcionamiento de los mercados y la utilización de los mecanismos previstos por esta ley;

ii. La satisfacción de la demanda de servicios públicos de telecomunicaciones en condiciones de libre competencia, asegurando la continuidad, generalidad, igualdad y neutralidad de dichos servicios; y

iii. El libre acceso a las redes y servicios públicos de telecomunicaciones en condiciones de transparencia y de no discriminación por parte de los prestadores y usuarios de servicios de telecomunicaciones, los generadores y receptores de información y los proveedores y usuarios de servicios de información;

b) Promover la prestación de servicios de telecomunicaciones con características de calidad y precio que contribuyan al desarrollo de las actividades productivas y de servicios en condiciones de competitividad internacional;

c) Garantizar el derecho del usuario a elegir el prestador del servicio de telecomunicaciones que a su criterio le convenga;

d) Ratificar el principio de la libertad de la prestación, por parte de titulares de concesiones obtenidas de acuerdo a la presente ley, de todo tipo de servicios públicos de telecomunicaciones, incluida la libertad de construcción y operación de sistemas y facilidades;

e) Promover la participación en el mercado de servicios públicos de telecomunicaciones de prestadores con capacidad para desarrollar una competencia leal, efectiva y sostenible en el tiempo, que se traduzca en una mejor oferta de telecomunicaciones en términos de precios, calidad de servicio e innovación tecnológica;

f) Asegurar el ejercicio, por parte del Estado, de su función de regulación y fiscalización de las modalidades de prestación, dentro de los límites de esta ley, de

modo imparcial, mediante la creación y desarrollo de un órgano regulador de las telecomunicaciones independiente y eficaz; y

g) Garantizar la administración y el uso eficiente del dominio público del espectro radioeléctrico.

2.1.1.1 Funciones

Según el artículo 76 de la Ley General de Telecomunicaciones No. 153-98 el INDOTEL es el órgano regulador de las telecomunicaciones, creado en virtud de la Ley General de Telecomunicaciones, No. 153-98, promulgada el 27 de mayo de 1998, el cual vela por el uso eficiente del espectro radioeléctrico; garantiza la existencia de una competencia leal, efectiva y sostenible de este mercado; defiende y hace efectivos los derechos de los usuarios; y promueve el desarrollo de las telecomunicaciones en la Republica Dominicana.

Sobre el INDOTEL recae la obligación de elaborar los reglamentos que complementan la Ley No.153-98 y de garantizar el fiel cumplimiento de las normas establecidas por la ley y por el órgano. El INDOTEL se caracteriza por su autonomía funcional, jurisdiccional y financiera, por su imparcialidad y porque está integrado por personas de incuestionable experiencia en el área de las telecomunicaciones y profesiones afines.

El primer Consejo Directivo del INDOTEL fue designado por decreto presidencial en abril de 1999, de conformidad con la Ley General de Telecomunicaciones No. 153-98. A través del Consejo Directivo se reafirma el compromiso asumido ante todos los usuarios de los servicios públicos de telecomunicaciones, de garantizar una correcta y justa interpretación del texto legal, como única vía para asegurar el cumplimiento cabal de los objetivos de desarrollo, equidad y justicia social que en él se plasman.

2.1.1.2 Misión

Promover el desarrollo de las telecomunicaciones implementando el principio del Servicio Universal para garantizar la existencia de una competencia sostenible, leal y efectiva en la prestación de los servicios públicos de telecomunicaciones, para defender y hacer efectivos los derechos de los clientes, usuarios y prestadores de los servicios de telecomunicaciónes además de velar por el uso eficiente del dominio público del espectro radioeléctrico en el país. (La misión se encuentra actualmente en revisión).

2.1.1.3 Visión

Ser una entidad eficiente y transparente con el fin de regular y promover la prestación de servicios de telecomunicaciones en beneficio de la sociedad, en un marco de libre, leal y efectiva competencia para el desarrollo de las comunicaciones en nuestro país. (La visión se encuentra actualmente en revisión).

2.1.1.4 Objetivos

Conforme al artículo 77 de la Ley General de Telecomunicaciones No.153-98 son los siguientes:

- Promover el desarrollo de las telecomunicaciones, implementando el principio del servicio universal definido por la Ley General de Telecomunicaciones No. 153-98.

- Garantizar la existencia de una competencia sostenible, leal y efectiva en la prestación de servicios públicos de telecomunicaciones.

- Defender y hacer efectivos los derechos de los clientes, usuarios y prestadores de dichos servicios, dictando los reglamentos pertinentes, haciendo cumplir las obligaciones correspondientes a las partes y, en su caso, sancionando a quienes no las cumplan, de conformidad con las

disposiciones contenidas en la presente Ley General de Telecomunicaciones No. 153-98 y sus reglamentos.

- Velar por el uso eficiente del dominio público del espectro radioeléctrico.

Según el Art. 77 de la Ley General de Telecomunicaciones No.153-98, las funciones del INDOTEL:

- Elaborar reglamentos de alcance general y dictar normas de alcance particular, dentro de las pautas establecidas por la Ley General de Telecomunicaciones No. 153-98.

- Regular aquellos servicios en los que la ausencia de competencia resulte perjudicial al usuario.

- Otorgar, ampliar y revocar concesiones y licencias en las condiciones previstas por la normativa vigente, permitiendo la incorporación de nuevos prestadores de servicios de telecomunicaciones.

- Prevenir o corregir prácticas anticompetitivas o discriminatorias, con arreglo a la Ley 153-98 y sus reglamentaciones.

- Reglamentar y administrar, incluidas las funciones de control, mediante las estaciones de comprobación técnica de emisiones que al efecto se instalen, el uso de recursos limitados en materia de telecomunicaciones, tales como el dominio público radioeléctrico, las facilidades de numeración, facilidades únicas u otras similares.

- Gestionar y administrar los recursos órbita espectro, incluida la gestión de las posiciones orbitales de los satélites de telecomunicaciones con sus respectivas bandas de frecuencias, así como las órbitas satelitales para satélites dominicanos que puedan existir y coordinar su uso y operación con organismos y entidades internacionales y con otros países.

- Dirimir, de acuerdo a los principios de la Ley General de Telecomunicaciones No. 153-98 y sus reglamentaciones y en resguardo del interés público, los diferendos que pudieran surgir entre los prestadores de servicios de Telecomunicaciones entre sí y con sus clientes o usuarios.

- Controlar el cumplimiento de las obligaciones de los concesionarios de servicios públicos de telecomunicaciones y de los usuarios del espectro radioeléctrico, resguardando en sus actuaciones el derecho de defensa de las partes.

- Fijar, cuando sea necesario, las tarifas de servicios al público y los cargos de interconexión, de acuerdo con la Ley General de Telecomunicaciones No. 153-98 y sus reglamentos.

- Administrar, gestionar y controlar el uso del espectro radioeléctrico, efectuando por sí o por intermedio de terceros la comprobación técnica de emisiones, la identificación, localización y eliminación de interferencias perjudiciales velando por que los niveles de radiación no supongan peligro para la salud pública.

- Aplicar el régimen sancionador ante la comisión de faltas administrativas previstas en la Ley General de Telecomunicaciones No. 153-98 y sus reglamentos.

- Administrar y gestionar los recursos de la CDT.

- Autorizar a los concesionarios de servicios públicos de telecomunicaciones que así lo soliciten, a que asuman la condición de signatarios de organismos internacionales de telecomunicaciones, de conformidad a las reglas aplicables, y, en su caso, coordinar la participación no discriminatoria de los concesionarios de servicios públicos de telecomunicaciones en los organismos internacionales de telecomunicaciones.

- Aprobar, previa consulta y coordinación con los interesados, y administrar los planes técnicos fundamentales de telecomunicaciones que la reglamentación establezca, otorgando plazos razonables para adecuarse a los mismos.

- Dictar normas técnicas que garanticen la compatibilidad técnica, operativa y funcional de las redes públicas de telecomunicaciones, la calidad mínima del servicio y la interconexión de redes. Dichas normas se adecuarán a las prácticas internacionales y a las recomendaciones de los organismos internacionales de que forme parte la República Dominicana.

- Elaborar especificaciones técnicas para la homologación de equipos, aparatos y sistemas de telecomunicaciones, así como expedir, en su caso, los correspondientes certificados de homologación.

- Administrar sus propios recursos.

- Ejercer las facultades de inspección sobre todos los servicios, instalaciones y equipos de telecomunicaciones. A estos efectos, los funcionarios de la inspección del órgano regulador tendrán, en el ejercicio de sus funciones, la condición de autoridad pública y deberán levantar acta comprobatoria de las mismas, las cuales harán fe de su contenido hasta prueba en contrario.

- Proponer al Poder Ejecutivo, mediante resolución motivada, el valor de las unidades de reserva radioeléctrica; y Garantizar en el “Plan nacional de atribución de frecuencias” la reserva de las bandas y frecuencias necesarias para los órganos de defensa nacional.

2.1.2 Provincia de Santo Domingo

El Distrito Nacional es una división político-administrativa especial donde se encuentra la capital de la República Dominicana y sede del Gobierno. Solamente tiene un municipio, el cual abarca toda la superficie del distrito, y su síndico actúa como gobernador provincial aunque es electo por los habitantes y no nombrado por

el Poder Ejecutivo. Al igual que en todas las provincias, sus habitantes eligen a un senador.La Provincia de Santo Domingo fue creada por la Constitución del 6 de noviembre de 1844. Pasó a ser Distrito Nacional en 1934.

2.1.2.1 Historia

La historia data desde la La Constitución del 6 de noviembre de 1844 creó, junto con otras 4 provincias, la Provincia de Santo Domingo, San Cristóbal, Baní, Los Llanos, Bayaguana, Monte Plata y Boyá. La Ley No. 355 del 5 de septiembre de 1854 sobre "Administración Provincial" le dió el nombre de Provincia de Santo Domingo de Guzmán, nombre que volvió a ser simplemente Provincia de Santo Domingo en las constituciones y leyes posteriores.

Las posteriores divisiones territoriales del país fueron creando nuevas provincias, reduciendo el territorio de la provincia. Por la Ley No. 391 del 11 de noviembre de 1932 pasó a llamarse Provincia Nacional.

El 7 de septiembre de 1934 se dispuso la creación del Distrito Nacional; la nueva demarcación quedó inaugurada el 1 de enero de 1935. Ya que el Distrito Nacional solamente tendría un municipio, las demás comunidades del territorio del distrito y que eran municipios, como San Antonio de Guerra, dejaron de serlo. El 15 de enero de 1936 fue promulgada la ley que le cambió el nombre a Distrito de Santo Domingo. Fue denominada definitivamente como Distrito Nacional por la Constitución del 1 de diciembre de 1955.

El último cambio fue en el año 2001, cuando se creó la actual Provincia de Santo Domingo y el territorio del Distrito Nacional quedó reducido a la ciudad de Santo Domingo de Guzmán.

2.1.2.2 División Geopolítica de la provincia

Santo Domingo o Provincia Santo Domingo es una de las 31 provincias de la República Dominicana. Fue separada del Distrito Nacional por ley del 16 de octubre de 2001. Nombrada por la ciudad de Santo Domingo de Guzmán, capital del país.

A partir del 20 de junio 2006, la provincia se divide en los siguientes municipios y distritos municipales:

- Boca Chica
- La Caleta
- Los Alcarrizos
- Palmarejo-Villa Linda
- Pantoja
- Pedro Brand
- La Cuaba
- La Guáyiga
- San Antonio de Guerra
- Hato Viejo
- San Luis
- Santo Domingo Este
- Santo Domingo Norte
- La Victoria
- Santo Domingo Oeste

2.1.2.3 Superficie

Posee una superficie de 1,297.60 kilómetros cuadrados. Está en el 16vo lugar en cuanto a superficie con un 2.7% del territorio nacional.

2.1.2.4 Límites

La provincia de Santo Domingo limita al norte con la provincia Monte Plata, al este con la provincia San Pedro de Macorís, al sur con el Mar Caribe y al oeste con la provincia San Cristóbal.

2.1.2.5 Geografía e Hidrología

En el norte de la provincia se encuentra la Sierra Prieta, que forma parte de la Sierra de Yamasá.

El principal río de la provincia es el Ozama, con sus grandes afluentes La Isabela y Yabacao. El Río Haina forma el límite con la provincia San Cristóbal mientras que el Brujuelas sirve de límite con la provincia San Pedro de Macorís.

2.1.2.6 Población

Al 2012 la población total era de 2, 995, 211, con una densidad de 1,829.8 habitantes/km^2,el porcentaje de población urbana 87.8%, siendo la ciudad más poblada: Santo Domingo Este, con población urbana de 851,853 habitantes.

Esta es la provincia más pujante de la República Dominicana, en gran medida porque en ella se encuentran dos de los aeropuertos más importantes del país, el Aeropuerto Internacional de Las Américas y Aeropuerto Internacional La Isabela. Los puertos más importantes del país tales como, el Puerto de Haina, y el Multimodar Caucedo.

El territorio de esta provincia es bastante fértil en toda su geografía, destacándose los ríos, Ozama, Haina, e Isabela. Limita con las provincias de Monte Plata al norte, San Cristóbal al oeste, San Pedro de Macorís al este, y con el mar Caribe al sur.

CAPITULO III. METODOLOGIA Y PRESENTACION DE LOS RESULTADOS

3.1 Análisis de los datos

El objetivo de este capítulo es relacionar los datos extraídos de las entrevistas con los indicadores y de esta forma comparar las respuestas y ajustarlas a las necesidades del estudio.

Se entrevistaron solo personal de la Gerencia de Tecnología de la Información y Comunicación, del INDOTEL incluidos el Gerente, Encargado de Redes, Analista de Redes y Soporte de Infraestructura. Con la finalidad de analizar los indicadores correspondientes a las variables extraídas de los objetivos específicos.

3.1.1 Herramientas Tecnológicas

A continuación se presentarán los indicadores de esta variable con la finalidad de responder de manera adecuada el objetivo específico.

3.1.1.1 Recursos

La pregunta correspondiente a este indicador fue:

¿Cuáles son los recursos que son utilizadas por la Gerencia de Tecnología de la Información y Comunicación para mantener la seguridad en informática?

Según el encargado de la infraestructura los recursos que son utilizados para mantener la seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación son firewall, IPS, Sniffer, System Operation Manager, Cisco SDM, Forefront como antivirus y para el sistema de backup se utiliza el System Center Data Protector Manager. De igual modo el soporte técnico de la infraestrura agregó que otras herramientas tecnológicas son la políticas de restricciones y los permisos administrativos, mientras que el analista de la infraestructura respondió añadiendo los siguientes recursos: DHCP snopping en

todos los switches, VLAN's, access list, SSH para conexión remota, VPN. Sistema de acceso biométrico y cámaras de seguridad IP.

3.1.1.2 Software

La pregunta correspondiente a este indicador fue:

¿Cuáles son los softwares que facilitan la gestión y control de todos los elementos informáticos de la organización?

Según el encargado de infraestructura el software que facilita la gestión y el control de todos los elementos informáticos es el Operation Manager, de ese mismo modo el soporte técnico agregó que además del Operation Manager se encuentra el Sistema de Gestion Interna (SGI), así como también el Dame ware, mientras que el analista de infraestructura dijo que cuentan con el Microsoft System Center Virtual Machine.

3.1.1.3 Hardware

La pregunta correspondiente a este indicador fue:

¿Es suficiente el hardware que posee la Gerencia de Tecnología de la Información para llevar a cabo la seguridad informática eficientemente en el INDOTEL?

Todos coincidieron que el hardware que posee la Gerencia de Tecnología de la Información y Comunicación no es suficiente, para llevar a cabo la seguridad informática eficientemente.

3.1.1.4 Gestión

La pregunta correspondiente a este indicador fue:

¿Facilitan las herramientas tecnológicas utilizadas por la Gerencia de Tecnología de la Información y Comunicación los procesos de gestión de la seguridad informática?

El 75 % de los entrevistados entienden que las herramientas tecnológicas utilizadas en la Gerencia de Tecnología de la Información facilitan los procesos de gestión, mientras que el resto opinó que entiende que no todas.

3.1.1.5 Documentación

La pregunta correspondiente a este indicador fue:

¿Existe en la Gerencia de Tecnología de la Información y Comunicación, la documentación necesaria para el control y los registros, que ayuden a realizar la labor diaria?

Todos los entrevistados coinciden en que en la actualidad no existe en la Gerencia de Tecnología de la Información y Comunicación ninguna documentación que se encuentre disponible para el control y los registros de las eventualidades.

3.1.2 Políticas de seguridad

A continuación se presentarán los indicadores de esta variable con la finalidad de responder de manera adecuada dicho objetivo específico.

3.1.2.1 Áreas de Normalización

La pregunta correspondiente a este indicador fue:

¿Cuáles áreas debe abarcar una política de seguridad, en la Gerencia de Tecnología de la Información y Comunicación?

Todos los entrevistados coincidieron que las áreas que debe abarcar una política de seguridad son tanto la seguridad física, como la seguridad lógica.

3.1.2.2 Elementos que conforman una política de segurida

La pregunta correspondiente a este indicador fue:

¿Qué elementos son vitales, al momento de definir una política de seguridad informática en la Gerencia de Tecnología de la Información y Comunicación?

Está pregunta no se aplica, ya que no existe ninguna Política de Seguridad en la Gerencia de Tecnología de la Información y Comunicación**.**

3.1.2.3 Procedimientos

La pregunta correspondiente a este indicador fue:

¿Existen procedimientos de Seguridad Informática en la Gerencia de Tecnología de la Información y Comunicación del INDOTEL?

Todos los entrevistados coincidieron en que en la Gerencia de Tecnología de la Información y Comunicación no existe ningún procedimiento de seguridad informática. Solo existe un procedimiento que está relacionado al mantenimiento correctivo y preventivo. Ver anexo 3.

3.1.3 Amenazas y Vulnerabilidades

A continuación se presentarán los indicadores de esta variable con la finalidad de responder de manera adecuada el objetivo específico.

3.1.3.1 Tipos de Amenzas

La pregunta correspondiente a este indicador fue:

¿Cuáles son los tipos de amenazas a los cuales la seguridad en informática se ve atentada?

Todos los entrevistados coincidieron que las amenazas a los cuales la seguridad informática se encuentra atentada son básicamente los cyber attack, denial of service, access point falsos, phishing, malware y virus.

3.1.3.2 Categorización

La pregunta correspondiente a este indicador fue:

¿Existe alguna categorización de las amenazas que enfrenta la seguridad en informática de la Gerencia de Tecnología de la Información y Comunicación del INDOTEL, de existir, podría decir cuáles son?

El encargado de Infraestructura expresó que no tienen una categorización como tal, pero que consideran que el cyber attack es crítico, sin embargo los demás entrevistados claramente expresaron que no hay categorización vigente en la Gerencia de Tecnología de la Información y Comunicación para las amenazas.

3.1.3.3 Riesgos

La pregunta correspondiente a este indicador fue:

¿Cuáles son los riesgos más frecuentes los que se ha enfrentado la seguridad informática de la Gerencia de Tecnología de la Información y Comunicación, del INDOTEL?

Según el encargado de infraestructura y el soporte técnico los riesgos más frecuentes son los cyber attack al portal web y al correo electrónico, así como también han sufrido ARP poison y Man in the Midldle, de igual forma el analista de la infraestructura agregó que otro riesgo son las aplicaciones usadas para romper la política de seguridad o bloqueo web, permitiendo esto la entrada a la red de la institución de virus, malware, troyanos y los denies of services.

3.1.3.4 Factores

La pregunta correspondiente a este indicador fue:

¿Cuáles factores son los que originan con mayor frecuencia las vulnerabilidades de seguridad en informática?

Todos los entrevistados coincidieron que los factores que originan con mayor frecuencia las vulnerabilidades de seguridad en informática son máquinas infectadas, usuarios mal intencionados externos, la aparición de ejecutables sin que el antivirus corporativo lo catalogue como archivo indeseado.

CONCLUSIONES

Las conclusiones del objetivo específico No. 1: Identificar las herramientas tecnológicas de la Gerencia de Tecnología de la Información y Comunicación del Instituto Dominicano de las Telecomunicaciones INDOTEL, Santo Domingo, República Dominicana**,** son las siguientes:

Los resultados de ésta entrevista han evidenciado que:

Los recursos que son utilizados para mantener la seguridad informática son: firewall, IPS, Sniffer, System Operation Manager, Cisco SDM, forefront como antivirus para el sistema de backup, políticas de restricciones, los permisos administrativos, DHCP snopping en todos los switches, Vlans, Access List, SSH para conexión remota, VPN, sistema de acceso biométrico y cámaras de Seguridad IP.

Los softwares que facilitan la gestión y el control de todos los elementos informáticos son: el Operation Manager, Sistema de Gestion Interna SGI, el Dame ware y el Microsoft System Center Virtual Machine.

El hardware que posee la Gerencia de Tecnología de la Información y Comunicación no es suficiente para llevar a cabo la seguridad informática de manera eficiente.

La Gestión a través de las herramientas tecnológicas de los procesos de la seguridad informática, según el 75% es eficaz, mientras que el resto entiende que no.

La Documentación necesaria para el control y los registros que ayudarían a la labor diaria para la seguridad informática, en la Gerencia de Tecnología de la Información y Comunicación no existe en la actualidad**.**

Las conclusiones del objetivo específico No. 2: Identificar las políticas de seguridad en informática aplicadas por la Gerencia de Tecnología de la Información y Comunicación del Instituto Dominicano de las Telecomunicaciones INDOTEL, Santo Domingo, República Dominicana**,** son las siguientes:

Los resultados de esta entrevista han evidenciado que:

Las Áreas de Normalización que debe abarcar una política de seguridad son la seguridad física y la seguridad lógica.

Los Elementos que conforman una política de seguridad no se pudieron determinar ya que en la actualidad la Gerencia de Tecnología de la Información y Comunicación no tiene diseñada ni contemplada una política de seguridad.

Los Procedimientos no se pudieron desvelar ya que en la actualidad en la Gerencia de Tecnología de la Informacion y Comunicación no existen procedimientos de seguridad informática, sino que sólo existe un procedimiento que está relacionado al mantenimiento correctivo y preventivo utilizado para la certificación ISO 27000. Ver anexo 3.

Las conclusiones del objetivo específico No. 3: Identificar las amenazas y vulnerabilidades que enfrenta la seguridad en informática de la Gerencia de Tecnología de la Información y Comunicación del Instituto Dominicano de las Telecomunicaciónes INDOTEL, Santo Domingo, República Dominicana**,** son las siguientes:

Los resultados de esta entrevista han evidenciado que:

Los Tipos de Amenazas a los cuales la seguridad en informática se ve atentada según el resultado extraído de las entrevista son: los cyber attack, denial of service, access point falsos, phishing, malware y virus.

La Categorización de las amenazas a la seguridad informática no está definida en la Gerencia de Tecnología de la Información y Comunicación.

Los Riesgos más frecuentes los que se ha enfrentado la seguridad informática de la Gerencia de Tecnología de la Información y Comunicación según los datos obtenidos a través de las entrevistas fueron: los cyber attack a sus portales web y al correo electránico, ARP Poison, Man in the Midldle, las aplicaciones usadas para romper la política de seguridad o bloqueo web, por lo que esto permite la entrada a la red institucional de cualquier virus, malware, troyanos y los denies of services (DoS).

Los Factores que originan con mayor frecuencia las vulnerabilidades de la seguridad en informática en la Gerencia de Tecnología de la Informacion y Comunicación según los entrevistados son las máquinas infectadas, los usuarios mal intencionados externos y la aparición de ejecutables sin que el antivirus corporativo lo catalogue como archivo indeseado.

RECOMENDACIONES

Tomando en cuenta las conclusiones realizadas por objetivos, los cuales sirvieron guía y marco de referencia para esta investigación acerca del “Análisis de los procesos de seguridad informática en la Gerencia de Tecnología de la Información y Comunicación del Instistuto Dominicano de las Telecomunicaciónes INDOTEL, en la ciudad de Santo Domingo”, se formularán las siguientes recomendaciones:

A los ingenieros de Infraestructura de Red de la Gerencia de Tecnología de la Información y Comunicación en el área de Seguridad Informática del INDOTEL:

- Hacer un levantamiento del hardware que hace falta en el área de la seguridad informática en la Gerencia de Tecnología de la Información y Comunicación, para que, de esta forma lo adquieran y logren un mejor desempeño.

- La Gerencia de Tecnología de la Información y Comunicación no debe escatimar esfuerzos para que exista la documentación necesaria en el área de infraestructura (bitacóras, registros diarios) que asegure el control y los registros, para realizar con eficacia, eficiencia y productividad la labor diaria.

- Todas las herramientas tecnológicas que sean utilizadas en la Gerencia de Tecnología de Infromación y Comunicación deben estar orientadas además a facilitar los procesos de gestión de la seguridad Informática.

- La Alta Dirección, conjuntamente con la Gerencia de Tecnología de la Información y Comunicación deben diseñar una política de seguridad la cual consista en un conjunto de directrices, normas , procedimientos que guien las instrucciones de trabajo y que definan los criterios de seguridad con el único objetivo de establecer, estandarizar y normalizar la seguridad

tecnológica. Teniendo esto por objeto concientizar acerca de la importancia y los servicios de la plataforma tecnológicas que sean críticos, requiriendo a la familia INDOTEL su fiel cumplimiento.

- Los elementos vitales que debería de tomarse en cuenta al momento de definir la política de seguridad son: alcance de la política, objetivos de la política, responsabilidades de todos los servicios y recursos informáticos, definiciones de violaciones y sanciones, responsabilidades del usuario por el acceso, redacción clara de la política y una actualización periódica de la misma.

- La Gerencia de Tecnología de la Información y Comunicación debe diseñar los procedimientos dentro de la política de seguridad.

- El área de Infraestuctura de Red debe tener una categorización de las amenazas, llevándose de los parámetros de las normas de seguridad, basándose en la Norma ISO 17799.

- Se deben realizar auditorías de seguridad en las cuales se contemple los análisis de riesgo, revisiones periódicas, visitas técnicas y monitoreo constante a la parte de infraestructura de red de la Gerencia de Tecnología de la Información y Comunicación.

- Deben tener una visión más clara sobre sus vulnerabilidades y de los esfuerzos que debe hacer la Gerencia de Tecnología de la Información para mejorar la parte de seguridad tecnológica.

- La Gerencia de Tecnología de la Información y Comunicación deberá asegurar el uso eficiente de los recursos informáticos, orientándolos al logro de los objetivos y las estrategias de la organización.

- La Gerencia de Tecnología de la Información y Comunicación deberá desarrollar un Plan de Contigencia para garantizar la continuidad de los servicios frente algún contingente.

REFERENCIAS BIBLIOGRAFICAS

Alvarez Marañon, G, (2000). IEC. Recuperado el 01 de Abril de 2013 http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html

Bernal, C. (2000). Metodología de la Investigación. (1era. Edición). Colombia: Pearson-Prentice Hall.

Distrito Nacional. Recuperado el 03 de abril de 2013, de http://www.jmarcano.com/mipais/geografia/province/prov_dn.html

Distrito Nacional. Recuperado el 04 de abril de 2013, de http://es.wikipedia.org/wiki/Distrito_Nacional

García, A, (2011) Seguridad Informática, (Madrid, España: Paraninfo, 2011) pág. 22Ibid. Pág. 15-29.

Hernández, F (2001). Investigación Documental y Comunicación Científica. Santo Domingo, República Dominicana: Búho.

Hernández, R. (2001). Metodología de la Investigación, 2da. Edición. Brazil: McGraw-Hill Interamericana Editores, S.A.

Kenneth C. Laudon y Jane P. Laudon,Prentice Hall . Administración de los Sistemas de Información, Organización y Tecnología, Tercera Edición, Hispanoamericana S.A., Impreso en México Copyright MCMXCIV. Pag: 702, 703, 704.

Norton, P.Introducción a la Computación, 1era Edición, Mc Graw Hill pág: 50, 52,53.

Pujol, Mª E. (1997) Documentación y periodismo. Pamplona: Eunsa

Royer, J (2004), Seguridad en la informática de la empresa, (Barcelona: ENI,) pág. 11-12.

Santo Domingo. Recuperado el 15 de abril de 2013, de http://es.wikipedia.org/wiki/Santo_Domingo_(provincia)

Schneier, B, Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas. Secrets & Lies. Página 28-29.

Tecpoyotl, J. (2012). DCYC. Recuperado el 12 de Marzo de 2013 http://www.dcyc.ipn.mx/wps/wcm/connect/dcyc/IPN/Inicio/SERVICIOS/DIVISION_DE_COMPUTO/DEPARTAMENTO_DE_SEGURIDAD/INDEX.HTM

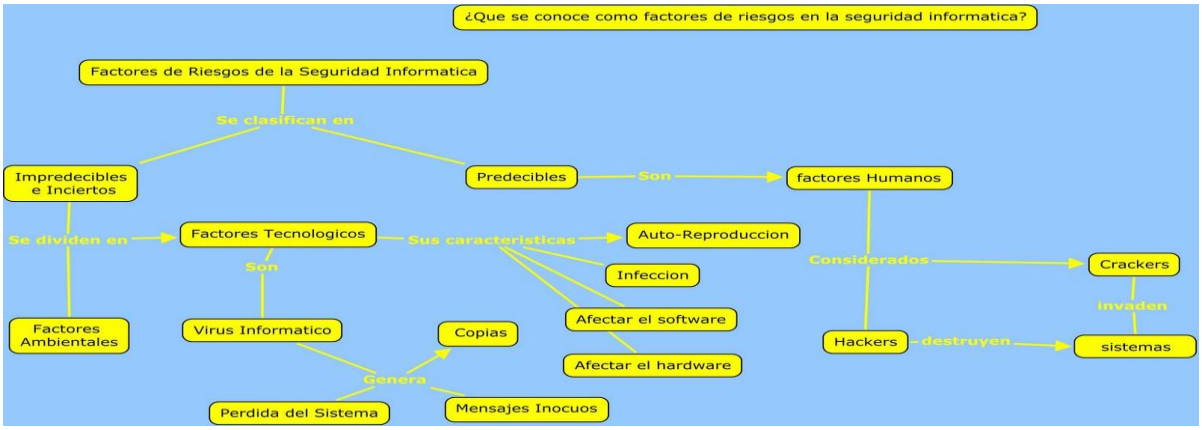
Telles Váldez, J. (1996) Derecho Informático. 2° Edición. Mc Graw Hill. México.

ANEXO

Anexo 1. **Amenazas humanas maliciosas**

Suplantación	• Falsificar mensajes de correo electrónico • Reproducir paquetes de autenticación
Alteración	• Alterar datos durante la transmisión • Cambiar datos en archivos
Repudio	• Eliminar un archivo esencial y denegar este hecho • Adquirir un producto y negar posteriormente que se ha adquirido
Divulgación de información	• Exponer la información en mensajes de error • Exponer el código de los sitios Web
Denegación de servicio	• Inundar una red con paquetes de sincronización • Inundar una red con paquetes ICMP falsificados
Elevación de privilegios	• Explotar la saturación de un búfer para obtener privilegios en el sistema • Obtener privilegios de administrador de forma ilegítima

Anexo 2. **Factores de riesgo de la seguridad informática**



Anexo 3. **Procedimiento mantenimiento preventivo y correctivo de la infraestructura informática.**

EMISION	ELABORO	REVISO	APROBO
NOMBRE:	Maika Santana	Annia Portela	Leovigildo Gómez
CARGO:	Soporte Técnico	Sub Encargada de Gestión de Calidad	Gerente de Tecnología de la Información y Comunicación
FIRMA:			
FECHA:			

1. PROPOSITO

Mantener en buen estado la infraestructura informática asegurando de esa forma el correcto funcionamiento de la misma.

2. ALCANCE

Desde que se realiza el levantamiento de la infraestructura informática que necesita mantenimiento preventivo hasta que es programado y realizado.

Desde que se recibe una solicitud informando un problema en la infraestructura informática hasta que la misma es atendida y solucionada.

3. DEFINICIONES

SGI: Sistema de Gestión Interna, es una herramienta que permite mantener el control de los documentos
entrantes y salientes.

4. DESCRIPCION DEL PROCEDIMIENTO

LEVANTAMIENTO DE LA INFRAESTRUCTURA INFORMATICA

RESPONSABLE	ACTIVIDADES Y DIRECTRICES	DOCUMENTOS APLICABLES
Gerente de Tecnología de la Información y Comunicación	**4.1 Levantamiento de la Infraestructura Informática:** 4.1.1 Solicita al Coordinador de Soporte Técnico la realización de un inventario de la infraestructura informática de la institución.	
Coordinador de Soporte Técnico	4.1.2 Coordina con los Soportes Técnicos la realización del levantamiento del inventario de la infraestructura informática de la institución.	
Soportes Técnicos	4.1.3 Realizan el inventario y proporcionan la información al Coordinador de Soporte Técnico.	

Coordinador de Soporte Técnico	4.1.4 Completa la información del inventario en el "Listado Infraestructura Informática" y coloca en el SharePoint. **Nota:** • Cada vez que se adquiera o se elimine algún equipo de la infraestructura informática el Coordinador de Soporte Técnico debe actualizar el "Listado Infraestructura Informática".	Listado Infraestructura Informática

MANTENIMIENTO PREVENTIVO DE LA INFRAESTRUCTURA INFORMATICA

RESPONSABLE	ACTIVIDADES Y DIRECTRICES	DOCUMENTOS APLICABLES
Encargado de Redes e Infraestructura	**4.2 Mantenimiento Preventivo:** 4.2.1 Verifica el Listado y realiza anualmente el "Programa Mantenimiento Preventivo de la Infraestructura Informática" y remite al Gerente de Tecnología de la Información y Comunicación.	INF-PROG-001
Gerente de Tecnología de la Información y Comunicación	4.2.2 Verifica y aprueba el "Programa Mantenimiento Preventivo de la Infraestructura Informática" y devuelve al Encargado de Redes e Infraestructura. 4.2.3 Distribuye a los involucrados para su conocimiento. 4.2.3 Define cuáles son los servicios críticos, que en caso de ocurrir generarían un caos en la institución.	INF-PROG-001
Encargado de Redes e Infraestructura	4.2.3 Recibe y verifica que los mantenimientos automatizados se realicen según lo que estipula el Programa y si se presenta algún problema que no puede solucionar ir al paso 4.2.6.2. 4.2.4 Asigna la verificación del funcionamiento de los servicios críticos en los servidores al Soporte Técnico de su Departamento.	
Soporte Técnico	4.2.5 Realiza diariamente una revisión básica de los servicios críticos en los servidores, para verificar su funcionamiento: 4.2.5.1 Si están funcionando, toma un screenshot de los servicios y remite a través de correo electrónico al Encargado de Redes e Infraestructura y al Gerente de Tecnología de la Información y Comunicación. 4.2.5.2 Si alguno no está funcionando, verifica el problema: 4.2.5.2.1 Si lo puede solucionar, lo hace y toma un screenshot del o los servicios críticos y remite a través de correo electrónico al Encargado de Redes e Infraestructura y al Gerente de Tecnología de la Información y Comunicación; termina el proceso. 4.2.5.2.2 Si no lo puede solucionar, informa al Encargado de Redes e Infraestructura.	
Encargado de Redes e Infraestructura	4.2.6 Recibe la información y verifica el problema: 4.2.6.1 Si lo puede solucionar, lo hace y toma un screenshot del o los servicios críticos y remite a través de correo electrónico al Gerente de Tecnología de la Información y Comunicación; termina el proceso. 4.2.6.2 Si no lo puede solucionar verifica: 4.2.6.2.1 Si el problema lo cubre el contrato de Microsoft, se comunica	

	con ellos y le notifica lo que sucede; ir al paso 4.2.8. 4.2.6.2.2 Si no lo cubre el contrato, informa al Gerente de Tecnología de la Información y Comunicación, envía un Memorando con la solicitud al Encargado de Logística vía el Gerente Administrativo para que sea contratado un Soporte Externo.	
Soporte Externo	4.2.7 Se presenta en la institución, realiza el arreglo e informa al Encargado de Redes e Infraestructura.	
Encargado de Redes e Infraestructura	4.2.8 Revisa el trabajo, verifica que la infraestructura informática esté funcionando correctamente y notifica al Gerente de Tecnología de la Información y Comunicación. 4.2.9 Informa al Departamento de Logística la conclusión del trabajo.	

MANTENIMIENTO CORRECTIVO DE LA INFRESTRUCTURA INFORMATICA

RESPONSABLE	ACTIVIDADES Y DIRECTRICES	DOCUMENTOS APLICABLES
Empleado	**4.3 Detección de problema:** 4.3.1 Detecta un problema en la infraestructura informática y lo reporta a través de un correo electrónico dirigido a Soporte Técnico o una llamada telefónica.	Correo Electrónico
Coordinador de Soporte Técnico	4.3.2 Diariamente verifica en el buzón de llamadas y el correo electrónico los soportes solicitados. 4.3.3 Selecciona un Soporte Técnico, asigna el trabajo y remite de manera electrónica. Si el soporte solicitado es sobre una línea telefónica o el Sharepoint, informa al Administrador Central PBX de Redes e Infraestructura.	
Soportes Técnicos	4.3.4 Reciben el correo y el soporte seleccionado, registra el caso en el Sistema de Gestión Interna (SGI). 4.3.5 Contacta al empleado por teléfono, vía correo o de manera personal para realizar el soporte. 4.3.6 Una vez concluido el soporte, contacta al empleado para notificárselo. 4.3.7 Informa al Coordinador de Soporte Técnico y concluye el caso en el Sistema de Gestión Interna (SGI).	
Coordinador de Soporte Técnico	4.3.8 Completa y remite al empleado el "Formulario Evaluación del Mantenimiento" de manera electrónica y le solicita que evalúe el soporte que le fue dado.	SG-F-001
Empleado	**4.4 Evaluación Soporte Recibido:** 4.4.1 Imprime el "Formulario Evaluación del Mantenimiento" evalúa el trabajo, firma y devuelve al Coordinador de Soporte Técnico.	SG-F-001
Coordinador de Soporte Técnico	4.4.2 Recibe, analiza, informa al Soporte Técnico el resultado de su evaluación para tomar las acciones que sean necesarias y almacena. 4.4.3 Mensualmente remite al Gerente de Tecnología de la Información y Comunicación los resultados de las evaluaciones que fueron realizadas durante el mes; termina el proceso.	
Coordinador	**4.5 Avisos de alertas cuando las tintas de las impresoras se estén agotando:**	

de Soporte Técnico	4.5.1 Determina los usuarios que van a recibir las alertas cuando los tóner de las impresoras de sus áreas se estén terminando. 4.5.2 Configura en el sistema de impresoras los usuarios que van a recibir las alertas y se los notifica mediante un correo electrónico.	Correo Electrónico

5. REFERENCIAS

5.1 Norma ISO 9001:2008, cláusula 6.3.

6. REGISTROS DE CALIDAD

6.1 Listado Infraestructura Informática.

6.2 Programa Mantenimiento Preventivo de la Infraestructura Informática (INF-PROG-001).

6.3 Correo Electrónico.

6.4 Formulario Evaluación del Mantenimiento (SG-F-001).

Anexo 4**. Entrevistas**

Entrevista A

Dirigido a: Francis Batista

Puesto: Encargado de la Infraestructura de Red

Institución: Instituto Dominicano de las Telecomunicaciones

Saludos

Mi nombre es Maika Sivelth Rodríguez Pérez soy estudiante de la Maestría Gerencia y Productividad de la Escuela de Graduados de UNAPEC (Recinto Santiago), el objetivo de ésta entrevista es conocer más a fondo los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes (INDOTEL), en la ciudad de Santo Domingo, Rep. Dom. Su opinión a estas diversas preguntas me ayudará a evaluar diferentes puntos de vistas:

¿Cuáles son las herramientas tecnológicas que son utilizadas por la Gerencia de Tecnología de la Información y Comunicación para mantener la seguridad en informática?

A nivel de hardware tenemos firewall, IPS y en cuanto a software se refiere tenemos el Cisco Center Operation Manager, Cisco SDM, el Forefront como antivirus, para la parte de backup utilizamos el System Center Data Protection Manager (Solo para los servidores y se realiza diario).

¿Cuáles son los softwares que facilitan la gestión y control de todos los elementos informáticos de la organización?

El software que facilita la gestión y control de todos los elementos informáticos de la organización es: Microsoft system center operation manager.

¿Facilitan las herramientas tecnológicas utilizadas por la Gerencia de Tecnología de la Información y Comunicación los procesos de gestión de la seguridad informática?

Si (pero no todos)

¿Es suficiente el hardware que posee la Gerencia de Tecnología de la Información para llevar a cabo la seguridad informática eficientemente en el INDOTEL?

No

¿Existe en la Gerencia de Tecnología de la Información y comunicación, la documentación necesaria para el control y los registros, que ayuden a realizar la labor diaria?

No

¿Qué elementos son vitales, al momento de definir una política de seguridad informática en la Gerencia TIC?

N/A

¿Cuáles áreas debe abarcar una política de seguridad, en la Gerencia de Tecnología de la Información y Comunicación?

Seguridad Física y Seguridad Lógica.

¿Cuáles son los tipos de amenazas a los cuales la seguridad en informática se ve atentada?

- Cyber Attack
- DoS
- Pishing
- Access Point falsos

¿Existe alguna categorización de las amenazas que enfrenta la seguridad en informática del departamento TIC del INDOTEL, de existir, podría decir cuáles son?

No

¿Cuáles son los riesgos más frecuentes los que se ha enfrentado la seguridad informática de la Gerencia de Tecnología de la Información y Comunicación, del INDOTEL?

- Hackeo a los portales y al correo
- ARP Poison

¿Cuáles factores son los que originan con mayor frecuencia las vulnerabilidades de seguridad en informática en el INDOTEL?

- Máquinas infectadas
- Usuarios mal intencionados

.

Entrevista B

Dirigido a: Gregory Rodríguez

Puesto: Soporte Técnico

Institución: Instituto Dominicano de las Telecomunicaciones

Saludos

Mi nombre es Maika Sivelth Rodríguez Pérez soy estudiante de la Maestría Gerencia y Productividad de la Escuela de Graduados de UNAPEC (Recinto Santiago), el objetivo de ésta entrevista es conocer más a fondo los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes (INDOTEL), en la ciudad de Santo Domingo, Rep. Dom. Su opinión a estas diversas preguntas me ayudará a evaluar diferentes puntos de vistas:

¿Cuáles son las herramientas tecnológicas que son utilizadas por la Gerencia de Tecnología de la Información y Comunicación para mantener la seguridad en informática?

Las herramientas tecnológicas utilizadas son: Forefront, firewall, políticas de restrinciones a la red y los permisos administrativos.

¿Cuáles son los softwares que facilitan la gestión y control de todos los elementos informáticos de la organización?

Los softwares que facilitan la gestión y control de todos los elementos informáticos de la organización:

- Sistema de Gestión Interna SGI
- Dameware

¿Facilitan las herramientas tecnológicas utilizadas por la Gerencia de Tecnología de la Información y Comunicación los procesos de gestión de la seguridad informática?

Sí

¿Es suficiente el hardware que posee la Gerencia de Tecnología de la Información para llevar a cabo la seguridad informática eficientemente en el INDOTEL?

No

¿Existe en la Gerencia de Tecnología de la Información y comunicación, la documentación necesaria para el control y los registros, que ayuden a realizar la labor diaria?

No

¿Qué elementos son vitales, al momento de definir una política de seguridad informática en la Gerencia de Ténología de la Información y Comunicación?

N/A

¿Cuáles áreas debe abarcar una política de seguridad, en la Gerencia de Tecnología de la Información y Comunicación?

Seguridad Física y Seguridad Lógica

¿Cuáles son los tipos de amenazas a los cuales la seguridad en informática se ve atentada?

- Hackeo
- Pishing

¿Existe alguna categorización de las amenazas que enfrenta la seguridad en informática del departamento TIC del INDOTEL, de existir, podría decir cuáles son?

No

¿Cuáles son los riesgos más frecuentes los que se ha enfrentado la seguridad informática de la Gerencia de Tecnología de la información y Comunicación, del INDOTEL?

- Hackeo a la página web.

¿Cuáles factores son los que originan con mayor frecuencia las vulnerabilidades de seguridad en informática del INDOTEL?

- Usuarios mal intencionado
- Introducen a la red hardware externo infectado

Entrevista C

Dirigido a: José Raúl Madera Oropeza

Puesto: Analista de la Infraestructura

Institución: Instituto Dominicano de las Telecomunicaciones

Saludos

Mi nombre es Maika Sivelth Rodríguez Pérez soy estudiante de la Maestría Gerencia y Productividad de la Escuela de Graduados de UNAPEC (Recinto Santiago), el objetivo de ésta entrevista es conocer más a fondo los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes (INDOTEL), en la ciudad de Santo Domingo, Rep. Dom. Su opinión a estas diversas preguntas me ayudará a evaluar diferentes puntos de vistas:

¿Cuáles son las herramientas tecnológicas que son utilizadas por la Gerencia de Tecnología de la Información y Comunicación para mantener la seguridad en informática?

Las herramientas tecnológicas utilizadas son:

- Network Access control(802.1x)
- Dhcp snopping on all switchs
- Vyatta firewall
- Vlans
- Access list
- Ssh for remote access
- Aaa model para acceso a los equipos de red.
- Vpn
- Microsoft TMG.
- Sistema de control de acceso biométrico.
- Cámaras de seguridad cctv e Ip.

¿Cuáles son los softwares que facilitan la gestión y control de todos los elementos informáticos de la organización?

Los softwares que facilitan la gestión y control de todos los elementos informáticos de la organización:

- Microsoft system center operation manager.
- Microsoft system center virtual machine manager.

¿Facilitan las herramientas tecnológicas utilizadas por la Gerencia de Tecnología de la Información y Comunicación los procesos de gestión de la seguridad informática?

No

¿Es suficiente el hardware que posee la Gerencia de Tecnología de la Información y Comunicación para llevar a cabo la seguridad informática eficientemente en el INDOTEL?

No

¿Existe en la Gerencia de Tecnología de la Información y comunicación, la documentación necesaria para el control y los registros, que ayuden a realizar la labor diaria?

No

¿Qué elementos son vitales, al momento de definir una política de seguridad informática en la Gerencia de la Tecnología de la Información y Comunicación?

N/A

¿Cuáles áreas debe abarcar una política de seguridad, en la Gerencia de Tecnología de la Información y Comunicación?

Desde acceso físicos a determinadas áreas, hasta acceso digital a diversos entornos informáticos (aplicaciones, web, etc.).

¿Cuáles son los tipos de amenazas a los cuales la seguridad en informática se ve atentada?

- Virus
- Malware
- Ataques a la página web(ddos)

¿Existe alguna categorización de las amenazas que enfrenta la seguridad en informática del departamento TIC del INDOTEL, de existir, podría decir cuáles son?

No

¿Cuáles son los riesgos más frecuentes los que se ha enfrentado la seguridad informática de la Gerencia de la Tecnología de la Información y Comunicación, del INDOTEL?

Aplicaciones usadas para romper la política de seguridad o blockeo web, abriendo puertas a virus, malware, troyan y Denies of services a la página.

¿Cuáles factores son los que originan con mayor frecuencia las vulnerabilidades de seguridad en informática?

En el caso de aplicaciones de proxy externos, la gran variedad y la continua aparición de estos ejecutables sin que el antivirus corporativo lo catalogue como archivo indeseado.

ANEXO 5**. Cuadro de Operacionalización de las Variables**

Objetivo General: Análisis de los procesos de seguridad en informática en la Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes, INDOTEL, Santo Domingo, República Dominicana.

Objetivo específico No.1	Variable/s	Definición de la variable	Indicadores	Objetivo del indicador	Preguntas
Identificar las Herramientas tecnológicas de la Gerencia Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes INDOTEL, Santo Domingo, República Dominicana.	Herramientas Tecnológicas	Son el conjunto software y hardware, los cuales permiten que los recursos informáticos de la Gerencia en Tecnología de la Información sean aplicados eficientemente.	Recursos	Determinar si las herramientas tecnológicas utilizadas por Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes son suficientes para realizar las labores de seguridad en informática.	¿Cuáles son las herramientas tecnológicas que son utilizadas por la Gerencia de Tecnología de la Información y Comunicación para mantener la seguridad en informática?

			Software	Determinar las aplicaciones que facilitan la gestión y control de todos los elementos informáticos en la Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes.	¿Cuáles son los software que facilitan la gestión y control de todos los elementos informáticos de la organización?
			Gestión	Determinar si las herramientas tecnológicas utilizadas facilitan los procesos de gestión de la seguridad informática en la Gerencia de Tecnología de la Información y Comunicación.	¿Facilitan las herramientas tecnológicas utilizadas por la Gerencia de Tecnología de la Información y Comunicación los procesos de gestión de la seguridad informática?

			Hardware	Determinar si el hardware que posee la Gerencia de Tecnología de la Información es suficiente para llevar a cabo la seguridad informática de manera eficientemente el INDOTEL.	¿Es suficiente el hardware que posee la Gerencia de Tecnología de la Información para llevar a cabo la seguridad informática eficientemente en el INDOTEL?
			Documentación	Verificar la existencia en la Gerencia de Tecnología de la Información y comunicación, la documentación necesaria para el control y registros, que ayuden a realizar la labor diaria.	¿Existe en la Gerencia de Tecnología de la Información y comunicación, la documentación necesaria para el control y los registros, que

					ayuden a realizar la labor diaria?

Objetivo específico No. 2	Variable/s	Definición de la variable	Indicadores	Objetivo del Indicador	Preguntas
Identificar las políticas de seguridad en Informática aplicadas por la Gerencia Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes INDOTEL, Santo Domingo, República Dominicana.	Política de Seguridad Informática.	Identificar los elementos, procedimientos y áreas de normalización que permitan a la Gerencia de Tecnología de la Información del INDOTEL salvaguardar sus sistemas y la información. .	Elementos que la conforman Áreas de normalización	Identificar los principales elementos de una Políticas de Seguridad Informática en la Gerencia de Tecnología de la Información y Comunicación. Las áreas que debe abarcar una política de seguridad, para proteger y mantener la disponibilidad de los sistemas informáticos y	¿Qué elementos son vitales, al momento de definir una política de seguridad informática en la Gerencia TIC? ¿Cuáles áreas debe abarcar una política de seguridad, en la Gerencia de Tecnología de la Información y Comunicación?

				de sus recursos.	

Objetivo específico No. 3	Variable/s	Definición de la variable	Indicadores	Objetivo del Indicador	Preguntas
Identificar las Amenazas y Vulnerabilidades que enfrenta la seguridad informática de la Gerencia de Tecnología de la Información y Comunicación, del Instituto Dominicano de las Telecomunicaciónes INDOTEL, Domingo, República Dominicana.	Amenazas	Determinar todos los problemas que afecten la seguridad de la información del INDOTEL.	Tipos de amenazas Categorización	Determinar los tipos de amenazas a las cuales se enfrenta la seguridad en informática, de la Gerencia de Tecnología de la Información y Comunicación del INDOTEL. Identificar los tipos de	¿Cuáles son los tipos de amenazas a los cuales la seguridad en informática se ve atentada? ¿Existe alguna categorización de las amenazas que enfrenta la seguridad en informática del

				categorización de las amenazas que existen en la Gerencia de Tecnología de la Información y Comunicación del INDOTEL.	departamento TIC del INDOTEL, de existir, podría decir cuáles son?
	Vulnerabilidades	Los diferentes riesgos y factores a los cuales se enfrenta la seguridad informática.	Riesgos	Determinar los riesgos más frecuentes a lo que se enfrenta la seguridad informática de la Gerencia de Tecnología de la Información y	¿Cuáles son los riesgos más frecuentes los que se ha enfrentado la seguridad informática de la Gerencia de Tecnología de la Información y Comunicación, del INDOTEL?

			Factores	Comunicación del INDOTEL. Son los factores que originan las vulnerabilidades en la seguridad informática de la Gerencia de Tecnología de la Información y Comunicación.	¿Cuáles factores son los que originan con mayor frecuencia las vulnerabilidades de seguridad en informática en el INDOTEL?