VICECERECTORÍA DE ESTUDIOS DE POSGRADO

TESIS PARA OPTAR POR EL TÍTULO EN MAESTRÍA EN GERENCIA Y PRODUCTIVIDAD

**TÍTULO:**

# "ANALIZAR EL PROCESO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA PRESIDENCIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (OPTIC). SANTO DOMINGO, AÑO 2015"


**POSTULANTE:**

HENRY GONZÁLEZ

**MATRÍCULA:**

2013-1666

**ASESORA:**

EDDA FREITES, MBA



SANTO DOMINGO, R.D.

ABRIL, AÑO 2015

# RESUMEN

La investigación para la elaboración de esta tesis tuvo como objetivo principal, elaborar un análisis del proceso de gestión de seguridad de la información, tomando como caso de estudio la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC). La metodología que se utilizó fue la del método deductivo, exploratoria, descriptiva y explicativa, además de utilizarse técnicas de recolección de información como las entrevistas y encuestas. Los principales hallazgos que sobresalieron en la investigación es que los incidentes de seguridad servicios de alojamiento de portales gubernamentales, correos institucionales, higiene de correo (Anti-Spam), aplicaciones web, entre otros servicios, presentan un nivel del 41.94% del total de los incidentes en sus diferentes categorías, cifras alarmantes para servicios certificados bajo la norma ISO 20000-1:2011 que contempla la gestión de seguridad de la información y los requisitos mínimos necesarios para hacer una buena gestión de la seguridad de la información. La mayor frustración de la división de infraestructura de TI se basa en el desconocimiento de la causa raíz de los incidentes de seguridad, las acciones correctivas son paliativas y no eliminan la causa raíz, la falta de presupuesto limita la inversión en software y hardware de seguridad actualizado, falta de entrenamientos de seguridad y monitoreo, entre otras variables. Sin embargo, en comparación al año 2013, los intentos de ataques fructíferos e incidentes de seguridad han disminuido en más de un 65%, demostrando que el proceso se encuentra en mejora continua, pero aún no está al nivel requerido.

# ÍNDICE

LISTA DE FIGURAS Y TABLAS ..... ii

DEDICATORIA ..... iii

AGRADECIMIENTO ..... iv

INTRODUCCIÓN ..... 1

CAPÍTULO I ..... 4

CONCEPTOS Y DEFINICIONES GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ..... 4

1.1. Conceptos de seguridad de información ..... 4

1.1.1. Activos ..... 4
1.1.2. Información ..... 6
1.1.3. Sistemas de información ..... 6
1.1.4. Sistemas informáticos ..... 7
1.1.5. Tipos de seguridad ..... 7
1.1.6. Sistema de información seguro ..... 8
1.1.7. Gestión de seguridad ..... 9

1.2. Sistema de gestión de la seguridad de la información ..... 9

1.2.1. Estrategia y táctica ..... 11
1.2.2. Planes ..... 11
1.2.3. Plan de contingencia ..... 12
1.2.4. Políticas ..... 13
1.2.5. Procesos ..... 14
1.2.6. Auditoría ..... 14
1.2.7. Acciones correctivas y preventivas ..... 15
1.2.8. Revisión del sistema de gestión de seguridad de la información ..... 15

1.3. Análisis de riesgo ..... 16
1.3.1. Amenaza ..... 16
1.3.4. Riesgo ..... 19
1.3.5. Gestión de riesgos ..... 19
1.3.6. Identificación del riesgo ..... 19
1.3.7. Evaluación de riesgo ..... 20
1.3.8. Vulnerabilidades ..... 20
1.3.9. Impactos ..... 20
1.3.10. Ataques ..... 20
1.4. Normas, reglamentos y leyes ..... 21
1.4.1. Normas de seguridad de la información ..... 21
1.4.2. COBIT ..... 21
1.4.3. Serie ISO 27000 ..... 22
1.4.4. Ley No. 53-07 sobre crímenes y delitos de alta tecnología ..... 22
CAPÍTULO II ..... 24
GENERALIDADES DE LA OFICINA PRESIDENCIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (OPTIC) ..... 24
2.1. Reseña histórica ..... 24
2.2. Marco estratégico ..... 26
2.3. Estructura organizativa ..... 27
2.4. Funciones de la institución ..... 27
2.5. Portafolio de servicios ..... 29
2.6. Plan estratégico 2014-2016 ..... 33
2.7. Política de calidad ..... 34
2.8. Levantamiento de información ..... 34
2.8.1. Encuesta ..... 37
2.8.2. Tabulación y graficación de los resultados ..... 38
2.8.3. Interpretación de los resultados ..... 38

CAPÍTULO III ..... 40
PROPUESTA DE MEJORA DEL PROCESO ..... 40
3.1 Análisis de impacto del negocio (BIA) ..... 40
3.2 Contingencia ante ataques o fallas ..... 42
3.3 Mantenimientos ..... 45
3.4 Seguridad y monitoreo ..... 45
3.4.1 Acceso a los sistemas ..... 45
3.4.2 Niveles de confianza ..... 46
3.5 Protocolos de acceso físico ..... 46
3.6 Estructura y responsable ..... 47
3.7 Uso aceptable de los servicios ..... 49
3.8 Uso prohibido de los servicios ..... 49
CONCLUSIONES ..... 52
BIBLIOGRAFÍA ..... 53

# LISTA DE FIGURAS Y TABLAS

Figura No.1: Diagrama del Sistema de Gestión de Seguridad de la Información ..... 10
Tabla No.1: Tabla de vectores de amenaza ..... 18
Figura No.2: Organigrama Institucional ..... 27
Tabla No.2: Relación de incidentes por categoría del 2012 al 2015 ..... 35
Figura No.3: Relación de incidentes por categoría del 2012 al 2015 ..... 35
Figura No.4: Tabulación de encuesta de seguridad de información. ..... 38
Tabla No.3: Tabla de matriz de impacto ..... 41
Tabla No.4: Tabla de objetivo de restauración ..... 41
Tabla No.5: Nivel de confianza ..... 46
Tabla No.6: Marco de Autoridades y Responsabilidades del Negocio ..... 47
Tabla No.7: Marco de Autoridades y Responsabilidades de los Planes ..... 48

# DEDICATORIA

**A mi madre María Mosquea,**

Porque mis sueños se convirtieron en tus sueños y para lograrlo recibí tu apoyo en todos los sentidos. Este logro es también tuyo.

**A mi padre Adalmiro González,**

Por ser el pilar fundamental en mi formación y educación como persona y por inculcar en mí los valores de la perseverancia y la constancia.

**A mis abuelas Generosa Berroa y Carmen Altagracia Mercedes,**

Porque han sido mi ejemplo como persona y por estar siempre presente en los momentos que más las he necesitado.

**A mi prometida Rosa Ureña,**

Por aguantarme todo este tiempo y saber comprender. Sabes que eres tan importante para mí que has representado un hito infinito y constante en mi vida.

**A mis hijos Alina y Jhusuell,**

Porque son el significado de todo lo que hoy en día estoy haciendo.

**A mis hermanos Eric, Melanin y Adalberto,**

Porque siempre han estado junto a mí como una especie de soporte.

**A mis tías Juana, Susana, Carmen y María,**

Porque siempre me han apoyado en todas mis decisiones personales y profesionales.

Henry González

# AGRADECIMIENTO

**A mis padres, María Mosquea y Adalmiro González,**

Por su apoyo incondicional, paciencia, comprensión, empeño, consejo y amor, que fueron valores que me impulsaron a seguir adelante y por su confianza a ojos cerrados en cada sueño y meta propuesta en la vida.

**A mi prometida, Rosa Ureña,**

Por impulsarme a lograr mis deseos, además de servirme de sendero en los tiempos que más lo necesité.

**A mi asesora Edda Freites,**

Por los conocimientos facilitados con esmero y profesionalidad, así como por su disposición y guía en el proceso de esta investigación.

Henry González

# INTRODUCCIÓN

La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) de la República Dominicana, es una institución con dependencia del Poder Ejecutivo, creada con la responsabilidad de planificar, dirigir y ejecutar las acciones necesarias para implementar el Gobierno Electrónico en el país mediante la difusión y uso de las Tecnologías de la Información y Comunicación (TIC).

Actualmente, la OPTIC cuenta con un catálogo de servicios que va desde servicios ciudadanos, extranjeros, empresas e instituciones del Estado, siendo esta última su principal cliente en la mayoría de los servicios.

Sin embargo, actualmente Estado Dominicano y el resto del mundo son el objetivo de mira dentro de los ataques de denegación de servicios (Ataque DoS), alteración de la imagen de portales gubernamentales (Deface Web) y extracción de información clasificada por los disgustos de la sociedad ante las acciones políticas. Por tanto, coloca a la OPTIC en punto de mira de los principales ataques tecnológicos que se producen en nuestro país por alojar 62 de instituciones de alto impacto gubernamental.

Así que en esta investigación se define la importancia de analizar el proceso de seguridad de la información para una empresa o institución, enfocados en aportar valor teórico para los estudiantes de infraestructura de TI, seguridad y monitoreo, así como para las empresas en sí mismas e instituciones gubernamentales.

En esta investigación se abordan cuatro factores problemáticos, por los cuales es importante la elaboración de este análisis, tal como el factor sobre del desconocimiento técnico, limitación presupuestaria, controles tecnológicos y el factor humano.

Esta investigación tiene como objetivo general elaborar un análisis del proceso de gestión de seguridad de la información y aportar un plan de mejora procedente del resultado del análisis, donde se detallan tres objetivos específicos como son: definir los controles mínimos necesarios para los sistemas de procesamiento de información, mostrar los aspectos de seguridad tomados en cuenta por otras organizaciones privadas, analizar los controles y nuevos riesgos de seguridad para diseñar un plan de mejora del proceso objeto de estudio.

La metodología utilizada para lograr dichos objetivos se hizo basada en una metodología bibliográfica descriptiva, la cual se concreta en mencionar de forma breve los aspectos sobresalientes de un contenido para conocer el estado de la cuestión, así como las características generales del trabajo, permitiendo ordenar los resultados de las observaciones por sus características, factores, hechos, procedimientos y otras variables de fenómenos.

Se utilizó informaciones de registro cuantitativo, las cuales permiten examinar los datos de manera numérica, se aplicó el método deductivo, partiendo de datos generales aceptados como válidos, para llegar a una conclusión de tipo particular, buscando sacar y separar consecuencias en el tema a investigar.

De igual forma, se utilizó el método inductivo, en los momentos que se necesitó analizar una información partiendo de casos particulares para llegar a conclusiones generales.

Toda la investigación ha sido dividida en tres capítulos, los cuales desglosamos de la siguiente manera:

En el primer capítulo se definen todos los conceptos a utilizar en el cuerpo del trabajo como son: las tecnologías de la información y comunicación, seguridad de la información, activos de TI, técnicas de mitigación de amenazas

secundarias y primarias, sistemas de gestión de seguridad de la información, riesgos, incidentes de seguridad, acuerdos de nivel de operación y acuerdos de niveles de servicios.

En el segundo capítulo se muestran las características generales de la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), sobre la cual conoceremos su historia, la cartera de servicios que ofrecen, posicionamiento y su importancia en el Estado Dominicano, así como un análisis detallado del estado en que se encuentra la OPTIC.

En el tercer capítulo se muestra el análisis detallado del proceso de gestión de seguridad de la información que a su vez comprenderá las recomendaciones y pautas a seguir para mejor el proceso en cuestión.

# CAPÍTULO I
# CONCEPTOS Y DEFINICIONES GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

## 1.1. Conceptos de seguridad de información

"Es la disciplina que se ocupa de diseñar las normas, procedimiento, metidos y técnicas destinados a conseguir un sistema de información seguro y confiable"[1].

### 1.1.1. Activos

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la institución y la consecución de los objetivos. Al hacer un estudio de activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido a otro.

Podemos clasificar en los siguientes tipos:

**Datos:** Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soporte de diferente tipo.

**Software:** Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

[1] Aguilera, Purificació. (2010). Seguridad Informática. Madrid, Espana: Editorial Editex, S.A.

**Hardware:** Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información. Se incluye en ese grupo los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vía de transmisión de los datos (módem, router, instalación eléctrica o sistemas de alimentación ininterrumpida, destructores de soportes informáticos, entre otros).

**Redes:** Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancia.

**Soportes:** Los lugares en donde la información queda registrada y almacenada durante largos períodos o de forma permanente (DCD, CD, memorias, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).

**Instalaciones:** Son los lugares que albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales o edificios, pero también pueden ser vehículos u otros medios de desplazamiento.

**Personal:** El conjunto de personas que interactúan con el sistema de información: administradores, programadores, usuarios internos y externos y resto de personal de la empresa.

**Servicios:** Que se ofrecen a clientes o usuarios, dígase productos, servicios, sitios web, fotos, correos electrónicos u otros servicios de comunicaciones, información, seguridad, etc.

### 1.1.2. Información

En las organizaciones, la información es a menudo uno de los activos más importante que una empresa posee y provee un impulso que ayuda a una empresa a ser más exitosa que otras.

La información debe ser clasificada de acuerdo a su público objetivo y ser manejado en consecuencia. Cada pieza de información debe estar clasificada en una de las siguientes categorías:

- **Información personal** no es propiedad de la organización, que pertenece a particulares.
- **Información Pública** que se distribuyen entre la visión y por el público en general.
- **Información confidencial** para uso de los empleados, contratistas y sólo socios comerciales.
- **La propiedad intelectual** de propiedad de la organización para ser manejado sólo por las partes autorizadas.
- **Información secreta** para uso exclusivo de personas designadas con una necesidad de saber.

### 1.1.3. Sistemas de información

"Un sistema de información es conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos"[2].

[2] Solís, Carlos. *Implantar Controles de Seguridad de la Información*. 2da edición, España: Editorial Academia España.

Estos elementos son:

**Recursos:** Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógico, como sistemas operativos y aplicaciones informáticas.

**Equipo humano**: Compuesto por las personas que trabajan para la organización.

**Información**: Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.

**Actividades**: Que se realizan en la organización, relacionadas o no con la información.

### 1.1.4. Sistemas informáticos

Un sistema informático está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos, entre otros) y con frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y el hardware).

### 1.1.5. Tipos de seguridad

Existen cuatro tipos de seguridad:

**Seguridad activa**: Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

**Seguridad pasiva:** Está formada por las medidas que se implantan para una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos.

**Seguridad física:** Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control.

**Seguridad lógica:** Se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos.

### 1.1.6. Sistema de información seguro

Los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización.

Su origen puede ser:

**Fortuito:** Errores cometidos accidentalmente por los usuarios, accidentes, cortes de red eléctrica, averías del sistema y catástrofes naturales.

**Fraudulento:** Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

Se considera seguro un sistema que cumple con las propiedades de:

- **Integridad:** La información debe ser correcta y completa.
- **Confidencialidad:** La información debe ser sólo accesible a sus destinatarios
- **Disponibilidad:** debe de tener acceso a la información cuando la necesitamos.

### 1.1.7. Gestión de seguridad

"Velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo"[3].

## 1.2. Sistema de gestión de la seguridad de la información

Es la parte del sistema general de gestión, basado en un enfoque de riesgo de negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

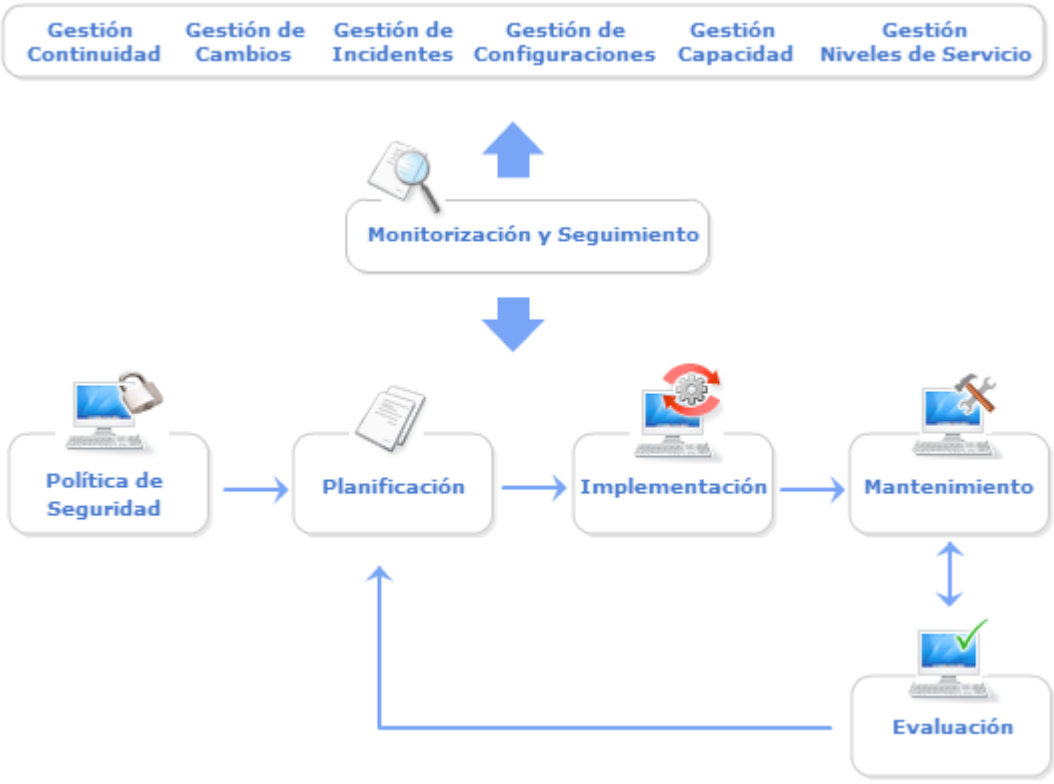
El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

Los principales objetivos de la gestión de la seguridad se resume en:

- Diseñar una política de seguridad, en colaboración con clientes y proveedores correctamente alineada con las necesidades del negocio.
- Asegurar el cumplimiento de los estándares de seguridad acordados.
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio.

[3] Gestión de la Seguridad. *Visión General*. Encontrado Marzo 30, 2015. En Osiatis: http://itil.osiatis.es

**Figura No.1: Diagrama del Sistema de Gestión de Seguridad de la Información**




Fuente: itilv3.osiatis.es

Los principales beneficios de una correcta gestión de la seguridad:

- Se evitan interrupciones del servicio causados por virus, ataques informáticos, etcétera.
- Se minimiza el número de incidentes.
- Se tiene acceso a la información cuando se necesita y se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumplen los reglamentos sobre protección de datos.
- Mejora la percepción y confianza de clientes y usuarios en lo que respecta a la calidad del servicio.

Las principales dificultades a la hora de implementar la gestión de la seguridad se resumen en:

- No existe el suficiente compromiso de todos los miembros de la organización TI con el proceso.
- Se establecen políticas de seguridad excesivamente restrictivas que afectan negativamente el negocio.
- No se dispone de las herramientas necesarias para monitorizar y garantizar la seguridad del servicio (firewalls, antivirus, etcétera).
- El personal no recibe una formación adecuada para la aplicación de los protocolos de seguridad.
- Falta de coordinación entre los diferentes procesos lo que impide una correcta evaluación de los riesgos.

### 1.2.1. Estrategia y táctica

Una estrategia de seguridad es la definición de todos los componentes de la arquitectura y de políticas que conforman un plan completo para la defensa, detección y disuasión. Tácticas de seguridad son las prácticas del día a día de las personas y las tecnologías asignados a la protección de los activos. Dicho de otra manera, las estrategias suelen ser proactivo y tácticas son a menudo reactivas. Ambos son igualmente importantes, y un programa de seguridad exitoso tiene que ser a la vez estratégica y táctica en la naturaleza. Con un plan estratégico bien definido conducir operaciones tácticas, el esfuerzo de seguridad tendrá la mejor oportunidad de éxito.

### 1.2.2. Planes

Es un documento que tiene por objetivo fijar los niveles de seguridad que han de ser incluidos como parte de los SLA, OLA y UC.

Este plan ha de ser desarrollado en colaboración con la gestión de niveles de servicio que es la responsable en última instancia tanto de la calidad del

servicio prestado a los clientes como la del servicio recibido por la propia organización TI y los proveedores externos.

El Plan de Seguridad debe diseñarse para ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio.

Siempre que sea posible deben definirse métricas e indicadores clave que permiten evaluar los niveles de seguridad acordados.

Un aspecto esencial a tener en cuenta es el establecimiento de unos protocolos de seguridad coherentes en todas las fases del servicio y para todos los estamentos implicados.

### 1.2.3. Plan de contingencia

"El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto"[4].

El plan de contingencia contiene medidas preventivas paliativas y recuperación de desastre.

El plan de contingencias consta de tres (3) sub-planes independientes:

- **Plan de respaldo:** Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en lugar seguro copias de seguridad de la información, instalar pararrayos o hacer simulacros de incendio.
- **Plan de emergencia:** Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse. Por

[4] Marc, Royer, *Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones,* 1ra Edición, Editorial Xavier Angelet.

ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.

- **Plan de recuperación:** Indica las medidas que se aplicarán cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento de sistema y de la organización. Por ejemplo, tener un lugar alternativo donde continuar la actividad si el habitual hubiese sido destruido, sustituir el material deteriorado, reinstalar aplicaciones y restaurar copias de seguridad.

### 1.2.4. Políticas

"Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la alta dirección"[5].

El objetivo principal de la redacción de una política de seguridad es de concienciar a todo el personal de una organización en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización.

En particular la política de seguridad debe determinar:

- La relación con la política general del negocio.
- La coordinación con los otros procesos de TI.
- Los protocolos de acceso a la información.
- Los procedimientos de análisis de riesgos.
- Los programas de formación.

[5] Pertier, Thomas. (2010). *Análisis de Riesgo de Seguridad de la Información*, 3era Edición, Editorial Auerbach.

- El nivel de monitorización de la seguridad.
- Qué informes deben ser emitidos periódicamente.
- El alcance del plan de seguridad.
- La estructura y responsables del proceso de gestión de la seguridad.
- Los procesos y procedimientos empleados.
- Los responsables de cada subproceso.
- Los auditores externos e internos de seguridad.
- Los recursos necesarios: software, hardware y personal.

### 1.2.5. Procesos

"Es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados"[6].

Los elementos de entrada para un proceso son generalmente resultados de otros procesos.

Un proceso en el cual la conformidad del producto resultante no pueda ser fácil o económicamente verificada, se denomina habitualmente "proceso especial".

### 1.2.6. Auditoría

La auditoría es un análisis pormenorizado de un sistema de seguridad de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan. Su finalidad es verificar que se cumplen los objetivos de la política de seguridad de la organización. Proporciona una imagen real y actual del estado de seguridad de un sistema de información.

Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de

[6]ISO 9001:2005 - Fundamentos – Vocabulario.

determinar el grado en que se cumplen los criterios de auditoría. (ISO 9000:2005 *Sistema de Gestión de la Calidad* – Fundamentos y Vocabulario).

### 1.2.7. Acciones correctivas y preventivas

Una acción correctiva es tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable. La acción correctiva se toma para prevenir que algo vuelva a producirse.

Una acción preventiva es tomada para eliminar la causa de una no conformidad potencial u otra situación no deseable. La acción preventiva se tomara para prevenir que algo suceda, mientras que la acción correctiva se toma para prevenir que vuelva a producirse.

### 1.2.8. Revisión del sistema de gestión de seguridad de la información

Consiste en llevar a cabo de forma regular evaluaciones sistemáticas de la conveniencia, adecuación, eficacia y eficiencia del sistema de gestión de seguridad de la información con respecto a los objetivos y a la política de calidad. La revisión puede incluir considerar la necesidad de adaptar la política y objetivos de seguridad en respuesta a las cambiantes necesidades y expectativas de las partes interesadas. La revisión incluye la determinación de la necesidad de emprender acciones.

La revisión del sistema de gestión debe contar de por lo menos con:

- Retroalimentación de los clientes.
- Desempeño de los procesos.
- Pronóstico actual y futuro de recursos humanos, técnicos, información y financiera.
- Riesgos.
- Resultados de la auditoría pasada.

- Resultados proveniente de la última revisión.
- Estatus de las acciones correctivas y preventivas.
- Cambios que podrían afectar el sistema de gestión.
- Oportunidades de mejora.

## 1.3. Análisis de riesgo

"El objetivo de un programa de seguridad es para mitigar los riesgos. La mitigación de riesgos no significa la eliminación de ellos; significa reducir a un nivel aceptable. Para asegurarse de que los controles de seguridad están controlando eficazmente los riesgos en su entorno, es necesario anticipar lo que puede ocurrir tipo de incidentes"[7].

Un análisis de riesgos tiene que ser parte de todos los esfuerzos de seguridad. Debería analizar y clasificar los activos que necesitan ser protegidos y los riesgos que deben ser evitados, y debe facilitar la identificación y priorización de los elementos de protección. También puede proporcionar un medio para medir la efectividad de la arquitectura global de seguridad, mediante el seguimiento de los riesgos y su mitigación asociado con el tiempo para observar las tendencias.

### 1.3.1. Amenaza

Presencia de uno o más factores de diversa índole (persona, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole danos aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores

[7] Gestión de Riesgos de Seguridad de la Información, Norma ISO/IEC 27005:2011.

intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

La evaluación de las amenazas es una parte importante del análisis de riesgos. Mediante la identificación de amenazas, puede darle a su enfoque estrategia de seguridad y reducir la posibilidad de pasar por alto importantes áreas de riesgo que de otro modo podrían permanecer sin protección. Las amenazas pueden tomar muchas formas, y con el fin de tener éxito, una estrategia de seguridad debe ser lo suficientemente amplio como para gestionar las amenazas más importantes.

Muchas de las amenazas del mundo real provienen de dentro de la organización, por lo que sólo la construcción de un muro alrededor de su interior de confianza no es lo suficientemente bueno. Independientemente de la ruptura de su organización en particular, debe asegurarse de que los controles de seguridad se centran en las amenazas de la derecha. Para evitar pasar por alto las fuentes de amenazas importantes, debe tener en cuenta todo tipo de amenazas. Esta consideración debe tener en cuenta los siguientes aspectos de las amenazas:

- Vectores de amenazas
- Las fuentes y destinos de amenazas
- Tipos de ataques
- Código móvil malicioso
- Amenazas persistentes avanzadas
- Ataques manuales

**Vector amenaza**

Un vector de amenaza es un término usado para describir el lugar donde se origina una amenaza y el camino que se necesita para alcanzar un objetivo. Un ejemplo de un vector de amenazas es un mensaje de correo electrónico

enviado desde fuera de la organización a un empleado en el interior, que contiene una línea de asunto irresistible junto con un archivo adjunto ejecutable que pasa a ser un programa troyano, que pondrá en peligro el ordenador del receptor si se abre.

Una buena manera de identificar los vectores potenciales amenazas es crear una tabla que contiene una lista de amenazas que le preocupan, junto con las fuentes y destinos, como se muestra en la tabla siguiente.

**Tabla No.1: Tabla de vectores de amenaza**

| Fuentes | Amenazas | Objetivo |
|---|---|---|
| **Empleado** | Robar | Propiedad intelectual |
| **Contratista** | Perder | Secreto comercial |
| **Consultor** | Exponer | Información de identificación personal |
| **Integrador de sistema** | Cambios no autorizados | Proteger la salud de la información |
| **Proveedor de servicio** | Supresión (Completa) | Datos financieros |
| **Distribuidor** | Supresión (Parcial) | Número de tarjeta de crédito |
| **Vendedor** | Inclusión no autorizada | Número de seguridad social |
| **Personal de limpieza** | Fraude | Documento |
| **Soporte técnico** | Suplantación | Computadora |
| **Competidor** | Acoso | Periférico |
| **Personal interno** | Espionaje | Almacenamiento |
| **Terrorista** | Denegación de servicio | Red |
| **Atacante web** | Mal funcionamiento | Sistema operativo |
| **Programa** | Corrupción | Correo electrónico |
| **Malware** | Mal uso | Comunicación de voz |
| **Software de errores** | Error | Aplicación |
| **Accidente** | Corte | Privacidad |
| **Clima** | Riesgo físico | Productividad |
| **Causas naturales** | Lesión | Salud y seguridad |

Tomado del libro: Seguridad de la Información, Mark Rhodes, 2da Edición.

### 1.3.4. Riesgo

"Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma"[8].

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (por ejemplo, contratando un seguro).

### 1.3.5. Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

### 1.3.6. Identificación del riesgo

Proceso de encontrar, reconocer y describir los riesgos.

La identificación de riesgos consiste en la identificación de las fuentes de riesgo, eventos, sus causas y sus posibles consecuencias.

La identificación de riesgos puede implicar datos históricos, análisis teórico, opiniones informadas y expertos, y las necesidades de las partes interesadas.

[8] Gestión de Riesgos de Seguridad de la Información, Norma ISO/IEC 27005:2011

### 1.3.7. Evaluación de riesgo

Proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable.

### 1.3.8. Vulnerabilidades

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Al hacer el análisis de riesgo hay que tener en cuenta la vulnerabilidad de cada activo.

### 1.3.9. Impactos

"Son las consecuencias de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado"[9].

Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen danos no cuantificables, como los causados contra los derechos fundamentales de las personas.

### 1.3.10. Ataques

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza. En función del impacto causado a los activos atacados, los ataques se clasifican en activos y pasivos.

**Ataque activo:** Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.

[9] García, Alfonso. (2011). Seguridad Informática, 1ra edición, Madrid, España: Editora Paraninfo, S.A.

**Ataque pasivo:** Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

## 1.4. Normas, reglamentos y leyes

Los intentos de prevenir el abuso y el fraude han dado lugar a un aumento de las regulaciones, normas y directrices, causando organizaciones que presten mayor atención a la gobernanza, que ha cambiado la dinámica de la gestión de seguridad de la información. Los delitos informáticos y ataques cibernéticos están en aumento, muchas de las cuales son perpetradas por el uso de técnicas de ingeniería social. Concienciación sobre la seguridad del edificio en la estructura de gobierno se ha convertido en esencial.

### 1.4.1. Normas de seguridad de la información

Conjuntos de "mejores prácticas" se han desarrollado y publicado por organizaciones internacionalmente reconocidas, y aceptado por la profesión seguridad de la información en general. Las más conocidas son:

- Objetivos de control para la información y tecnologías relacionadas (COBIT).
- Norma internacional ISO 27001 e ISO 27002.
- Ley No. 53-07 sobre crímenes y delitos de alta tecnología.

### 1.4.2. COBIT

COBIT es publicado por ISACA, la Asociación de Auditoría de Sistemas de Información y Control (Information Systems Audit and Control Association). ISACA es una organización de gobierno de TI independiente ampliamente reconocido, y sus directrices de COBIT son utilizados por la administración de TI en muchas organizaciones para definir y gestionar los procesos basados en

un modelo de madurez como el Capability Maturity Model (CMM). COBIT no se trata de información de seguridad, es un estándar de TI en general, pero algunas prácticas de seguridad están integrados dentro de ella. COBIT contiene un alto nivel de las directrices de seguridad de información de la serie ISO 27000, para ajustar los objetivos de negocio con los objetivos de TI.

### 1.4.3. Serie ISO 27000

La serie de normas de seguridad de la información ISO 27000 proporciona un conjunto de marcos para el desarrollo de un programa de seguridad, desde el concepto de madurez. Se divide en varias partes con el fin de ser manejable, cada parte prescribe un conjunto de actividades que pertenecen a fases comparables a los de Planificar-Hacer-Verificar-Actuar (o más exactamente, Plan-Do-Check-Ajuste) (PDCA ) ciclo Deming, similar a lo que hace COBIT.

El marco de la serie ISO 27000 combina la evaluación del riesgo inicial familiarizado con los controles esenciales para el cumplimiento de las regulaciones más típicos controles que se consideran las mejores prácticas comunes para la seguridad de la información. Controles de mejores prácticas incluyen la creación de un documento de políticas de seguridad de la información, el desarrollo de un plan de organización con responsabilidades de seguridad claramente definidos, educación y formación concerniente a seguridad, de información apropiada de incidente, y desarrollo de un plan de recuperación de desastres.

### 1.4.4. Ley No. 53-07 sobre crímenes y delitos de alta tecnología

La ley No. 53-07 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 morales, 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.

Esta ley se aplicará en todo el territorio de la República Dominicana, a toda persona física o moral, nacional o extranjera, que cometa un hecho sancionado por sus disposiciones, en cualquiera de las siguientes circunstancias:

- Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional;
- Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio dominicano;
- Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentran en el territorio nacional; y finalmente,
- Cuando se caracterice cualquier tipo de complicidad desde el territorio dominicano.

La presente ley es de aplicación general a todas las personas físicas o morales, públicas o privadas, nacionales o internacionales.

# CAPÍTULO II
# GENERALIDADES DE LA OFICINA PRESIDENCIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (OPTIC)

## 2.1. Reseña histórica

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 el Estado, aumentar la competitividad del sector productivo y socializar el acceso a la información. Siendo de interés muy particular 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, fue 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, en miras de 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.

## 2.2. Marco estratégico

**Misión:** Implementar y desarrollar el Gobierno Electrónico, impulsando y acelerando el proceso de modernización del Estado Dominicano a través del desarrollo y uso de las TIC en la gestión de recursos y la prestación de los servicios públicos.

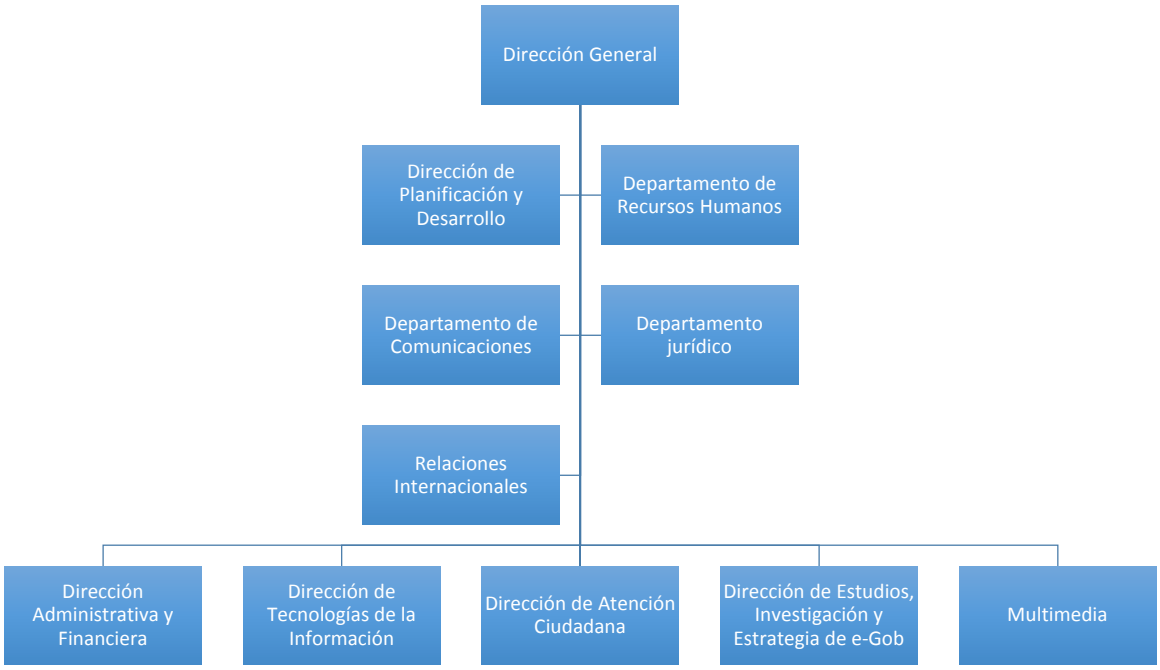
**Visión:** Contribuir a la transformación del Estado en más moderno, transparente, eficaz, eficiente, productivo, participativo y proactivo, a los fines de insertar la República Dominicana en la Sociedad de la Información y del Conocimiento.

**Valores**

- Modernidad
- Planificación
- Excelencia
- Capacidad
- Trabajo En Equipo

## 2.3. Estructura organizativa

**Figura No.2: Organigrama Institucional**




Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

## 2.4. Funciones de la institución

- Diseñar, proponer y definir las políticas, establecer los lineamientos y elaborar las estrategias, planes de acción y programas para promover, desarrollar y garantizar mayor acceso, conectividad e implantación de nuevas tecnologías de la información y comunicación, con el fin de fomentar su uso, como soporte del crecimiento económico y competitividad hacia la sociedad de la información, gestionando los proyectos conforme a tales directrices; y que garanticen el acceso equitativo a los mercados al sector productivo como esfuerzo para la política de generación de empleo, para mejorar la calidad de vida, crear

oportunidades de educación, trabajo, justicia, cultura y recreación, y otros.

- Asesorar, realizar la planificación estratégica; formular, gestionar, ejecutar y evaluar proyectos de tecnologías de información y comunicación (TIC) en las distintas instituciones de gobierno.
- Propiciar y apoyar la creación de redes de cooperación entre el sector público, privado y sociedad civil para facilitar y optimizar la gestión de los organismos gubernamentales y la contratación administrativa.
- Realizar investigaciones y estudios, promover la transferencia de conocimientos, de información y de nuevas tecnologías a la sociedad y a la comunidad empresarial.
- Comunicar y difundir el uso de las tecnologías de la información y comunicación (TIC) en la sociedad dominicana.
- Formular políticas e implementar el proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado hacia la sociedad de la información, promoviendo la integración de nuevas tecnologías, su compatibilidad, interoperabilidad y estandarización en materia de tecnologías de información y comunicación (TIC).
- Asistir a las instituciones gubernamentales centralizadas, autónomas y descentralizadas en la identificación de oportunidades de implantación de tecnologías de la información y comunicación, para la mejora y eficiencia de la función pública y en el diseño de proyectos de implantación identificados, sin perjuicio de la iniciativa que debe corresponder a cada entidad, buscando promover la adopción y uso de las tecnologías de la información y comunicación en las entidades públicas, particularmente para su mejor relación con los ciudadanos.
- Proponer políticas para difundir y promover la generación de una cultura de tecnología de la información y comunicación en el país.
- Participar en los proyectos de desarrollo, innovación, implementación e integración de las Tecnologías de la Información y Comunicación (TIC),

cualquiera que fuese su fuente de financiamiento, a fin de optimizar las inversiones en el ámbito del sector público.

- Velar, asistir y supervisar en los aspectos y políticas relativas a la seguridad y privacidad de la información digitalizada y electrónica en el ámbito del sector público.
- Coordinar, dar seguimiento y proponer ajustes y nuevos proyectos para la ejecución de la Agenda del Gobierno Electrónico.
- Preparar y proponer el instructivo presidencial para la aplicación y desarrollo de la agenda de Gobierno Electrónico 2005-2008.
- Proponer acciones y otros instructivos presidenciales que se entiendan necesarios en vías de garantizar la buena gestión y aprovechamiento de los recursos tecnológicos por parte del Gobierno y el país para insertarnos en la sociedad de la información.

## 2.5. Portafolio de servicios

**Atención Presencial al Ciudadano – Punto Gob:** Es un sistema presencial de Servicio al Ciudadano conformado por instituciones del Estado, incorporando el uso de los recursos de información para la prestación de los servicios.

**Atención Telefónica al Ciudadano (*462, 311 y Línea 700):** Este servicio consiste en ofrecer a los ciudadanos:

- Consultas y/o trámites de los servicios de las Instituciones de la Administración Pública a través del *GOB (*462).
- Realizar denuncias de abuso de niñas, niños y adolescentes a través de la Línea 700.

- Realizar Denuncias, Quejas, Reclamaciones y/o Sugerencia relativas a cualquier entidad o servidor del Gobierno de la República Dominicana a través de la línea 311.

**Alojamiento de Portales Gubernamentales:** Alojar portales para instituciones del Estado, este provee la capacidad de gestión descentralizada.

**Alojamiento de Aplicaciones Web:** Alojar aplicaciones web en los servidores de la institución bajo tecnología propietario y/o código abierto.

**Servicio de Centro de Datos (Colocación):** Colocación de servidores en un lugar con máximas características de seguridad, confiabilidad y con las condiciones ambientales, energéticas y respaldo de los servicios.

**Correo Electrónico a las Instituciones del Estado:** Este servicio tiene como finalidad proveer a organismos del Estado el alojamiento de sus respectivos correos electrónicos institucionales, de manera eficiente y confiable. Adicional a este servicio, se adhiere el servicio de Higiene de Correo (Anti-Spam).

**Higiene de Correo (Anti-Spam):** Servicio de prevención de correo basura (Spam).

**Servidor Dedicado:** Este servicio consiste en brindar la facilidad de tener un servidor virtual, donde el cliente pueda aprovechar todos los recursos del servidor.

**Asesoría Técnica:** Consiste en proveer asesoramiento técnico a las instituciones del Estado en las diferentes áreas de las Tecnologías de la Información y Comunicación (TIC).

**Inclusión al Centro de Contacto Gubernamental (Línea *462 y 311):** Consiste en proveer de un canal abierto a todas las instituciones para informar a los ciudadanos sobre el estatus de procesos y/o tramitación de documentos proporcionándole las facilidades para la actualización de datos sirviendo de vía alterna para realizar encuestas.

**Inclusión al Centro de Atención Presencial (Punto Gob):** Consiste en ofrecer un moderno y dinámico sistema presencial de Servicio Ciudadano, incorporando el uso de los recursos de información para la prestación de los servicios institucionales.

**Programa de Alfabetización Digital (PAD) y Capacitación de Gobierno Electrónico a Servidores Públicos:** Consiste en formar a los servidores públicos en los conocimientos y técnicas de informática, con miras a incorporar las nuevas Tecnologías de la Información y Comunicación dentro de los procesos de la Administración Pública para el desarrollo y modernización de la gestión pública.

**Estadísticas Nacionales e Internacionales sobre el Avance de Gobierno Electrónico:** Ofrecer información oportuna, objetiva, confiable, continua, actualizada y comparable en materia de Gobierno Electrónico de la República Dominicana. Estas estadísticas incluyen los índices y rankings de las instituciones gubernamentales en materia de e-Gob.

**Asistencia en Formulación e Implementación de Estrategias y Proyectos de Gobierno Electrónico:** Consiste en proveer apoyo a las instituciones gubernamentales para formular y plantear sus requerimientos TIC en términos de diseñar una solución tecnológica óptima que satisfaga los requerimientos levantados.

**Asistencia Técnica en Implementación de Gobierno Electrónico:** Consiste en proveer asesoría técnica en gobierno electrónico a las instituciones gubernamentales e instituciones provinciales y municipales, así como proveer soluciones para los mismos.

**Certificación NORTIC:** Este servicio consiste en la asesoría, auditoria y posterior certificación bajo las NORTIC sobre el compendio de normas que regirán al Estado Dominicana en materia de TIC.

**Servicio de e-Gob Provinciales / Municipales:** Consiste en proveer asistencia en la agenda de implementación de actividades y proyectos de gobierno electrónico en las localidades atendidas por el programa de comités de tecnología provinciales/municipales. También asisten en la recolección de información local de asuntos de e-Gob.

## 2.6. Plan estratégico 2014-2016

El Plan Estratégico 2014 de la OPTIC, refleja el enfoque de la organización en aquellos proyectos de mayor incidencia, principalmente en las áreas de buen gobierno y atención al ciudadano, que permitirán que la institución cumpla a cabalidad su misión de impulsar el desarrollo del Gobierno Electrónico en el país. Identificadas estas áreas de enfoque, y en torno a las mismas, se establecieron los objetivos institucionales, de los cuales se desprenden las estrategias departamentales y los indicadores que conforman el Plan Operativo 2014 de la institución.

El propósito fundamental de la OPTIC es promover la aplicación de las tecnologías de información y comunicación al mejor funcionamiento de la administración pública, a la prestación de servicios públicos y a la comunicación con los ciudadanos, para ello, las estrategias a ejecutar para este año 2014 van alineadas a lograr los siguientes objetivos:

- Promover el desarrollo del Gobierno Electrónico en los ámbitos de decisión del sector público.
- Implementar Canales de Atención Ciudadana.
- Promover el uso de los servicios de Gobierno Electrónico en la sociedad Dominicana y el sector privado.
- Acelerar el desarrollo integral del Gobierno Electrónico con criterios de eficacia, eficiencia y transparencia.
- Evitar el doble empleo de recursos en el desarrollo del Gobierno Electrónico.
- Racionalizar las inversiones y gastos en TIC del sector público.
- Difundir las mejores prácticas en materia de Gobierno Electrónico.

## 2.7. Política de calidad

Nos comprometemos a contribuir con la transformación del Estado Dominicano mediante el fortalecimiento institucional, la tecnología, la transparencia, la mejora continua de nuestros procesos y servicios, la prestación de servicios de calidad y clientes satisfechos según sus expectativas y necesidades, cumpliendo con la normativa y el marco regulatorio vigentes.

Nos proponemos garantizar a nuestros clientes, servicios:

- De Excelencia
- Profesionales
- Eficientes
- Disponibles

## 2.8. Levantamiento de información

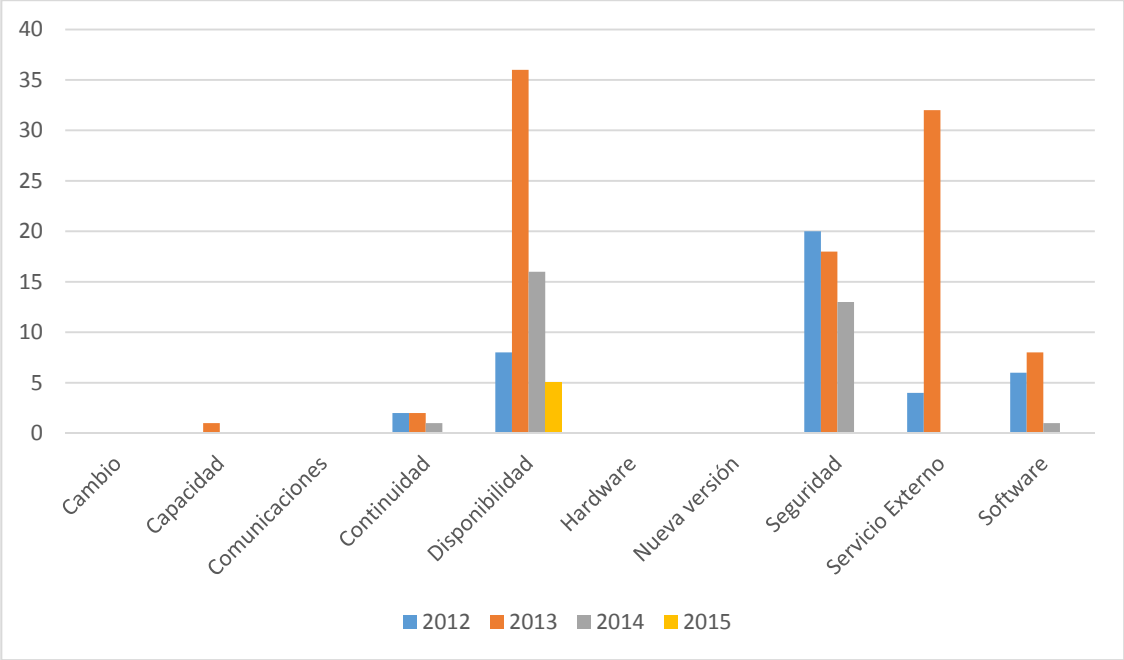
Durante el levantamiento de la información se realizaron encuestas, se recogieron información estadística de los incidentes de seguridad y se analizaron los indicadores de desempeño del proceso de gestión de seguridad de la información.

**Tabla No.2: Relación de incidentes por categoría del 2012 al 2015**

| Tipo de Incidente | 2012 | 2013 | 2014 | 2015 | Total |
|---|---|---|---|---|---|
| **Cambio** | 0 | 0 | 0 | 0 | **0** |
| **Capacidad** | 0 | 1 | 0 | 0 | **1** |
| **Comunicaciones** | 0 | 0 | 0 | 0 | **0** |
| **Continuidad** | 2 | 2 | 1 | 0 | **5** |
| **Disponibilidad** | 8 | 36 | 16 | 5 | **65** |
| **Hardware** | 0 | 0 | 0 | 0 | **0** |
| **Nueva versión** | 0 | 0 | 0 | 0 | **0** |
| **Seguridad** | 6 | 8 | 13 | 0 | **27** |
| **Servicio Externo** | 4 | 32 | 0 | 0 | **36** |
| **Software** | 6 | 8 | 1 | 0 | **15** |
| **Total** | **26** | **87** | **31** | **5** | **149** |

Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

**Figura No.3: Relación de incidentes por categoría del 2012 al 2015**




Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

**Resultados de los indicadores de gestión**

Los indicadores más relevantes para este levantamiento son:

- Incidentes mayores registrados.
- Cantidad de pruebas realizadas al plan de continuidad.
- Cantidad de riesgos de continuidad identificados.
- Cantidad de riesgos registrados.
- Cantidad de incidentes de seguridad.

Durante el año 2014 a la fecha, se han registrado nueve (9) incidentes mayores y ninguno de estos son productos a incidentes de seguridad. Las pruebas realizadas al plan de continuidad se han realizado al cien por cierto de lo programado y sin ningún contratiempo. No se han identificados nuevos riesgos en el sistema de gestión y los incidentes de seguridad del 2012 al 2015 ha acumulado un total de 27 casos.

Los informes de desempeño de los servicios de TI indican que los servicios superan el 99% de disponibilidad prometido a los clientes, pero la satisfacción de los mismos ha disminuido por los eventos de seguridad que se han presentado.

### 2.8.1. Encuesta

La presente encuesta está enfocada al análisis del proceso de gestión de seguridad de la información de la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC), con el fin de identificar posibles oportunidades de mejoras en el proceso.

**Alcance de la encuesta:** Todo el personal que maneja, supervisa y controla los sistemas de información de la OPTIC.

**Escala de las preguntas:** El número [5] es "Totalmente de Acuerdo" y el [1] "Totalmente en Desacuerdo".

**Preguntas formuladas:**

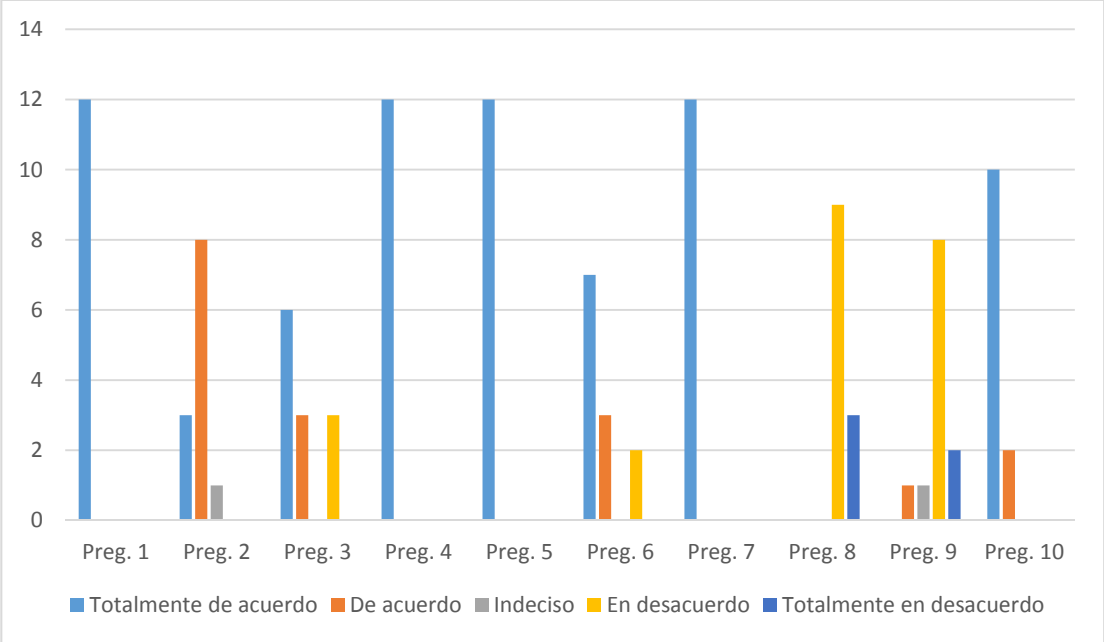
- El personal de TI cuenta con las competencias y aptitudes necesarias para afrontar los incidentes de seguridad.
- Se cuenta con los controles lógicos necesarios para mitigar las vulnerabilidades.
- Se cuenta con los controles físicos mínimos necesarios.
- Se cuenta con políticas, procedimientos e instructivos documentados de seguridad de información.
- Las informaciones alojadas son de carácter críticos.
- Se cuenta con Back-Up o respaldo de todos los sistemas de información.
- La institución cuenta con planes de contingencia y centro alterno de continuidad del negocio.
- Se invierten los recursos necesarios en seguridad de la información.
- El data center está adecuado ante amenazas de seguridad física.
- Se cuenta con los controles físicos mínimos necesarios.

**Población de la encuesta:**

12 técnicos del área de TI.

## 2.8.2. Tabulación y graficación de los resultados

**Figura No.4: Tabulación de encuesta de seguridad de información.**




Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

## 2.8.3. Interpretación de los resultados

El cien por ciento de los encuestados piensa que:

- Cuentan con las competencias y aptitudes necesarias para afrontar los incidentes de seguridad.
- Tienen conocimiento de la existencia de una política de seguridad, procedimientos e instructivos documentados.
- Las informaciones alojadas son de carácter crítico.
- La institución cuenta con un plan de contingencia.

Por otra parte, los encuestados piensan que:

- El personal técnico considera que hacen faltan controles lógicos para mitigar vulnerabilidades.
- No se cuenta con los controles mínimos necesarios.

- No re realizan back-up a todos los sistemas de información o por lo menos los que se están realizando no van de acuerdo a la política de Back-up.
- No se invierten los recursos necesarios.

# CAPÍTULO III
# PROPUESTA DE MEJORA DEL PROCESO

## 3.1 Análisis de impacto del negocio (BIA)

La interrupción de los servicios, puede causar un impacto negativo al negocio, orientado en varias direcciones:

- **Financieros:** Debido a los sobrecostos necesarios para la restauración del servicio y a la pérdida del valor del servicios ante sus clientes.
- **Imagen:** Esta puede provocar problemas de imagen pública del proveedor y posteriormente la pérdida de clientes actuales y la reducción de la captación de nuevos clientes.

El proveedor ha pactado con el cliente los objetivos del servicio, entre ellos la disponibilidad, el cual será el principal factor que este plan busca mantener.

El objetivo de disponibilidad esta trazado en un 99% de disponibilidad permite un tiempo de caída de 87.6 horas anuales, debido a la naturaleza del servicio, y las limitaciones financieras que lo circundan, el proveedor ha pactado ciertas exclusiones de disponibilidad, estas exclusiones son las siguientes:

- Desastres naturales.
- Mantenimientos programados dentro de las ventanas de mantenimiento.
- Ataques maliciosos.
- Acciones legales tomadas contra el cliente.
- Interrupciones causadas por situaciones de índole social como revueltas, guerras o protestas que causen daños a las instalaciones o componentes relacionados con el servicio.

- Daños causados por mala administración de los clientes.

Ante estas situaciones, el proveedor de servicios hará su mejor esfuerzo por la restauración del servicio, teniendo en cuenta las prioridades establecidas por los lineamientos gubernamentales establecidos en caso de la emergencia.

Ante los incidentes fuera de estas exclusiones, se ha establecido la siguiente matriz de impacto:

**Tabla No.3: Tabla de matriz de impacto**

| Servicio | Impacto | Bajo | Moderado | Alto | Critico |
|---|---|---|---|---|---|
| | Servicio de Portales Gubernamentales | 1 Hr | 8 Hr | 24 Hr | 32 Hr |
| | Servicio de Alojamiento de correo Institucional | 1 Hr | 4 Hr | 16 Hr | 24 Hr |

Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

El impacto establecerá la estrategia a tomar en relación al servicio, con el objetivo de su restauración dentro de los RTO (Recovery Time Objetive) establecidos.

**Tabla No.4: Tabla de objetivo de restauración**

| SERVICIO | RTO |
|---|---|
| Alojamiento de Portales Gubernamentales | 24 Horas |
| Alojamiento de Correo Institucional | 16 Horas |

Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

Existen servicios o procesos internos que son requeridos para los fines de operar correctamente el servicio, entre estos podemos listar:

- Procesamiento de Nomina Institucional.
- Compras y Contrataciones de Bienes, Servicios u Obras.

Estos procesos tienen un RTO no mayor a 72 horas, debido a que posteriormente a este plazo empezarían a crearse inconvenientes en el aprovisionamiento de los servicios, en la provisión de servicios contratados y el personal que soporta el servicio.

En caso de necesitar la activación del centro alterno, este no necesariamente presentaría las mismas cargas de capacidad por los que para este periodo de funcionamiento se obviarían los umbrales de capacidad para fines de inversión en expansión.

Estos servicios están basados específicamente en la plataforma de gestión financiera

## 3.2 Contingencia ante ataques o fallas

Varios tipos de amenazas pueden causar la interrupción del servicio, entre ellas la falta de disponibilidad de cualquiera de los componentes críticos del sistema, según el diagrama del servicio. Otras amenazas que pueden incidir en la falta de disponibilidad son los siniestros generados por incendios, incidentes de seguridad física, interrupción en los servicios externos relacionados al servicio, la falta de capacidad inesperada de los elementos relacionados.

Entre los riesgos más comunes que podrían impactar la continuidad del servicio se encuentran:

- Interrupción del servicio por fallo en suministro eléctrico.
- Interrupción del servicio por falta de capacidad.
- Interrupción del servicio por falta de condiciones ambientales y de localidad inadecuadas.
- Falta de conectividad del servicio.
- Interrupción del servicio por falta de datos.
- Interrupción del servicio por falta de fondos financieros.

Los criterios para activación del plan de contingencia, están contemplados dentro de los criterios de clasificación de incidentes mayores, el cual indica que todos los incidentes con potencial de comprometer al menos un 0.28% (24.36 horas) de la disponibilidad prometida serán clasificados como incidentes mayores, luego de su análisis y determinación de estrategia a seguir, dependiendo la necesidad de tiempo para restaurar el servicio y los RTO involucrados.

Dependiendo de la amenaza y el impacto causado por el incidente, se tomaran las decisiones de la estrategia más conveniente de acuerdo a las circunstancias y estado del servicio.

**Interrupción del Servicio por fallo en suministro Eléctrico**

Para la reducción del impacto de este riesgo, se han tomado las previsiones de proveer con sistemas de energía ininterrumpida (UPS) los componentes de los servicios de TI, adicionalmente a esto se cuenta con dos generadores de emergencia en serie con el fin de proveer disponibilidad N+1 de un componente alterno.

Verificar Procedimiento TI-FL-001 Procedimiento Caso de Interrupción por Fallo del Suministro Eléctrico.

**Interrupción del Servicio por Falta de Capacidad**

Verificar Procedimiento TI-FL-002 Procedimiento Caso de Interrupción por Falta de Capacidad.

**Interrupción del Servicio por falta de condiciones ambientales y de localidad inadecuadas**

Para la reducción del impacto de este riesgo, se han tomado las previsiones de proveer con sistemas enfriamiento paralelo, cada uno con la capacidad de proveer las condiciones ambientales necesarias en el cuarto de equipos de manera individual. Sin embargo, las condiciones de humedad y temperatura solo representan una parte de las condiciones ambientales la cual incluyen que el local este adecuado para el funcionamiento de los servicio.

Verificar Procedimiento TI-FL-003 Procedimiento Caso de Interrupción por Falta Condiciones Ambientales

**Interrupción del Servicio por Falta de Conectividad del Servicio**

Para la reducción del impacto de este riesgo, se han tomado las previsiones de proveer con líneas alternas de conectividad con distintos proveedores y distintas tecnologías, fibra óptica e inalámbrica.

Verificar Procedimiento TI-FL-004 Procedimiento Caso de Interrupción por Falta de Conectividad del Servicio.

**Interrupción del Servicio por falta de datos.**

El respaldo de los datos estará regulado por la política técnica de backup.

Verificar Procedimiento TI-FL-005 Procedimiento Caso de Interrupción por Falta Datos.

Los pasos de vuelta anormalidad están identificados en cada uno de los riesgos estipulados, en tal sentido la organización hará todo lo posible,

utilizando los mismos procesos habituales de gestión de incidentes, requerimientos, Compra o contratación de bienes, servicios y obras, que soportaran los pasos requeridos para la vuelta a la normalidad de los servicios.

## 3.3 Mantenimientos

Las ventanas de mantenimiento se realizarán los sábados de 11:00 PM a 5:00 AM. El objetivo es de tener un tiempo para cualquier mantenimiento o cambio que la plataforma requiera.

En el acuerdo de nivel de servicio con los clientes se debe especificar la exclusión de las ventanas de mantenimientos en los momentos que sea afectada la disponibilidad del servicio.

## 3.4 Seguridad y monitoreo

### 3.4.1 Acceso a los sistemas

El acceso a los sistemas está regulado por esta política y por las actividades surgidas de los controles adoptados para mitigar los riesgos identificados que afectan los servicios y sus componentes.

**Regla General:** Ningún usuario se puede auto asignar permisos a ninguno de los sistemas o documentación relacionados a los servicios.

Tipos de usuarios:

- **Usuarios Internos:** Usuarios bajo contrato del proveedor de servicio con los beneficios de empleado.
- **Contratistas Externos:** Consultores que tienen contratos de servicios con el proveedor de servicios.

- **Usuarios Externos:** cualquier otra persona que necesite acceso a los sistemas.

### 3.4.2 Niveles de confianza

Cada usuario será puesto en una escala del 0 al 5, esta escala gobierna el nivel de acceso que tendría el usuario a los componentes del servicio

**Tabla No.5: Nivel de confianza**

| Nivel | Tipo de Acceso |
|---|---|
| **0** | Acceso público a todos los componentes que no requieran una credencial. |
| **1** | Acceso temporal a sistemas no críticos, supervisado por un técnico responsable del sistema. |
| **2** | Acceso temporal a sistemas críticos, supervisado por un técnico responsable del sistema |
| **3** | Acceso permanente a elementos no críticos del sistema |
| **4** | Acceso administrativo a elementos no críticos del sistema. |
| **5** | Acceso administrativo a todos los elementos del sistema. |

Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

## 3.5 Protocolos de acceso físico

**Acceso físico**

Todas las facilidades están aseguradas y vigiladas por el personal del área de seguridad. El acceso físico es controlado en base los mismos niveles de confianza descritos en la tabla anterior.

Por defecto tienen permiso de acceso físico las siguientes personas:

- Personal del departamento de bomberos en servicio en caso de registrarse una emergencia.
- Personal Paramédico en servicio en caso de una emergencia médica.

- Personal Policiaco en caso de una emergencia de seguridad que amerite su intervención, previa autorización de la Alta Dirección.
- Personal del área de seguridad del proveedor de servicios.
- Personal del área de tecnologías de la información.
- La Alta Dirección.

**Desactivación de credenciales**

Es responsabilidad del área de Recursos Humanos, y de los responsables administrativos de los servicios, por parte del cliente, informar cuando un empleado sea dado de baja, con el objetivo de ser deshabilitadas sus credenciales.

## 3.6 Estructura y responsable

**Tabla No.6: Marco de Autoridades y Responsabilidades del Negocio**

| Procesos | Gestores del Proceso |
|---|---|
| **Gestión del Nivel de Servicio** | Director de Tecnologías de la Información |
| **Presentación de Informes** | |
| **Gestión de la Continuidad y Disponibilidad del Servicio** | |
| **Gestión de la Capacidad** | |
| **Gestión de la Seguridad de la Información** | |
| **Gestión Relación con los Proveedores** | |
| **Gestión de Incidentes y/o Requerimientos** | |
| **Gestión de Problemas** | |
| **Gestión de la Configuración** | |

| | |
|---|---|
| **Gestión Diseño y transición de servicios nuevos o modificados** | |
| **Gestión de Cambios** | |
| **Gestión de Entrega** | |
| **Gestión de Relación con el Cliente** | |
| **Presupuesto y Contabilidad para los Servicios** | Directora Administrativa y Financiera |

Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

**Tabla No.7: Marco de Autoridades y Responsabilidades de los Planes**

| Planes | Gestores del Proceso |
|---|---|
| **Plan del Sistema de Gestión de Servicio** | Director de Tecnologías de la Información |
| **Plan de la Continuidad del Servicio** | |
| **Plan de Capacidad del Servicio** | Encargado de Servicios de Infraestructura |
| **Plan de la Disponibilidad del Servicio** | |
| **Plan de Análisis y Evaluación de Riesgos** | |

Fuente: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC)

## 3.7 Uso aceptable de los servicios

Se prohíbe el uso del servicio o sus componentes relacionados con el fin de distribuir contenido ilegal, amenazador, difamatorio, o promover conductas por medio a este que se constituyan en un delito penal o de responsabilidad civil, o que viole cualquier ley tanto nacional como internacional.

Se prohíbe el almacenamiento de cualquier material que viole la propiedad intelectual, el proveedor de servicios se reservara el derecho de eliminar dicho contenido a solicitud de la parte afectada.

Los clientes deben abstenerse de publicar información ofensiva a la moral, material pornográfico o que infrinja las buenas costumbres.

Se prohíbe el envío de comunicaciones comerciales no solicitadas (SPAM) mediante este servicio y cualquier comunicación que acose, amenace o intimide a sus destinatarios, mediante los servicios ofrecidos por el proveedor.

Se prohíbe el envío y/o almacenamiento de código malicioso mediante cualquiera de los servicios ofrecidos por el proveedor.

Se prohíbe la falsificación de cabeceras de correo electrónico por medio a los servicios ofrecidos por el proveedor.

Se prohíbe el uso de los servicios del proveedor para fines de infringir cualquier ley, tanto nacional como internacional.

## 3.8 Uso prohibido de los servicios

La Institución no tolerará o permitirá ningún acto ilegal, abusivo, dañino o impropio de los Servicios o ningún uso de los Servicios que interfieran, o puedan interferir con el uso o goce de los Servicios por otros Usuarios.

Coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar, en cualquier forma, actos ilegales, inmorales, engañosos, y/o fraudulentos; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, y actos que invadan la privacidad de otro, actos obscenos, pornográficos, profanos, racistas, discriminatorios u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo por medio de los sistemas o componentes informáticos propiedad de la Institución.

Coleccionar, almacenar, divulgar, transmitir, instalar o solicitar cualquier material o software, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona;

Coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la ley, o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier ley nacional o internacional;

Coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos malicioso o cualquier tipo de material asociados a estos;

Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "Cartas en Cadena" o "Las Pirámides";

Falsificar encabezados de correos electrónicos, utilizar nombres de dominio que sean inválidos o inexistentes, u otras formas engañosas de enviar correo electrónico;

Transmitir correo electrónico en forma anónima, retransmitir correo electrónico a servidores de correos de terceras partes sin el permiso

correspondiente, o utilizar técnicas similares con el propósito de esconder o camuflar la fuente del correo electrónico;

Agregar, remover, o modificar encabezados de redes con información personal, con el propósito de engañar o defraudar;

Personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal;

Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar los servicios de internet por otros Usuarios, incluyendo sin limitación alguna, "negación de servicios" ataques contra otros sistemas o contra el anfitrión de redes u otros Usuarios;

Sobrecargar, inundar, atacar o de otra forma sabotear o interferir con nuestro sistema y/o redes, a través del envío de correos electrónicos o piratería de internet;

Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o de la red, cualquiera de los siguientes actos: accesar el sistema o red, monitorear datos o tráfico, sondear, copiar, probar "firewalls", atentar contra la vulnerabilidad del sistema o redes, o violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red;

Utilizar cualquier Servicio para violar la política de uso y/o términos de uso aceptable de otro proveedor de servicio;

Cualquier otra utilidad del Servicio que la Institución determine, a su sola discreción, como ilegal, abusiva o dañina.

# CONCLUSIONES

Los servicios de alojamiento web, alojamiento de portales gubernamentales, higiene de correo, entre otros, tienen más de 5 años bajo ataques maliciosos, accesos no autorizados y mal uso de los servicios por parte de los clientes, donde los demás servicios de Data Center de empresas que hacen la competencia, tienen este tema superado.

Sin embargo, la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) ha estado trabajando en el Data Center del Estado Dominicano, lugar que traerá consigo nuevas herramientas para la mitigación de riesgo y un mayor rendimiento de los servicios mismos.

Actualmente la OPTIC cuenta con 117 dominios clientes en sus servidores, siendo el de alojamiento de correo electrónico y de portales el más consumido.

En comparación al 2013, en el 2014 el servicio de correos electrónicos solo presentó dos (2) incidentes en todo el año, disminuyendo con esto un 96.77% la cantidad de incidentes.

Las mejoras realizadas en los servicios han sido producto de los grandes esfuerzos del personal técnico, independientemente de la adquisición o inversión en software y/o hardware para la mitigación de los incidentes de seguridad.

Se ha dedicado un presupuesto de RD$80,000,000.00 para la construcción del Data Center del Estado Dominicano y todos los nuevos elementos de seguridad a usar para fines de mitigación de incidentes globales de los servicios.

# BIBLIOGRAFÍA

## Libros


- García, Alfonso. (2011). Seguridad Informática, 1ra edición, Madrid, España: Editora Paraninfo, S.A.
- Pertier, Thomas. (2010). Análisis de Riesgo de Seguridad de la Información, 3era Edición, Editorial Auerbach.
- Marc, Royer, Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones, 1ra Edición, Editorial Xavier Angelet.
- Solís, Carlos. Implantar Controles de Seguridad de la Información. 2da edición, España: Editorial Academia España.
- Aguilera, Purificación. (2010). Seguridad Informática. Madrid, España: Editorial Editex, S.A


## Normas


- Sistema de Gestión de Seguridad de la Información, Norma ISO/IEC 27001:2005.
- Código de Práctica Para la Gestión de Seguridad de la Información, Norma ISO/IEC 27002:2005.
- Guía de Implementación de un Sistema de Gestión de Seguridad de la Información, Norma ISO/IEC 27003:2010.
- Gestión de Riesgos de Seguridad de la Información, Norma ISO/IEC 27005:2011
- ISO 9001:2005 - Fundamentos – Vocabulario.


## Internet


- Gestión de la Seguridad. Visión General. Encontrado Marzo 30, 2015. En Osiatis: http://itil.osiatis.es